

SYNGRESS®



CYR



Securing Exchange Server 2003 and Outlook Web Access

COVER YOUR A* BY GETTING IT RIGHT THE FIRST TIME

Henrik Walther
Patrick Santry
Technical Editor

- Prove You Did It Right the First Time
- Be Responsible, Don't Be to Blame
- Secure Your Network and Your Career

Register for Free Membership to

s o l u t i o n s @ s y n g r e s s . c o m

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2000*, Brian Caswell and Jay Beale's *Snort 2.0 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only **solutions@syngress.com** program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy to search web page, providing you with the concise, easy to access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

SYNGRESS®

CYIA



Securing Exchange Server 2003 and Outlook Web Access

COVER YOUR A* BY GETTING IT RIGHT THE FIRST TIME

Henrik Walther

Patrick Santry Technical Editor

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

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

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

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

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

KEY SERIAL NUMBER

001	CV764IHHYY
002	PO9873KSS6
003	KLASS34F62
004	IMWQ295T6T
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3
008	2987GVTWMK
009	LPE987NK34
010	629MP5SDJT

PUBLISHED BY

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

CYA: Securing Exchange Server 2003 & Outlook Web Access

Copyright © 2004 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0

ISBN: 1-931836-24-8

Acquisitions Editor: Christine Kloiber
Technical Editor: Patrick Santry
Page Layout and Art: Patricia Lupien

Cover Designer: Michael Kavish
Copy Editor: Darlene Bordwell
Indexer: Odessa&Cie

Distributed by O'Reilly & Associates in the United States and Canada.



Acknowledgments

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

Syngress books are now distributed in the United States by O'Reilly & Associates, Inc. The enthusiasm and work ethic at ORA is incredible and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Lynn Schwartz, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C.J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, and Rob Bullington.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Rosie Moss, Chris Hossack, and Krista Leppiko, for making certain that our vision remains worldwide in scope.

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

Kwon Sung June at Acorn Publishing for his support.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Geoff Ebbs, Hedley Partis, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

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



Author

Henrik Walther is a Senior Microsoft Server Consultant working for an IT outsourcing services company in Copenhagen, Denmark. Henrik has over 10 years of experience in the industry. He specializes in migrating, implementing, and supporting Microsoft Windows Active Directory and Microsoft Exchange environments.

Henrik is a Microsoft Exchange MVP (Most Valuable Professional). He runs the www.exchange-faq.dk website and writes Exchange-related articles for both www.msexchange.org and www.outlookexchange.com. He also spends time helping his peers in the Exchange community via forums, newsgroups, and mailing lists.

Henrik would like to thank his forever patient and understanding girlfriend Michella without whom he would never have been where he is today.



Technical Editor

Patrick Santry is the Corporate Webmaster for a Cary, NC-based manufacturing company. He has been designing, developing, and managing Web-centric applications for eight years. He is co-author of several books, and has authored many magazine articles. He holds MCSE, MCSA, MCP+SB, i-Net+, A+, and CIW certifications. He also writes for his highly popular web site, www.Coder.com, which is frequently featured on the ASP.NET website for articles on ASP.NET portal development. He is a frequent presenter at Microsoft events in the Northwestern Pennsylvania area.

Patrick dedicates his writing to his family: his wife Karyn, daughters Katie and Karleigh, and his son Patrick Jr. (P.J.).

Contents

About this Book	xvii
Chapter 1 Introducing Exchange 2003	
 Security	1
Exchange 2003:“Secure Out of the Box”	2
Exchange 2003: Secure by Design	4
Exchange 2003: Secure by Default	6
Outlook Web Access 2003 Security Enhancements	7
Exchange 2003: Secure by Upgrade?	8
Your A★★ Is Covered If You...	8
Chapter 2 Windows and Exchange 2003	
 Security Practices	9
In this Chapter	9
Windows 2000/2003 Security	10
Patch Management	10
Microsoft Baseline Security Analyzer	10
Network Security Hotfix Checker (Hfnetchk)	12
Recommended Windows 2003 Security	
Reading	12
Keep Up to Date on New Security Bulletins	13
Exchange 2003 Windows Dependencies	13
Exchange 2003 Components	16
Applying Best Security Practices	18
Defining Acceptable Use	19
Practice Safe Computing	20
Good Physical Security	21
Installing Exchange 2003 Best Practices	21
Installation Checklist	22
Building the Hardware Platform	22

Installing the Operating System	23
Installing Exchange 2003	23
Your A★★ Is Covered If You...	24
Chapter 3 Delegating and Controlling Permissions in Exchange 2003	25
In this Chapter	25
Delegating Administrative Control in System Manager	26
Exchange Server 2003 Permissions	26
Viewing Exchange Server Permissions in Exchange System Manager	29
Using the Exchange Administration Delegation Wizard	30
Exchange Full Administrator	31
Exchange Administrator	32
Exchange View Administrator	32
Controlling Mailbox Permissions	36
Delegating Mailbox Access Through Outlook 2003	36
Granting Mailbox Permissions to Folders Without Using Delegation	39
Opening the Additional Mailbox	40
Granting Mailbox Permissions Through Active Directory	43
Controlling Public Folder Permissions	45
Creating and Setting Permissions on Public Folders in Outlook 2003	46
Creating and Setting Permissions on Public Folders in System Manager	49
Setting Permissions on Top-Level Public Folders in Exchange System Manager	53
Your A★★ Is Covered If You...	53
Chapter 4 SMTP Security	55
In this Chapter	55
Securing the SMTP Service	56
SMTP Authentication Settings	59
Secure SMTP Communication	60

Setting Relay Restrictions	62
SMTP Connectors and Relaying	64
Setting Mailbox Message Limits	67
Setting Mailbox Message Limits Globally	68
Configuring Internet Message Formats	69
Setting Public Folder Limits	70
Protecting Mail-Enabled Groups	71
Enabling SMTP Protocol Logging	72
Modifying the SMTP Banner	75
Configure a Corporate Legal Disclaimer	79
SMTP Relaying	80
Open Relay Test Methods	83
E-Mail Address Spoofing	85
Authentication and Resolving E-Mail Addresses .	86
Reverse DNS Lookup	87
Internet Mail Headers	89
Your A** Is Covered If You...	92
Chapter 5 Securing the Outlook Web Access Server	93
In this Chapter	93
OWA Authentication	94
OWA Virtual Directories	94
Authentication Methods	98
Read, Write, Browse, and Execute Permissions .	100
Connection Limits	101
Enabling SSL on OWA	103
Installing the Microsoft Certificate Service .	104
Creating the Certificate Request	108
Third-Party Certificates	116
Restricting User Access	116
Disabling OWA Access for a Specific User .	117
Disabling OWA Access for a Server	119
OWA Segmentation	119
Allowing Password Changes Through OWA . . .	120
Creating the IISADMPWD Virtual Directory .	121

Enabling the Change Password Button in OWA	124
Testing the Change Password Feature in OWA	125
Redirecting HTTP Requests to SSL Requests	127
Your A★★ Is Covered If You...	131
Chapter 6 OWA Front-End/Back-End Deployment Scenarios	133
In this Chapter	133
Deploying a Single-Server Scenario	134
Deploying a Front-End/Back-End Scenario	136
HTTP Authentication	136
Using Dual Authentication	137
Using Pass-Through Authentication	138
Securing a Front-End Server	139
Disabling Unnecessary Front-End Services	140
Dismounting and Deleting the Mailbox Store	141
Dismounting and Deleting the Public Folder	
Store	143
Front-End Servers in the Perimeter Network	144
Allowing RPC Traffic Through the Intranet	
Firewall	145
Disallowing RPC Traffic Through the Intranet	
Firewall	146
Using IPSec	148
URLScan	150
Front-End Servers on the Internal Network	150
Exchange 2003 Behind an ISA Server 2000	152
Publishing the Exchange 2003 Services	153
Message Screener	154
OWA 2003 Publishing	154
More ISA Server Information	155
Your A★★ Is Covered If You...	156
Chapter 7 Outlook Web Access Client Security Features	157
In this Chapter	157
S/MIME Support	158

Junk E-Mail Filter	162
Safe Senders	163
Safe Recipients	164
Blocked Senders	164
Web Beacon Blocking	166
Enhanced Attachment Blocking	168
Forms-Based Authentication	170
Username and Password	173
Clients: Premium and Basic	173
Security: Public or Shared Computer and Private Computer	174
Your A★★ Is Covered If You	177
Chapter 8 Exchange Protocol/Client Encryption	179
In this Chapter	179
Encrypting SMTP Traffic	180
Configuring SMTP with TLS/SSL	180
Enabling TLS/SSL for Inbound Mail	185
Enabling TLS/SSL for Outbound Mail	187
Enabling TLS/SSL for One or More Domains .	188
Enabling IPSec Between SMTP Servers	188
Encrypting MAPI Information on the Network .	189
Encrypting POP3 and IMAP4 Traffic	190
Securing Clients Using S/MIME	192
Using S/MIME	193
Enabling S/MIME and Outlook	194
Configuring RPC over HTTP(S)	195
Requirements	196
Configure RPC Over HTTP on a Front-End Server	198
Specifying the RPC Proxy Ports	202
Disabling DCOM Support in RPC over HTTP	204
Configuring the Client	205
Your A★★ Is Covered If You...	212

Chapter 9 Combating Spam	213
In this Chapter	213
Client-Side Filtering	214
Safe Senders	217
Safe Recipients	218
Blocked Senders	219
Server-Side Filtering	222
Connection Filtering	224
Display Name	225
DNS Suffix of Provider	225
Custom Error Message to Return	227
Return Status Code	227
Disable This Rule	228
Exception Lists	229
Global Accept and Deny List	230
Recipient Filtering	234
Filtering Recipients Not in the Directory	235
Sender Filtering	235
The Intelligent Message Filter	237
Things Worth Noting About the IMF	238
Your A★★ Is Covered If You...	240
Chapter 10 Protecting Against Viruses	241
In this Chapter	241
E-Mail Viruses	242
Server-Side Protection	244
Exchange Server	245
SMTP Gateway	248
Client-Side Protection	249
Educate Your Users	250
Default Outlook 2003 Attachment Blocking	251
Cleaning Up After a Virus Outbreak	254
Your A★★ Is Covered If You...	260

Chapter 11 Auditing Exchange	261
In this Chapter	261
Windows 2000/2003 Auditing	262
Auditing Changes to the Exchange Configuration	264
Exchange Diagnostics Logging	266
Microsoft Operations Manager and Exchange 2003	269
Your A★★ Is Covered If You...	270
Appendix Planning Server Roles and Server Security	271
Understanding Server Roles	272
Domain Controllers (Authentication Servers)	275
Active Directory	275
Operations Master Roles	276
File and Print Servers	278
Print Servers	278
File Servers	279
DHCP, DNS, and WINS Servers	279
DHCP Servers	279
DNS Servers	279
WINS Servers	280
Web Servers	280
Web Server Protocols	280
Web Server Configuration	280
Database Servers	282
Mail Servers	282
Certificate Authorities	282
Application Servers and Terminal Servers	282
Application Servers	283
Terminal Servers	285
Planning a Server Security Strategy	285
Choosing the Operating System	287
Identifying Minimum Security Requirements for Your Organization	289
Identifying Configurations to Satisfy Security Requirements	291

Planning Baseline Security	292
Customizing Server Security	292
Securing Servers According to Server Roles	292
Security Issues Related to All Server Roles	293
Securing Domain Controllers	297
Securing File and Print Servers	298
Securing DHCP, DNS, and WINS Servers	300
Securing Web Servers	301
Securing Database Servers	302
Securing Mail Servers	303
Index	305



About the Series

Network System Administrators operate in a high-stress environment, where the competitive demands of the business often run counter to textbook “best practices”. Design and planning lead times can be non-existent and deployed systems are subject to constant end-runs; but at the end of the day, you, as the Administrator, are held accountable if things go wrong. You need help and a fail-safe checklist that guarantee that you’ve configured your network professionally and responsibly. You need to “CYA”.

CYA: Securing Exchange Server 2003 and Outlook Web Access is part of the new CYA series from Syngress that clearly identifies those features of Exchange/OWA that represent the highest risk factors for attacks, performance degradation and service failures; and then walks you through step-by-step configurations to assure they have been thorough and responsible in their work.

In this Book

This book fills the need of Networking professionals whose Exchange/OWA installation is vulnerable to attacks, poor performance, or down time because it has been improperly configured or maintained. It will provide:

- A comprehensive “checklist” to all of the security related configuration consoles in Exchange/OWA.
- A clear presentation of Microsoft’s recommended security configurations/policies based on the business needs of your network.
- A warning of the drawbacks of some of the recommended practices. The promise to the readers is essentially that they won’t get busted for being negligent or irresponsible if they follow the instructions in the book.

The book is organized around the security services offered by Exchange/OWA. The table of contents reflects the hierarchy of topics within the Exchange/OWA MMC, and covers the configuration options within Exchange/OWA that relates to security.

In Every Chapter

There will be several introductory paragraphs with a **By the Book** configuration checklist. This section identifies, according to the product manufacturer, the function/benefit/protection of the feature that you are about to configure. There are also sections entitled **Reality Checks** that provide you with insight into situations where **By the Book** may not be the only solution, or where there are hidden costs or issues involved with the **By the Book** solution.

Your A** is Covered if You...

At the end of every chapter, you are provided with a bullet list of items covering the most essential tasks completed within the chapter. You will use this section to make sure you are ready to move on to the next set of configurations in the following chapter.

Chapter 1

Introducing

Exchange 2003 Security

Welcome to Exchange Server 2003—Microsoft's latest messaging server, which was released in late 2003. Exchange 2003 is the first Exchange release specifically developed following the Microsoft Trustworthy Computing Initiative, making it the most secure version of Exchange ever released. As the title of this book indicates, we will focus on the security-related features of Exchange 2003 and Outlook Web Access (OWA). We will supply you with best-practice solutions, step-by-step instructions, and plenty of insider tips and real-world insights. But before we jump into a detailed discussion of the security-related features of the product, let's first take a superficial look at the features that have made Exchange 2003 more secure than any previous versions.

Exchange 2003: “Secure Out of the Box”

When Microsoft came up with its Trustworthy Computing Initiative in 2002, the company conducted a full code review of all its products in an attempt to locate potential security problems. When they found problems, they tightened the security of the product even further. The first product to benefit from this initiative was Microsoft Windows 2003 Server; then came Microsoft Exchange Server 2003.



BY THE BOOK...

Exchange Server 2003 benefits from the Trustworthy Computing Initiative, a Microsoft initiative to improve customers' experience in the areas of security, privacy, reliability, and business integrity. As part of this initiative, which was introduced companywide in January 2002, Microsoft now follows development processes that help ensure that its products and product deployments are secure. The Microsoft Exchange Server 2003 team incorporated those processes to create a product that is secure by design, secure by default, and secure in deployment. After deployment, Microsoft supports ongoing customer and partner communications about security issues. The result is that Exchange Server 2003 is the most secure version of Exchange to date.

We already mentioned that Exchange Server 2003 is the most secure Exchange version released to date, but bear in mind that to achieve the most secure Exchange 2003 environment possible, Exchange 2003 must be installed on a Windows 2003 server. We say this because it's also possible to install Exchange 2003 on Windows 2000 (SP3) server. Because Windows 2003 Server has been through a full code review and has been designed with security in mind, by default it's much more secure than Windows Server 2000. In terms of security, Internet Information Server (IIS) especially has been improved from Windows 2000 to 2003. And because Exchange has been heavily integrated with IIS, both in regard to OWA and because of the change to use SMTP as its basic messaging transport protocol, this affects Exchange quite a lot as well. You may ask, doesn't Exchange include its own SMTP service? No; when you install Exchange, it actually extends IIS's SMTP service further and uses this as its primary messaging transport service. This is the reason that it's a requirement that the IIS SMTP service be installed before you can install Exchange 2003.

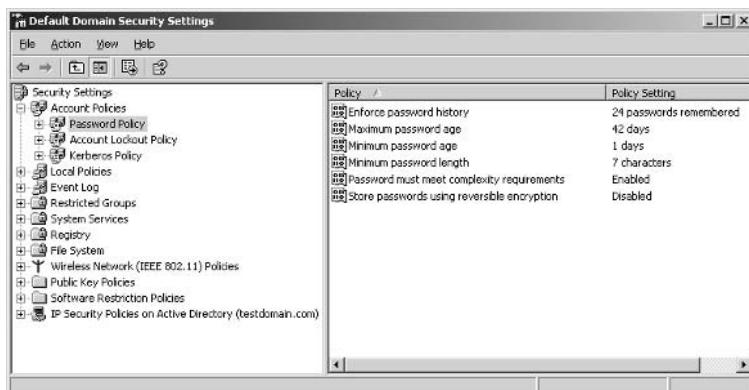


REALITY CHECK...

If you want to learn more about the Microsoft Trustworthy Computing Initiative in general, we suggest you visit the Trustworthy Computing site at www.microsoft.com/mscorp/twc.

Other default Windows 2003 Server settings that affect Exchange 2003 are the strong password policy, which is much stricter than the defaults in Windows 2000. Take a look at Figure 1.1, which shows the default password policy on a Windows 2003 server.

Figure 1.1 Windows 2003 Strong Password Policy Defaults



Because Exchange users normally use a Windows account to log into their mailboxes, this strong password policy clearly improves security in your Exchange 2003 environment. If you don't change this policy, it will actually be very difficult for an attacker to, for example, obtain a user's password by running a brute-force attack (one that involves trying every possible code, combination, or password until you find the right one) or something similar against your AD domain. For Exchange 2003 security, it hinders the chance of experiencing SMTP Auth attacks in your messaging environment.



REALITY CHECK...

For those who don't know what an SMTP Auth attack is all about, it basically means that one or more of your Windows user accounts are hijacked, typically by an evil spammer, who can then use the account to send spam by relaying through your

server, even though you don't have an open relay. One of the primary ways to defend against this type of attack is to have user accounts with strong passwords. In Chapter 4, we'll talk a lot more about these kind of attacks and what you can do to prevent them.

When you install Windows 2003 Server, the OS is secure by default, meaning that a lot of the OS components will be in a locked-down state, and many services that were enabled by default in Windows 2000 Server are disabled in Windows 2003 Server. Users and services also get only the permissions they need to do their jobs. For example, take IIS. As you probably remember, IIS was installed and enabled by default in Windows Server 2000. However, the IIS component is not even installed in Windows 2003, which is a big improvement.

Exchange 2003: Secure by Design

When the Exchange 2003 development team was making Exchange 2003, they went through a secure-by-design process (as part of the Trustworthy Computing Initiative) whereby they initiated a security audit. This audit involved spending two months studying each Exchange component and the interaction between components. For every potential security-related threat they found, they had to do a threat analysis to evaluate each issue. To combat the issues, they did additional design and testing work to neutralize the potential security issues.

The whole idea behind this security audit was to make sure all components included in Exchange didn't perform in a way that wasn't intended. To eliminate as many security threats as possible, the team even hired an external security consultant firm to do an independent review of each software component contained in Exchange. This independent team also did an analysis of various threat scenarios.

Thanks to these design efforts, Exchange includes many server security features. For example, it's now possible to restrict distribution list access to authenticated users. You can also specify users who can and can't send to specific distribution lists. This is especially a good defense against spam and other unsolicited mail. Finally, Exchange 2003 natively supports real-time block lists (RBLs), which help organizations fight spam and other unsolicited e-mail (though some might say the feature is a little too basic). Exchange 2003 has an inbound recipient filtering option, which reduces the amount of received spam and other unsolicited e-mail by filtering inbound e-mail based on the recipients. E-mail that is addressed to users who are

not found or to whom the sender does not have permissions to send is not accepted for delivery. We will talk much more about the native Exchange 2003 antispam features and provide step-by-step instructions on how to configure them properly in Chapter 9.

Exchange 2003 also supports what is known as signed Lightweight Directory Access Protocol (LDAP) requests in Active Directory, with which Exchange administrative components are signed and sealed by default when using LDAP to communicate with Active Directory. This feature can reduce the risk of “man-in-the-middle” attacks.

Exchange 2003 includes the capability for recipients to verify whether a message was from an authenticated or anonymous sender outside the organization. This helps users understand whether a message originated from a user spoofing a sender address. (*Spoofing* is the practice of pretending to be someone else to deceive users into providing passwords and other information to facilitate unauthorized access into an environment.)

In addition to these new Exchange 2003 features, the Exchange team also improved further on some of the existing features already found in Exchange 2000. Here are some of the more important improvements:

- **Virus Scanning Application Programming Interface (VSAPI) 2.5** Exchange 2003 improves the virus-scanning API by allowing antivirus products to run on Exchange servers that do not have resident Exchange mailboxes. Antivirus products are allowed to delete messages and send messages to the sender in the Exchange 2003 AV API 2.5 version.
- **Clustering authentication** Exchange Server 2003 clustering supports Kerberos authentication against an Exchange virtual server.
- **Administrative permissions** Cross-forest support and the ability to administer both Exchange 2000 Server and Exchange Server 2003 help organizations that have segmented the administration of their Windows-based environment and Exchange environment into two unique groups.
- **Ability to restrict relaying** Relaying can be restricted to a limited number of security principles through the standard Windows 2000 Discretionary Access Control List (DACL). The ability to grant relaying to an IP address is still present.
- **Public folder permissions for unknown users** Folders with distinguished names in access control lists that cannot be resolved to Security IDs drop the unresolvable distinguished names.

Exchange 2003: Secure by Default

Exchange 2003 is secure not only by design but also by default, which means that potentially vulnerable components are disabled by default. Customers can enable these as appropriate for their specific environment. For example, Exchange 2003 introduces new default message sizes for both mailbox stores and public folders stores. The new sending message size and the receiving message size are, by default, set to 10MB, if the value isn't already set. This means that if you do an in-place upgrade from Exchange 2000 to 2003, and you specified a specific message size in Exchange 2000, this setting will not be overridden by the new Exchange 2003 setting. If a message size hasn't been specified (no limit), Exchange 2003 will set the new value to 10MB. This size limit also applies to messages posted to your Exchange 2003 Public Folder Stores.

You might remember that in Exchange 2000 it was possible for “Everyone” to create a top-level public folder. This setting has fortunately also been changed, so now only domain admins, enterprise admins, and members of the Exchange Domain Servers group can create these top-level public folders. The Exchange 2000 “bug,” which was guilty of resetting already specified top-level public folder permissions back to “Everyone” when a new Exchange 2000 server was installed into the Exchange organization, has also been eliminated.

Anonymous authentication for Network News Transfer Protocol (NNTP) has been disabled in Exchange 2003. When Exchange 2003 is installed on a member server, a Group Policy does not allow accounts with only User permissions to log on locally to the server, as was the case in Exchange 2000.

Seldom-used protocols such as Post Office Protocol (POP), Internet Message Access Protocol (IMAP), and NNTP are disabled on new Exchange 2003 installations, but keep in mind that during an in-place upgrade from Exchange 2000, for example, the settings specified in Exchange 2000 are retained for these protocols.

The new Outlook Mobile Access (OMA) feature is also disabled by default, which reduces attack by noncompany-controlled clients. The OMA is a new feature that enables mailbox access from mobile devices such as PocketPCs and smart phones.

If it's not already configured on the server, the Exchange System Manager recommends Secure Socket Layer (SSL) when you promote an Exchange server to a front-end server.. This is a nice addition because there are still too many people deploying OWA over the nonsecure Hypertext Transfer Protocol (HTTP).

Outlook Web Access 2003 Security Enhancements

One of the components in Exchange 2003 that has benefited from a complete update, in terms of both functionality and security improvements, is Outlook Web Access (OWA). OWA now supports S/MIME, just like the full Outlook MAPI client. This is a big improvement because it allows you to digitally sign and encrypt e-mail messages and attachments to protect them against tampering or eavesdropping. OWA also provides session inactivity timeouts when you're using forms-based authentication (see Figure 1.2).

Figure 1.2 OWA 2003 New Forms-Based Authentication Logon Page



This feature allows support for timed logoff as well as secure logoff, even if the browser is left open with a current session to the server. In addition, OWA supports attachment blocking, making it possible for customers to selectively disable attachments being viewed outside the firewall. Customers can prevent sensitive documents from being downloaded outside the network or cached on a potentially insecure hard drive at an Internet kiosk. OWA also includes a privacy protection feature via which, by default, content from outside a user's network is automatically blocked. Users can override this to view external content. This feature helps prevent spammers from identifying valid e-mail addresses by links to external content. OWA includes a junk e-mail filter and supports block and sender lists, just like the full Outlook 2003 MAPI client.

If you think we rushed a little too fast through the new OWA features, don't worry—they will be covered in depth in Chapter 7.

Notes from the Underground...

Remember to Visit Microsoft's Exchange Security Site

To keep up to date with all the changes, we recommend you regularly visit the Microsoft Exchange Security site. It already contains a wealth of good Exchange 2003 security-related information. The site can be found at www.microsoft.com/exchange/security.

Exchange 2003: Secure by Upgrade?

Upgrades of Exchange 2000 and Windows 2000 are possible, and many organizations will undoubtedly follow this path rather than installing new servers. The upgrade is possible, provided that you upgrade Exchange 2000 to Exchange 2003 first and then the Windows 2000 platform to Windows 2003. Carefully installed Exchange 2000 installations may already be more secure than a basic Exchange 2003; this is especially true if you have followed good security practices with Exchange 2000. More information on upgrades and Exchange compatibility can be found at www.microsoft.com/exchange/evaluation/ti/TiWinNet.asp. We still recommend a fresh installation of both Windows 2003 and Exchange 2003, if possible, using an installation checklist that focuses on not only security but system stability.

Your A Is Covered If You...**

- Know what the Microsoft Trustworthy Computing Initiative is all about and know how it affects Microsoft products such as Windows 2003 Server and Exchange 2003.
- Are aware of the default settings when comparing Exchange 2000 and Exchange 2003.
- Have a superficial idea of the new and/or enhanced security features introduced in Exchange and OWA 2003.

Chapter 2

Windows and Exchange 2003

Security Practices

In this Chapter

No matter what type of environment you're dealing with, we strongly advise you to take security seriously. A successful attack on the servers in your organization's Exchange Messaging environment can be quite severe, greatly damaging the entire organization and costing huge amounts of money in lost productivity.

In this chapter, we'll look at the following issues:

- Windows 2000/2003 security
- Exchange 2003 Windows dependencies
- Applying best security practices
- Installing Exchange 2003 best practices

This chapter will provide you with useful information needed in order to successfully install, maintain, and secure your Exchange Messaging environment. We start by giving you a few tips and relevant links you will find useful when installing and maintaining your Exchange messaging servers. You will also be presented with information on how the various Exchange services depend on Windows. We end the chapter by providing you with a couple of best practices.

While this chapter will only touch upon some issues, you can refer to the Appendix at the back of this book for additional information on Windows and server security.

Windows 2000/2003 Security

To end up with a secure Exchange 2003 messaging environment, you must keep in mind that the operating system (OS) needs as much attention as Exchange itself. But if this book were to cover all Windows-related security issues in addition to Exchange security, we would still be writing! So instead we provide a few tips as well as some helpful Windows security-related Microsoft links.



BY THE BOOK...

One of the biggest problems in regard to computer security is that many organizations find it hard to believe that anything bad can happen to them—until it does. Unfortunately, the truth is that bad things do happen, and they actually happen far more often than you might think. No matter how or why your business is attacked, recovering the lost “stuff” usually takes significant time and effort. Try to imagine if your computer systems were unavailable for, say, a week. Or imagine if you lost all the data stored on the Windows/Exchange servers in your organization. Those are scary thoughts, so we can’t say it too many times: Take security seriously! Otherwise, it’s just a matter of time and you will have cause to regret not taking it seriously. If you don’t want to spend large amounts of money on security software, consider using some of the free utilities such as MBSA and Hfnetchk, available for download directly from Microsoft. We will provide you with more information and download links to these tools in this section.

Patch Management

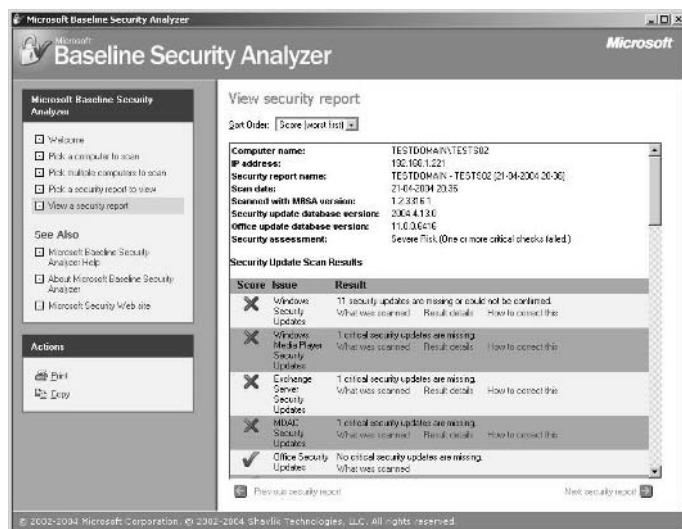
One of the most vital things to keep your Exchange messaging environment as secure as possible is to remain current with the latest patches, for both Windows 2000/2003 and Exchange. To keep current with the latest patches, Microsoft provides a couple of free utilities: MBSA and Hfnetchk.

Microsoft Baseline Security Analyzer

As part of Microsoft’s Strategic Technology Protection Program and in response to direct customer need for a streamlined method of identifying common security misconfigurations, Microsoft developed the Microsoft Baseline Security Analyzer (MBSA). MBSA Version 1.2 (which is the

most recent version at the time of this writing) includes a graphical and command-line interface that can perform local or remote scans of Windows systems. MBSA can determine which critical security updates are applied to a system by referring to an Extensible Markup Language (XML) file (mssecure.xml) that is continuously updated and released by Microsoft. The XML file contains information about which security updates are available for particular Microsoft products. This file contains security bulletin names and titles as well as detailed data about product-specific security updates, including files in each update package and their versions and checksums, registry keys that were applied by the update installation package, information about which updates supersede others, related Microsoft Knowledge Base article numbers, and much more. To see MBSA in action, take a look at Figure 2.1.

Figure 2.1 MBSA in Action



As you can see, the Exchange server on which MBSA was run seriously needs patching!

MBSA 1.2 supports most of the Microsoft operating systems and server products, including Windows 2003 and Exchange 2003. To provide thorough details about MBSA, Microsoft released a white paper, which can be read at Microsoft Baseline Security Analyzer V1.2: www.microsoft.com/technet/security/tools/mbsawp.mspx.

To download a copy of MBSA 1.2, visit Microsoft Baseline Security Analyzer V1.2 at www.microsoft.com/technet/security/tools/mbsahome.mspx#XSLTsection124121120120.

Network Security Hotfix Checker (Hfnetchk)

The Hfnetchk tool is a command-line tool that administrators can use to centrally assess a computer or group of computers for the absence of security updates. As of the version 1.1 release of the MBSA, Hfnetchk is exposed through the MBSA command-line interface, mbsacli.exe /hf. The latest version of the Hfnetchk engine is available in MBSA version 1.2. To see Hfnetchk in action, have a look at Figure 2.2.

Figure 2.2 Hfnetchk in Action

```
C:\>Program Files\Microsoft Baseline Security Analyzer>mbsacli /hf
Microsoft Baseline Security Analyzer
Version 1.1 (Build 3315.1)
(C) Copyright 2002-2004 Microsoft Corporation. All rights reserved.
HFNetChk developed for Microsoft Corporation by Shavlik Technologies, LLC.
(C) Copyright 2002-2004 Shavlik Technologies, LLC. www.shavlik.com

Please use the -v switch to view details for
Patch NOT Found, Warning and Note messages

Scanning TESTS02
Attempting to get CAB from http://go.microsoft.com/fwlink/?LinkId=18922
XML successfully loaded.

Done scanning TESTS02
TESTS02 (192.168.1.221)

* WINDOWS SERVER 2003, STANDARD EDITION GOLD
Patch NOT Found MS03-023 823559
Note MS03-030 819696
Patch NOT Found MS03-034 824105
Patch NOT Found MS03-041 823182
Patch NOT Found MS03-043 828835
Patch NOT Found MS03-044 825519
Patch NOT Found MS03-045 825541
Patch NOT Found MS04-011 835732
Patch NOT Found MS04-012 828741
Patch NOT Found MS04-014 837001

* INTERNET INFORMATION SERVICES 6.0 GOLD
```

To get more detailed information about Hfnetchk, read Microsoft KB article 303215, “Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available,” at www.support.microsoft.com/?id=303215.

Recommended Windows 2003 Security Reading

Here we list some of the best Microsoft documentation—absolutely mandatory reading:

- **Windows Server 2003 Security Guide** www.microsoft.com/downloads/details.aspx?FamilyID=8a2643c1-0685-4d89-b655-521ea6c7b4db&displaylang=en



REALITY CHECK

The Windows 2003 Security Guide should be used in conjunction with the Exchange 2003 Security Hardening Guide, which can be downloaded from Exchange Server 2003 Security Hardening Guide at www.microsoft.com/downloads/details.aspx?FamilyID=6A80711F-E5C9-4AEF-9A44-504DB09B9065&displaylang=en

- **Technical Overview of Windows Server 2003 Security Services** www.microsoft.com/windowsserver2003/techinfo/overview/security.mspx
- **Windows 2000 Security Hardening Guide**
www.microsoft.com/downloads/details.aspx?FamilyID=15e83186-a2c8-4c8f-a9d0-a0201f639a56&displaylang=en
(if you're using Windows 2000)

Keep Up to Date on New Security Bulletins

To keep up to date on any new patches Microsoft releases, we recommend that you subscribe to the Microsoft Security Bulletins, which can be found at Get Notified Right Away of Important Security Updates, www.microsoft.com/security/security_bulletins/alerts2.asp.

Exchange 2003 Windows Dependencies

Exchange 2003 is completely dependent on several components of Windows 2000/2003 operating system. It's therefore vital that you know the ins and outs of these services and why Exchange depends on them. Failing to do so will quickly have you end up in a not so pleasant Exchange admin role.



BY THE BOOK...

Exchange 2003 is tightly integrated with Windows 2000/2003, which among many other things means that the Exchange 2003 services are dependent on several Windows 2000/2003 services.

The Internet Information Server (IIS) element of the Windows product is especially vital for Exchange to work.

A list of services (see Table 2.1) must be running prior to the Exchange 2003 System Attendant starting. The first of these dependencies is the Windows Active Directory itself. Previous versions of Exchange included a fairly sophisticated directory service; this directory service was touted by many as the “crown jewel” of the Exchange platform. This directory contained information about each mailbox such as the home Exchange server name, message size restrictions, and storage restrictions as well as mailbox owner “white pages” information such as address, city, state, and telephone number. A sometimes complex process to keep the directories between Exchange 4.0 and 5.x servers had to be maintained. Since Active Directory is capable of providing sophisticated directory services, the need for a separate directory is not necessary; thus Exchange 2003 uses the Windows Active Directory to store configuration information as well as information about all mailboxes and other mail-enabled objects. The Active Directory bears a resemblance to the earlier versions of the Exchange directory due in part to the fact that many of the developers were transferred to the Active Directory team. Exchange servers must maintain communication with at least one Active Directory domain controller and global catalog server at all times.

Table 2.1 Exchange 2003 Services and Dependencies

Exchange 2003 Service	Windows 2000/2003 Service Dependencies
Microsoft Exchange System Attendant (mad.exe) (Mailer Administrative Daemon)	Remote Procedure Call (RPC) Remote Procedure Call (RPC Locator) NT LM Security Support Provider Event Log Server Workstation
Microsoft Exchange Information Store(store.exe) (This service usually consumes most of the RAM in an Exchange server. This is normal.)	IIS Admin Service Microsoft Exchange System Attendant
Simple Mail Transport Protocol (SMTP) (process of inetinfo.exe, installed with Windows 2000)	IIS Admin Service

Continued

Table 2.1 Exchange 2003 Services and Dependencies

Exchange 2003 Service	Windows 2000/2003 Service Dependencies
Microsoft Exchange Routing Engine (process of inetinfo.exe)	IIS Admin Service
Microsoft Exchange IMAP4 (process of inetinfo.exe)	IIS Admin Service
Microsoft Exchange POP3 (process of inetinfo.exe)	IIS Admin Service
Microsoft Exchange MTA Stacks (emsmta.exe)	IIS Admin Service Microsoft Exchange System Attendant
Network New Transport Protocol (NNTP) (process of inetinfo.exe, installed with Windows 2000)	IIS Admin Service
Microsoft Search (mssearch.exe)	NT LM Security Support Provider Remote Procedure Call (RPC)



REALITY CHECK

Exchange 2003 will not function if it loses communication with either a domain controller and/or a global catalog server. Communications with these servers must be guaranteed for message flow to continue.

Prior to Exchange 2003 installation, the Windows 2000 or Windows 2003 server must have the Internet Information Services (IIS) HTTP, SMTP, and NNTP components installed and running. Once Exchange 2003 is installed, these services do not necessarily need to remain running, but some services (such as Web services or message transport) will not function if they are disabled.

During Exchange installation, the SMTP and NNTP components are extended to provide additional functionality required by Exchange. Virtual HTTP directories are created to provide access to Outlook Web Access (OWA) supporting files, mailboxes, and public folders. The Exchange installation process also installs POP3 and IMAP4 services that function as part of IIS.

The IIS SMTP service is extended during the installation of Exchange to allow the service to expand distribution lists, query the Active Directory for mailbox properties, use the routing engine, and provide Exchange-to-Exchange communication. All Exchange 2000/2003-to-Exchange 2003 communications are handled via the SMTP engine. One of the components is called the Advanced Queuing Engine; this component processes every message that is sent on the Exchange server.

Exchange 2003 Components

Exchange Server is not a single, large program, but rather a number of small programs that each carry out specialized services. The Exchange installation process not only installs new services—it extends a number of existing Windows services. Table 2.1 lists the common Exchange 2003 services, each service's executable service, and the Windows 2000/2003 service on which this service depends. This table differs slightly for Exchange 2000; the service dependencies were flattened out so that Exchange could restart more quickly in a clustered environment.

The first Exchange-specific component that starts is the Microsoft Exchange system attendant. The system attendant service runs a number of different processes. One of these processes is the DSAccess cache; this cache keeps information that has been recently queried from Active Directory. The default cache lifetime is 5 minutes. As a general rule, components such as the Information Store and IIS use the DSAccess cache rather than querying Active Directory over and over again. The exception to this rule is the SMTP Advanced Queuing Engine (AQE). The AQE queries an Active Directory global catalog server each time it processes a message.

Another process is the DSProxy process, which handles querying the Active Directory for address list information that is queried by older MAPI clients (Outlook 97 and 98). This service essentially emulates the MAPI functions that the Exchange 5.x directory service handled. For Outlook 2000 and later MAPI clients, the system attendant runs a process called the Name Service Provider Interface (NSPI) or the DS Referral interface that refers the client to a global catalog server.

A third process is the Directory Service to Metabase (DS2MB) process, which is responsible for querying the Internet protocol configuration data located in the Active Directory and updating the IIS Metabase with any updated configuration information. The system attendant also runs a process called the Recipient Update Service (RUS). This process is responsible for updating Exchange properties on objects (servers, public folders, user accounts, groups, contacts) found in the Active Directory. This information includes e-mail addresses and address list membership.



REALITY CHECK

One of the more common problems with Exchange occurs when an administrator attempts to tighten security on Active Directory objects. The administrator blocks inheritance on an OU or removes the Domain Local group Exchange Enterprise Servers from the Security list. This prevents the Recipient Update Service from accessing certain objects in the Active Directory and making the necessary updates.

The crown jewel of Exchange 2003 is now the Information Store. The Information Store service provides access to the mailbox and public folder stores for all types of clients. MAPI clients access the Information Store directly, whereas standard Internet clients (POP3, IMAP4, NNTP) access the store through Internet Information Service (IIS). The Information Store service uses the Extensible Storage Engine (ESE98) database engine to handle database file access and management of transaction logs.

Exchange 2003 includes a kernel-mode device driver called the Exchange Installable File System (ExIFS) driver. This allows properly authorized users to access messages and files in their mailbox as well as public folders via the file system. You might remember that Exchange 2000 servers exposed the Information Store databases via a drive letter (the M: drive), but this must be enabled via a Registry key in Exchange 2003 servers.

A shared memory component called the Exchange Inter-Process Communication (ExIPC) layer provides high-speed communication and queuing between the Information Store and components such as SMTP, HTTP, and POP3 that operate under the Inetinfo process. The developers called the ExIPC process DLL EPOXY because it is the glue that holds the information store and IIS together.

An additional component of the Information Store is called the Exchange Object Linking and Embedding Database layer (ExOLEDB). This component is a server-side component that allows developers to use Active Data Objects (ADO) or Collaborative Data Objects (CDO) to access public folder and mailbox data programmatically through OLE DB. By default, ExOLEDB is only accessible locally by programs running on a specific Exchange server; however, the functionality could be wrapped in to a Component Object Model (COM) component and used remotely by ASP pages or other Web applications.

Exchange still provides an X.400 compliant message transfer agent (MTA), but this component is only used if the server is communicating

with X.400 messaging services or if the Exchange server is communicating with non-Exchange 2003 servers.

Note: If you are interested in further reading about the Exchange 2003 architecture, consult Chapter 26 of the Exchange 2000 Resource Kit from Microsoft Press.

Applying Best Security Practices

The most secure Exchange organizations are the ones in which the administrators have evaluated as many of the possible threats as they can possibly determine and developed a series of best practices to mitigate the likelihood of these threats happening. A number of these best practices are put in place to make sure that the server continues to operate reliably and that the administrator can quickly detect compromises or potential problems.



BY THE BOOK...

E-mail is a mission-critical service for almost all organizations today. Therefore, it's crucial that you provide your organization with the most secure and, at least as important, reliable Exchange 2003 messaging system as possible. In short, you have to build the most secure foundation possible. Failing to do so will have severe consequences.

Here is a list of daily practices that we recommend implementing for all Exchange organizations:

- Review the System, Application, and Security event logs for any events that indicate operation outside normal specifications.
- Perform and verify daily full backups; keep at least two weeks' worth of daily tapes and weekly tapes for at least a month.
- Check and record available disk space; confirm that the disk space has not grown unusually since the last time available disk space was recorded.
- Examine the outbound SMTP and X.400 queue lengths for unusual queue growth or SMTP domain destinations.
- Update the antivirus software daily. The scanning engine and signatures should be as up to date as possible.

Few tasks need to be performed weekly or monthly on an Exchange server, but there are a few things that really do not need to be done daily. Exchange 2003 rarely (if ever) needs offline maintenance of the databases or reboots. Here is a list of tasks that you should perform somewhere between once a week and once a month:

- Check with Microsoft for the latest service packs and security fixes for the Windows operating system, Internet Information Server (IIS), and Exchange Server. Wait at least a month after the release of a service pack before applying the new service pack. Examine each fix with a critical eye toward whether or not it is fixing something you need fixed. For example, Windows Media Player updates are not necessary on an Exchange server. Fixes to the Network News Transport Protocol (NNTP) are not necessary if you are not using NNTP. There is no need to schedule downtime to apply a fix that is not necessary.
- Examine the SMTP BADMAIL directory for unusual accumulations of messages. This directory holds e-mail that was either malformed (client problems) or failed relay attempts. This directory should be purged periodically. You should attempt to get to the bottom of the problem.
- Purge or archive any protocol logs that you are keeping (such as SMTP or HTTP). If you are keeping long-term records, import these into your log analysis tools.
- Archive message-tracking logs if you keep these logs. Otherwise they will be purged.

Other security practices are more configuration-related than procedural. These configuration steps can help you when you need to help steer your users away from causing you problems. These include storage limits, maximum message size limits, autoresponse limitations, and maximum recipients per message.

Defining Acceptable Use

Many organizations are now publishing acceptable-use policies for their employees. An acceptable-use policy document defines the e-mail system's functionality, user limitations, and the expectations of the user. Although the policy is not directly related to security, setting users' expectations as to how they are expected to treat an organization's messaging system can help reduce problems and accidental security breaches.

A well-written, legally defensible acceptable-use policy can also help reduce an organization's liability when it comes to inappropriate material that employees send to one another. A good acceptable-use policy should include expectations and definitions such as these:

- E-mail system usage and whether or not personal use of the e-mail system is permitted.
- Define data types that must not be transmitted in e-mail messages, if applicable. For example, a military network might prohibit classified information from being sent over an unclassified e-mail network. A hospital might prohibit messages containing patient information from being sent without being encrypted.
- Define message types that are unacceptable, such as copyrighted material, MP3 files, off-color humor, sexual harassment, threatening remarks, or explicit pictures.
- E-mail system restrictions such as message size, maximum recipients, and mailbox storage limits.
- Whether or not mailboxes are subject to management inspection and under what circumstances management or human resources will request mailbox data be viewed.
- Define exactly what will happen if users violate the acceptable-use policy. Be realistic and define a punishment that fits the crime.

The SANS Institute publishes many sample policies. These can be found at www.sans.org/resources/policies.

Practice Safe Computing

Here are a couple of tips and suggestions for keeping your Exchange servers safe and more secure:

- Never configure or install e-mail clients (Outlook or Outlook Express) on the console of the Exchange server.
- Avoid “surfing the Web” from the Exchange server console. The console of the Exchange server should be hallowed ground.
- Dedicate Exchange servers to running Exchange. Avoid putting unnecessary services or software on an Exchange server. Shared folders on an Exchange server should be accessible to only the Exchange administrators. This includes directories such as the message-tracking log directory.

- In an organization with multiple Exchange servers, create dedicated Exchange server roles (mailbox, public folder, bridge-head/communications gateway, OWA front end.) These servers are easier to rebuild in the event of a disaster and security can be tightened more due to the fact that they have limited roles.
- Whenever possible, use a different SMTP alias and address from the Active Directory UPN name or the Active Directory account name. Even if you are using strong passwords, why give a potential intruder half of the hacking equation?
- Never configure NTFS compression on any Exchange data, log, or binaries directory.

Good Physical Security

Rule number three of The Ten Immutable Laws of Security (www.microsoft.com/technet/columns/security/essays/10imlaws.asp) states: "If a bad guy has unrestricted physical access to your computer, it is not your computer anymore." This is not only true, it is fairly obvious. Yet we walk into many organizations where the servers are in a copy room or on a spare desk. They are usually in a location that anyone could walk to and do whatever they wanted to the server. There are a few points regarding physical security that should always be kept in mind:

- All servers, routers, and networking equipment must be in a physically secure and environmentally stable location.
- Backup device (tapes, CD-RWs, and DVD±RW/Rs) usage should be restricted both by policy and physical access.
- Backup media (optical and tape) must be stored in a physical location. Often we see good physical security on servers and tape media in the hallway on a shelf outside the computer room door.

Installing Exchange 2003 Best Practices

One of the most important parts of running an Exchange organization is ensuring that your Exchange servers are operating in a consistent and predictable fashion. This means knowing the exact configuration of each Exchange server and knowing how to rebuild the server in the event of a

disaster. Designing a secure and stable platform for your servers is the first step toward this goal. Following a checklist will help you achieve this goal; too many times steps are missed, skipped, or overlooked when servers are installed. Once the servers are installed, make sure that you have a consistent configuration by using Active Directory Group Policies to apply as many configuration items as possible.



BY THE BOOK...

A growing number of organizations regard messaging systems as some of the most mission-critical systems in the whole organization. For this reason, companies place strict reliability and availability requirements on their e-mail systems. Therefore, you as an Exchange admin must install the Exchange 2003 messaging system in as sufficient a way as possible.

Installation Checklist

The following sections comprise a basic checklist of things that we do for every Exchange server installation. This list can be updated depending on customer needs.

Building the Hardware Platform

Often administrators overlook the importance of hardware in their installation process. Sure, we all know we need good hardware, but the hardware might not be ready right out of the box to install an operating system and applications. There are a few things you can do to make sure that the server hardware platform is going to be stable and secure. In preparing for an Exchange installation, a single-vendor hardware platform is best. Determine exactly which components are going to operate best, right down to the hardware firmware level. Keep in mind the following points:

- Confirm that the Flash upgradeable BIOS on the motherboards, disk controllers, disks, and other peripherals is updated to a reasonably recent release. If using storage area network (SAN) or network-attached storage (NAS) devices, make sure that the entire disk subsystem is updated to a vendor-approved level. The latest version is not always the best version.
- The server should be in a secure location.

- Physically connect the server and monitor to a UPS that will hold the server up for at least 15 minutes in the event of a power failure.
- Confirm that you have recent versions of device drivers and supporting software for your particular hardware platform. Again, the latest version is not always the best version. Consult with a knowledgeable representative from your vendor.
- Configure disk fault tolerance. When configuring disk drives, make sure that you allow separate physical hard disks for each storage group's transaction logs.
- Secure, tie-wrap, or put in to cable guides the network, disk, power, and external device cables.
- Document the server's hardware and disk drive configurations.

Installing the Operating System

The next step is to install the Windows operating system. Even though Exchange 2003 will run on top of Windows 2000, we strongly recommend installing it on Windows 2003. The Windows 2003 platform is more stable and more secure. Keep in mind the following:

- Install Windows 2003 and update the operating system with updates and service packs that affect all operating system components, IIS, and Internet Explorer.
- Set the size of the page file to RAM times two.
- Format all disks using NTFS.
- Confirm that all network adapters are operating at maximum speed (i.e., 100MB/s full duplex).
- Configure UPS monitoring software.
- If applicable, install file-based antivirus scanning software and make sure that the Exchange directories are excluded.
- Move the server into an Active Directory Organizational Unit that has the correct Exchange server GPO applied to it.

Installing Exchange 2003

This checklist assumes that all the necessary preparation steps have been done, such as the forest prep and domain prep process. Keep in mind the following:

- Install Exchange 2003 and apply any necessary service packs or fixes.
- Enable message tracking.
- Statically map the information store and system attendant MAPI TCP ports.
- Configure default limits for the mailbox and public folder stores.
- Move the transaction logs and stores to the correct disk drives.
- If this server is to be used for direct connectivity from Internet clients (OWA, POP3, IMAP4, NNTP), install certificates for each of these services.
- If this server is hosting direct connectivity from Internet clients (such as if this is a front-end server), enable protocol logging.
- Disable unnecessary services.
- Install the backup software or the backup agent.
- Install the Exchange aware antivirus software (software that is AVAPI 2.5 compliant); confirm that it is up to date and that it has the latest scanning engine.
- Configure the antivirus software with your “forbidden attachment” list.
- Document any custom settings that were made to this server.
- Disable NetBIOS over TCP/IP if NetBIOS is not required in your organization.

Your A** Is Covered If You...

- Take security seriously in your organization!
- Use MBSA and Hfnetchk.
- Have a basic understanding of the Exchange 2003 Windows dependencies.
- Apply security best practices by following at least some of the information provided in this chapter.
- Make sure Exchange servers are installed and thereafter operated in a consistent and predictable fashion.

Chapter 3

Delegating and

Controlling Permissions

in Exchange 2003

In this Chapter

Even though Exchange Server 2003 has been developed under Microsoft's Trustworthy Computing Initiative, meaning that the product is secure by design and secure by default, you still need to manage, delegate, and control different types of Exchange-related permissions throughout your organization. Since Exchange 2003 builds on the Windows 2000/2003 security model, this concept shouldn't be too foreign to you.

In this chapter, we look at the following topics:

- Delegating administrative control in System Manager
- Controlling mailbox permissions
- Controlling Public Folder permissions

By the time you reach the end of this chapter, you will have been introduced to some of the general Exchange 2003 permissions, and you will have seen how to delegate control to groups or users via the Exchange Administration Delegation Wizard. You will also have learned how you assign Exchange (or more specifically, MAPI) permissions when dealing with mailboxes and Public Folders.

Delegating Administrative Control in System Manager

You can use the Exchange Administration Delegation Wizard to assign various administrative permissions to different Windows 2000/2003 groups or users.



BY THE BOOK...

The Exchange Administration Delegation Wizard simplifies the process of delegating permissions to Exchange administrators. You can delegate administrative permissions at the organization level in System Manager or at an administrative group level. The scope of permissions you set is determined by the location from which you launch the wizard. If you start the wizard from the organization level, the groups or users that you specify will have administrative permissions at the organizational level. If you launch the wizard from the administrative group level, the groups or users that you specify will have administrative permissions at the administrative group level.

Before we show how you, with the help of the Exchange Administration Delegation Wizard, can delegate administrative control to Windows groups or users within the Exchange System Manager, we think it's a good idea to provide you with some general Exchange 2003 permissions information.

Exchange Server 2003 Permissions

Exchange Server 2003 includes several permissions that can be applied to various objects within the Exchange System Manager to make it possible to restrict administrative access. The permissions for these Exchange 2003 objects are applied to Windows 2000/2003 users and/or groups. When you install Exchange 2003 into your Active Directory domain or forest, several groups are granted access to Exchange 2003. Two of these groups—Exchange Domain Servers and Exchange Enterprise Servers—are created during the initial Exchange installation; the others are pre-existing Windows 2003 security groups.

Here is a list of the relevant groups:

- **Domain Admins** This group's members are all Administrators. They can manage user accounts, contacts, groups, mailboxes, computers, messaging features, delivery restrictions, and storage limits. By default, this group is a member of the Administrators group on the Exchange 2000 Server, and its only member is the local user, Administrator.
- **Enterprise Admins** This group's members are administrators of the enterprise. The group is used to administer any domain of the enterprise. Members of this group have full control over Exchange 2000 Server, meaning that they aren't restricted in any way. By default, this group is also a member of the Administrators group, and its only member is the local user, Administrator.
- **Exchange Domain Servers** This group can manage mail interchange and queues. All computers running Exchange Server 2003 are members of this group. This group is a member of the domain local group, Exchange Enterprise Servers.
- **Exchange Enterprise Servers** This group is a domain local group. By default, this group has Exchange Domain Servers as its only member.
- **Everyone** This group's members are all interactive, network, dialup, and authenticated users. By default, all members of this group could create top-level Public Folders, subfolders within Public Folders, and named properties in the Information Store. This has been adjusted in Exchange 2003 so that only Domain Admins, Enterprise Admins, and the Exchange Domain Server have this permission.

Exchange 2003 permissions control access to resources and provide specific authorization to perform an action. Exchange 2003 permissions are based on the Windows 2000/2003 permission model, meaning that permissions on an object and on the object's child objects can be assigned to a user and/or a group. As you might already know, when an object is created in Windows 2000/2003, the object inherits permissions from its parent object. This is called *inheritance* and can be overridden either by assigning permissions directly to the object or by specifying that the object should not inherit permissions.

Note: A discussion of the specific options for setting inheritance in Windows 2000/2003 is out of the scope of this book. For more information on inheritance and Windows security in general, we suggest you check the Windows 2003 Help files.

In addition to all the standard Windows 2000/2003 Active Directory permissions, which can be set on objects, there are a number of Exchange 2003 specific permissions as well. They are listed in Table 3.1.

Table 3.1 Exchange 2003 Specific Permissions

Permissions	Description
Administer Information Store	Allowed to administer Information Store
Create named properties in Information Store	Allowed to create named properties in Information Store
View Information Store status	Allowed to view the status of the Information Store
Open mail send queue	Allowed to open the Mail Send queue and message queuing
Read metabase properties	Allowed to read the properties of the metabase
Create top-level Public Folder	Allowed to create top-level Public Folder
Create Public Folder	Allowed to create Public Folder under top-level folder
Mail-enable Public Folder	Allowed to mail-enable a Public Folder
Modify Public Folder ACL	Allowed to modify access control list (ACL) on a Public Folder
Modify Public Folder admin ACL	Allowed to modify the admin ACL on a Public Folder
Modify Public Folder deleted item retention	Allowed to modify the deleted item retention
Modify Public Folder expiry	Allowed to modify a Public Folder expiration date
Modify Public Folder quotas	Allowed to modify quota of a Public Folder
Modify Public Folder replica list	Allowed to modify the replication list for a Public Folder

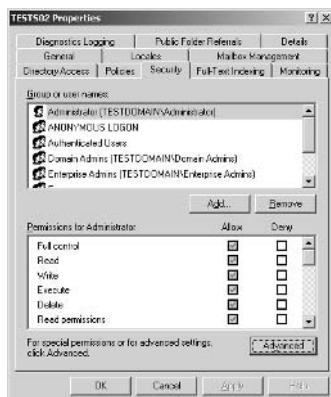
We can further examine the permissions listed in Table 3.1 by clicking **Properties**, then clicking the **Security** tab of the respective node (such as **Server** or **Public Folder**) in the Exchange System Manager.

Viewing Exchange Server Permissions in Exchange System Manager

You can view or edit permissions of a root or leaf node in the Exchange System Manager the following way:

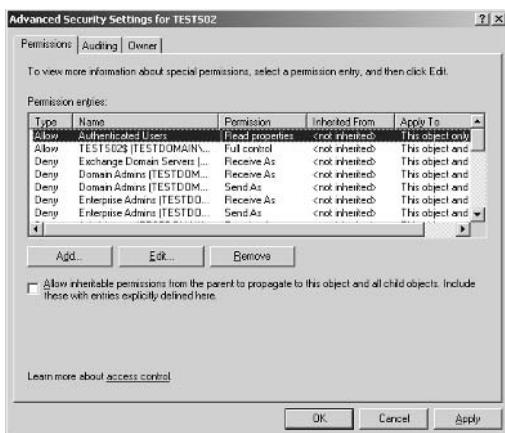
1. On the Exchange 2003 Server, open the **Exchange System Manager**.
2. Right-click the **Node** (for example, the server node itself, which can be found directly under Servers), then select **Properties**.
3. Click the **Security** tab (see Figure 3.1).

Figure 3.1 The Security Tab of a Leaf Node in the Exchange System Manager



Note that in Figure 3.1, the check marks under the **Allow** column are grayed out. This is because this leaf node inherits its permissions.

4. To disable this behavior, click the **Advanced** button, and then deselect **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** (see Figure 3.2).

Figure 3.2 Deselect Inheritance from Parent Object

5. A Security Message information box will appear (see Figure 3.3). Click **Copy**.

Figure 3.3 Security Message Information Box

Note: You should typically click **Copy** because all inherited permissions will be removed if you click **Remove**. Afterward, you can remove any groups or users manually.

Using the Exchange Administration Delegation Wizard

The Exchange 2003 Administrative Delegation Wizard, accessible through the Exchange System Manager, simplifies assigning permissions to Exchange objects. Instead of assigning permissions to individual administrators, it's a good idea to create groups of administrators, then use the delegation wizard to assign a set of administrative permissions to each group. Creating security groups and then adding specific users to them greatly simplifies the administrative burden of managing administrative permissions throughout the organization.

With the Exchange 2003 Administration Delegation Wizard, you can assign the following three types of permissions to either users or groups: Exchange Full Administrator, Exchange Administrator, and Exchange View Administrator.

Exchange Full Administrator

Users or groups given this role can fully administer all Exchange system information and modify permissions. In detail, an Exchange Full Administrator is granted the following permissions:

- **Organization permissions**
 - Full Control permissions on the MsExchConfiguration container (this object and its subcontainers)
 - Deny Receive-As permissions and Send-As permissions on the Organization container (this object and its subcontainers)
 - Read permissions and Change permissions on the Deleted Objects container in the Configuration naming context, or Config NC (this object and its subcontainers)
- **Administrative Group permissions**
 - Read, List object, and List contents permissions on the MsExchConfiguration container (this object only)
 - Read, List object, and List contents permissions on the Organization container (this object and its subcontainers)
 - Full Control, Deny Send-As, and Deny Receive-As permissions on the Administrator Groups container (this object and its subcontainers)
 - Full Control permissions (except for Change) on the Connections container (this object and its subcontainers)
 - Read, List object, List contents, and Write properties permissions on the Offline Address Lists container (this object and its subcontainers)

Exchange Administrator

Users or groups given this role can fully administer all Exchange system information. In detail, an Exchange Administrator is granted the following permissions:

- **Organization permissions**
 - All permissions (except for Change permissions) on the MsExchConfiguration container (this object and its sub-containers)
 - Deny Receive-As permissions and Send-As permissions on the Organization container (this object and its subcontainers)
- **Administrative Group permissions**
 - Read, List object, and List contents permissions on the MsExchConfiguration container (this object only)
 - Read, List object, and List contents permissions on the Organization container (this object and its subcontainers); all permissions (except for Change, Deny Send-As, and Deny Receive-As permissions) on the Administrator Group container (this object and its subcontainers)
 - All permissions (except for Change permissions) on the Connections container (this object and its subcontainers); Read, List object, List contents, and Write properties permissions on the Offline Address Lists container (this object and its subcontainers)

Exchange View Administrator

Users or groups given this role can view Exchange configuration information. In detail, an Exchange View Administrator is granted the following permissions:

- **Organization permissions**
 - Read, List object, and List contents permissions on the MsExchConfiguration container (this object and its sub-containers)
 - View Information Store Status permissions on the Organization container (this object and its sub-containers).

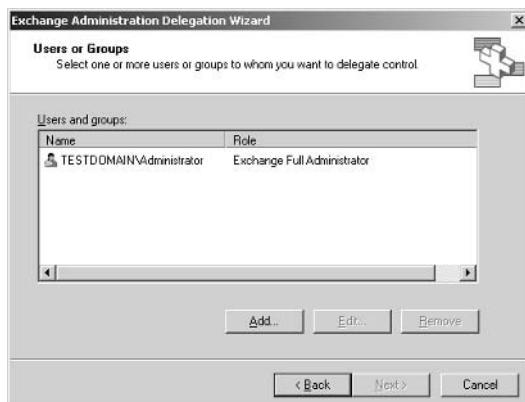
■ Administrative Group permissions

- Read, List object, and List contents permissions on the MsExchConfiguration container (this object only)
- Read, List object, and List contents permissions on the Organization container (this object only)
- Read, List object, and List contents permissions on the Administrator Groups container (this object only)
- Read, List object, List contents, and View Information Store Status permissions on the Administrator Groups container (this object and its subcontainers)
- Read, List object, and List contents permissions on the MsExchRecipientsPolicy container, the Address Lists container, Addressing, Global Settings, System Policies (this object and its subcontainers)

The Exchange 2003 Administration Delegation Wizard can be used at the organization level or any administrative group level. Setting permissions using the Exchange 2003 Administration Delegation Wizard is done by following these steps:

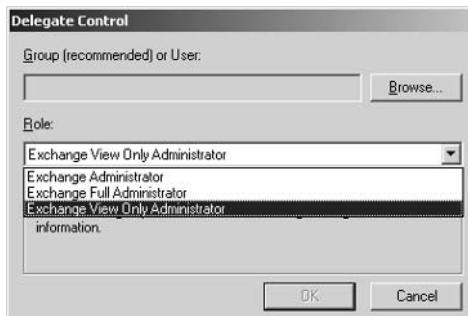
1. On the Exchange server, open the **Exchange System Manager**.
2. Right-click either the organization (globe with envelope) or an administrative group, then select **Delegate Control**.
3. Click **Next**. You'll be presented with the screen shown in Figure 3.4.

Figure 3.4 Selecting One or More Users or Groups That Should Be Delegated Control



4. Click **Add**, and select the type of role to be delegated (see Figure 3.5).

Figure 3.5 Selecting Exchange Administrator Role



5. Click **Browse** (refer back to Figure 3.5), and then specify any users or groups who should be delegated the selected role.
6. Click **OK**, then click **Next | Finish**.

Invoked Delegation Wizard Permissions

When the delegation wizard is invoked at the organizational level, the permissions shown in Table 3.2 are applied.

Table 3.2 Permissions Invoked at the Organizational Level

Role	Objects	Permissions
Exchange Full Administrator	Organization Object	All permissions except Send As and Receive As
Exchange Full Administrator	Administrative Group	All permissions except Send As and Receive As
Exchange Administrator	Organization Object	All permissions except Send As, Receive As, Change Permissions, and Take Ownership
Exchange Administrator	Administrative Group	All permissions except Send As, Receive As, Change Permissions, and Take Ownership
Exchange View Only Administrator	Organization Object	Read, Execute, Read Permissions, List Contents, Read Properties, List Object, View Information Store Status permission

Table 3.2 Permissions Invoked at the Organizational Level

Role	Objects	Permissions
Exchange View Only Administrator	Administrative Group	Read, Execute, Read Permissions, List Contents, Read Properties, List Object, View Information Store Status permission

When the delegation wizard is invoked at the administrative group level, the permissions shown in Table 3.3 apply.

Table 3.3 Permissions Invoked at the Administrative Group Level

Role	Objects	Permissions
Exchange Full Administrator	Organization Object	Read, Execute, Read Permissions, List Contents, Read Properties, List Object
Exchange Full Administrator	Administrative Group	All permissions except Send As and Receive As
Exchange Administrator	Organization Object	Read, Execute, Read Permissions, List Contents, Read Properties, List Object
Exchange Administrator	Administrative Group	All permissions except Send As, Receive As, Change Permissions, and Take Ownership
Exchange View Only Administrator	Organization Object	Read, Execute, Read Permissions, List Contents, Read Properties, List Object
Exchange View Only Administrator	Administrative Group	Read, Execute, Read Permissions, List Contents, Read Properties, List Object, View Information Store Status permission

Controlling Mailbox Permissions

Outlook 2003 provides the capability to grant other users access to information in a user's mailbox. The mailbox can be shared by either granting permission to specific users or by giving one or more users access using the Outlook 2003 delegates feature. You can also grant mailbox permissions through Active Directory Users and Computers. All three methods are covered in this section.



BY THE BOOK...

In some situations, one or more users might need access to another person's mailbox. This could be more temporary access, where one person went on vacation and another needs to take care of that person's work. It could also be more permanent access, where a secretary has access to her boss's mailbox. It could also be help desk personnel who have a mailbox they share in the help desk department in addition to their own personal mailbox. This can be accomplished by granting other people permission to the mailbox. Granting rights to a mailbox can be done using two different methods: through Active Directory Users and Computers or directly through the Outlook client.

Delegating Mailbox Access Through Outlook 2003

Delegating other people access to a person's mailbox through Outlook 2003 must be done either by the mailbox owner, an Administrator or another user who already has been granted access to the user's mailbox.

Notes from the Underground...

Grant Administrators Access to All Mailboxes

As you might already know, the Administrator account, or any other user account member of either Domain Admins or Enterprise Admins, is explicitly denied access to all mailboxes other than its own in Exchange 2000/2003. This is even the case if you have full administrative rights over the Exchange System.

Continued

Unlike Exchange 5.5, all Exchange 2000/2003 administrative tasks can be performed without having to grant an administrator sufficient rights to read other people's mail. This default restriction can be overridden in several ways, but again, doing so should be in accordance with your organization's security and privacy policies. In most cases, using these methods is appropriate only in a recovery server environment.

For specific details on granting administrators access to all mailboxes, see Microsoft KB article 821897, "How to Assign Service Account Access to All Mailboxes in Exchange Server 2003," at www.support.microsoft.com/?id=821897.

In the following steps, we delegate access to a mailbox through Outlook:

1. Log on to your client machine, then open **Outlook**.
2. In the menu, select **Tools | Options**, then click the **Delegates** tab. You'll be presented with the screen shown in Figure 3.6.

Figure 3.6 The Delegates Tab Under Options in Outlook



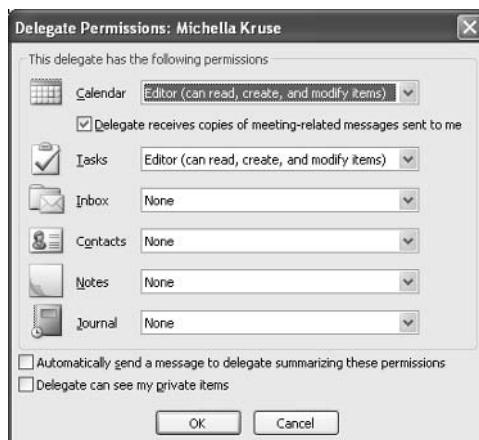
3. Click the **Add** button. This is where we select the users we want to grant permissions to our mailbox (see Figure 3.7).

Figure 3.7 Selecting Users Who Are to Be Granted Access to Our Mailbox



4. Select a user by double-clicking on his or her name, then click OK. The screen in Figure 3.8 will appear. This is where we specify the type of permissions the users should be granted to each object.

Figure 3.8 Specifying the Type of Permissions to Grant the User



As you can see, adding a user, by default, gives that user the Editor role to the Calendar and Tasks, as well as enables the option **Delegate receives copies of meeting-related messages sent to me**. But as you can see, we can also grant permissions to the user's Inbox, Contacts, Notes, and Journal. We can assign one of four different roles to each; we have listed the roles in Table 3.4.

Table 3.4 Four Different Permission Roles

Role	Permissions Granted
None	No permissions
Reviewer	Read permissions
Author	Read and create permissions
Editor	Read, create, and modify permissions

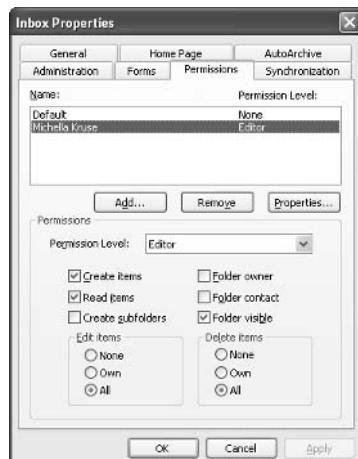
- Because we want to assign full mailbox control, we assign the **Editor** role to all items, then click **OK** twice.

Granting Mailbox Permissions to Folders Without Using Delegation

You can also grant permission to individual mailbox items simply by choosing the properties of each item in Outlook, then selecting the Permissions tab. This works much the way you grant permissions to a Public Folder through Outlook, which we do in the next section of this chapter. Here we perform the following steps:

- In Outlook, right-click the **Inbox**, then select **Properties**.
- Click the **Permissions** tab. You'll see the screen shown in Figure 3.9.

Figure 3.9 Granting Access to Individual Folders Through the Permissions Tab in Outlook



As you can see, it's possible to assign either individual permissions or grant permission level roles to the users you select by clicking the Add button. We describe each permission option in the next section of the chapter, where we discuss controlling Public Folder permissions.

Note: The observant reader will notice the users we granted editor permissions using the delegates option are shown in Figure 3.9.

- When you have granted the respective permissions, click **OK** twice and close Outlook.

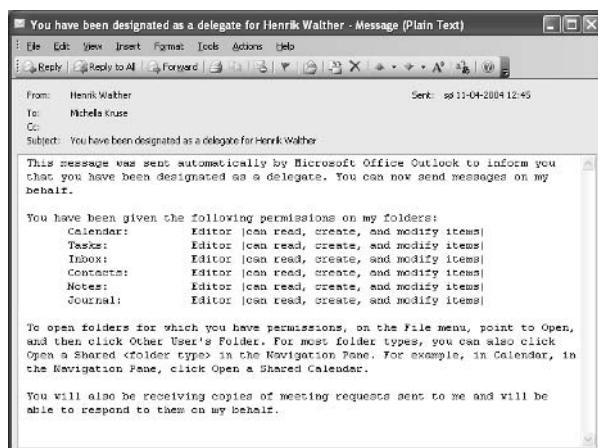
Opening the Additional Mailbox

Now that we have granted another user permissions to access and manipulate our mailbox, let's see how the user actually accesses it.

- Log on to a client machine (as the other user), then open **Outlook**.

Because we enabled the **Automatically send a message to delegate summarizing these permissions** option (refer back to Figure 3.8), there should be at least one unread mail in the user's inbox, and it should look something like the one shown in Figure 3.10.

Figure 3.10 Message to Delegate Summarizing These Permissions



As you can see, this message informs the user of the permissions he or she has been granted, and we even have instructions on how to open the folders to which the user has been granted permissions. Is that easy or what?

2. As the instructions in the mail inform you, click **File** in the menu, then select **Open | Other User's Folder**.
3. Type the user's name or click **Name** and browse your way to it (see Figure 3.11).

Figure 3.11 Open Other User's Folder in Outlook 2003

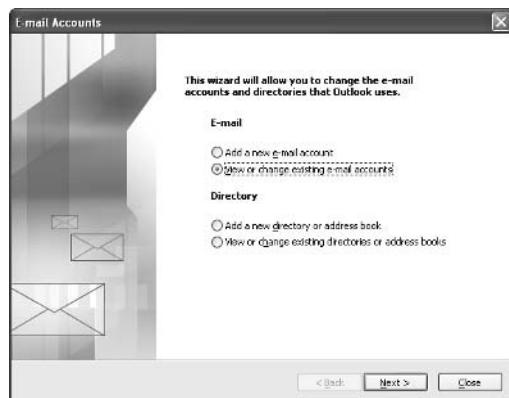


4. Select the type of folder you want to open in the drop-down text box **Folder type**, then click **OK**.

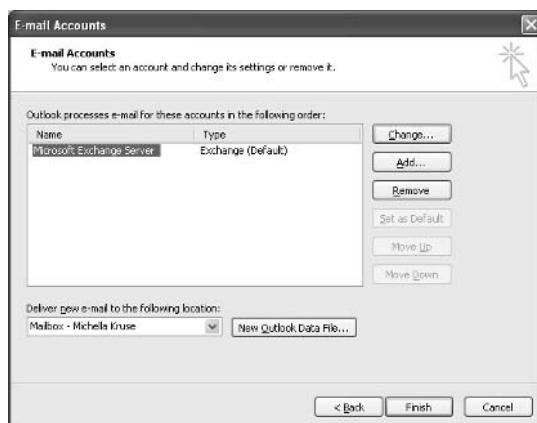
Note: For most folder types, you can also click **Open a Shared <folder type>** in the Navigation Pane. For example, in Calendar, in the Navigation Pane, click **Open a Shared Calendar**.

But what if you want to have access to all items (Inbox, Calendar, etc.) on a more permanent basis? Then you instead need to do the following:

1. In Outlook, click **Tools** in the menu, then click **E-mail accounts**.
2. Enable **View or Change existing e-mail accounts** (see Figure 3.12), then click **Next**.

Figure 3.12 Select View or Change Existing Mail Accounts

3. Click **Change** (see Figure 3.13), then click **More Settings**.

Figure 3.13 Changing Mailbox Account Settings

4. Select the **Advanced** tab, then click **Add** (see Figure 3.14).

Figure 3.14 The Advanced Tab of Mailbox

5. Type the name or alias of the mailbox owner, then click **OK** | **Next** | **Finish**.

The user's mailbox can now be found in the Outlook folder list in the left pane.

Note: If you get an “unable to expand folder” error message on the added mailbox, you might have to set permissions on the mailbox item itself. You do that exactly the same way you set individual permissions on the mailbox items: Choose the properties of the mailbox, then select permissions and set the appropriate permissions.

Granting Mailbox Permissions Through Active Directory

Besides the two ways of delegating or providing access to mailboxes through the Outlook client, it's also possible to configure mailbox rights in Active Directory Users and Computers. So let's switch back to the server side again. More specifically, log on to the Exchange 2003 server and do the following:

1. Click **Start** | **Administrative Tools** | **Active Directory Users and Computers**.

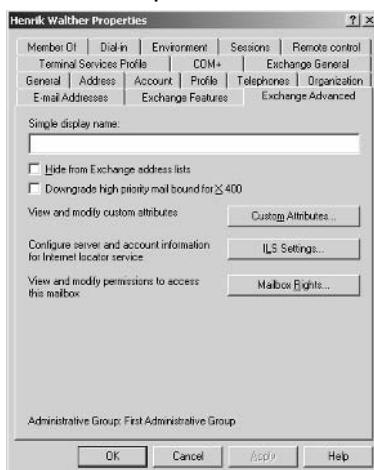


REALITY CHECK...

You might wonder why we have to log on to the Exchange Server and not a domain controller, when we're going to access Active Directory Users and Computers. That's because by default you can't administer the Exchange-related tasks of your Active Directory user accounts from a domain controller. But you can administer Exchange-related tasks of your AD user accounts from a domain controller without problems. We hear some of you grumble—yes, that is possible, but to do that you first need to insert the Exchange 2003 CD into your domain controller and then install the System Manager tools from it.

2. Double-click a user account, then select the **Exchange Advanced** tab (see Figure 3.15).

Figure 3.15 The Exchange Advanced Tab of a User Account in Active Directory Users and Computers

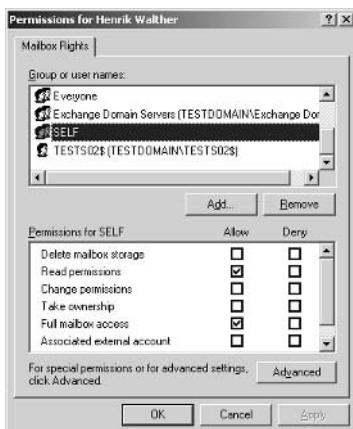


3. Click the **Mailbox Rights** button.

Here we can grant access rights to the whole mailbox instead of separate mailbox items (such as Inbox, Calendar, and Tasks). As shown in Figure 3.16, you can, under Mailbox Rights, grant and deny mailbox permissions for a mailbox-enabled user. You can also view and change mailbox permissions for a mailbox-enabled user, assign mailbox permissions to

another user or group, and change inherited permissions. The mailbox owner is granted Read permissions and Full mailbox access through the special SELF account.

Figure 3.16 Mailbox Rights on a User in Active Directory Users and Computers



Controlling Public Folder Permissions

The primary purpose of Public Folders is to have a shared or centralized place to post e-mail messages and other files (Freedocs) within an organization. When you create a Public Folder, it will be placed under the Public Folder Store on an Exchange 2003 server. The Public Folder Store on a given Exchange server can replicate its Public Folders to Public Folder Stores located on other Exchange servers in the organization. It's possible to create multiple Public Folder Stores (only in Enterprise Edition). You can create additional Public Folder trees, which can contain their own set of Public Folder hierarchies. Because this book is about Exchange security, we won't go into detail on how to administer and manage Public Folders, Public Folder Stores, and Public Folder Trees, but instead we'll dive into how you configure permissions in regard to Public Folder Stores and Public Folders.



BY THE BOOK...

If an organization is split into many departments, some Public Folders might need to be accessible by everyone, some accessible only to Authenticated users, and some might need to be tightened down, strictly to be accessible by users in a specific department. This is exactly where Public Folder permissions come into the picture. By setting specific permission on a Public Folder, you can control what one or more users can do to it—more specifically, give users read, write, and/or modify permissions to the given Public Folder. These permissions can be set either through the Exchange System Manager or from an Outlook MAPI client.

In the following section we show you how to create a Public Folder and discuss the methods available for setting permissions on the Public Folder.

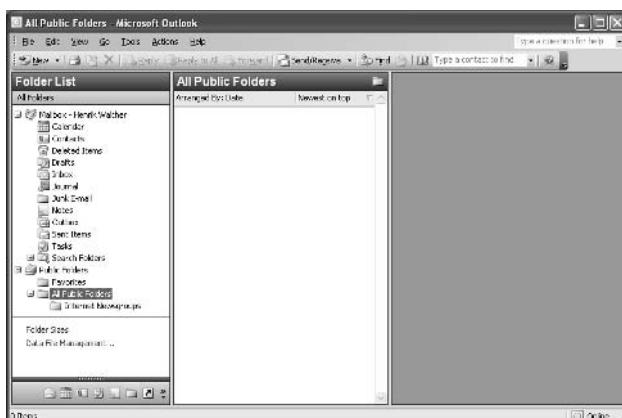
A Public Folder can be created either through the Exchange System Manager or from within a mail client such as an Outlook 2003 or OWA 2003.

Creating and Setting Permissions on Public Folders in Outlook 2003

Let's start by creating a Public Folder in Outlook. Open your Outlook 2003 client and follow these steps:

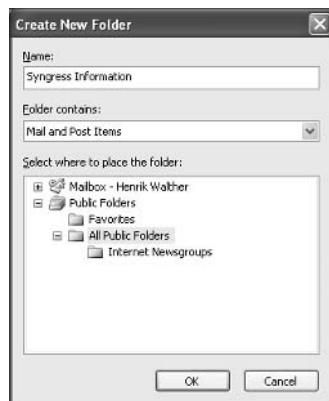
1. In the left pane, expand **Public Folders** (see Figure 3.17).

Figure 3.17 Expand the Public Folder Tree in Outlook 2003



2. Right-click **All Public Folders**, and select **New Folder**.
3. Give the folder a name, then select the type of Public Folder you want to create (see Figure 3.18). Click **OK**.

Figure 3.18 Creating a New Public Folder Through Outlook 2003



4. Right-click the new **Public Folder**, select **Properties**, and click the **Permissions** tab. You'll see a screen like the one shown in Figure 3.19.

Figure 3.19 The Permissions Tab of Public Folder in Outlook 2003



As you can see, users can be assigned different roles. Each role holds a set of specific permissions. The types of permission listed in Table 3.5.

Table 3.5 Public Folder Permissions Through Outlook 2003

Permission Option	Grant User Permission To
Create items	Post or create items in the Public Folder
Read items	Open (read) items in the Public Folder
Create subfolders	Create subfolder(s) within the Public Folder
Folder owner	Assign permissions (to others) and users get full permissions to the folder
Folder contact	Receive status messages such as NDRs
Folder visible	See the folder in the Public folder hierarchy
Edit items	None: Cannot edit items Own: Can edit items created by the user himself All: Can edit any item in folder
Delete items	None: Cannot delete items Own: Can delete items created by the user himself All: Can delete any item in the folder

Based on the type of permission level role a user is assigned, he or she is automatically granted a specific set of permissions. To see which are assigned under each Permission role, refer to Table 3.6.

Table 3.6 Permissions Included Under Each Permission Role

Permission role	Permissions Granted
Owner	Create, Read, Modify, Delete all items and files, Create subfolders, Change permissions
Publishing Editor	Create, Read, Modify, Delete all items and files, Create subfolders
Editor	Create, Read, Modify, Delete all items and files
Publishing Author	Create, Read items and files, Modify, Delete own items and files
Author	Create, Read items and files, Modify, Delete own items and files
Nonediting Author	Create, Read items and files, Delete own items and files
Reviewer	Read items and files
Contributor	Create items and files
None	No permissions

Notes from the Underground...

Always Use the Outlook Client or Exchange System Manager to Modify MAPI Permissions

You should always use only the Permissions dialog box provided by Outlook and the Client Permissions dialog box provided by Exchange System Manager to modify MAPI permissions. Said in another way, you should never edit permissions using the Windows file system user interface. The reason they are not interchangeable is that Windows Explorer uses the Windows 2000 ACL format to set security permissions on the MAPI Public Folder hierarchy, whereas Exchange System Manager and Outlook use the MAPI ACL format.

To read more about this issue, we suggest you check Microsoft KB article 270905, "XADM: Unable to Set Client Permissions on Public Folders Through Exchange System Manager," at www.support.microsoft.com/?kbid=270905.

Creating and Setting Permissions on Public Folders in System Manager

Now that you know how to create and assign user permissions to Public Folders using the Outlook 2003 client, we can move on to see how Public Folders are created and how you set permissions through the Exchange System Manager.



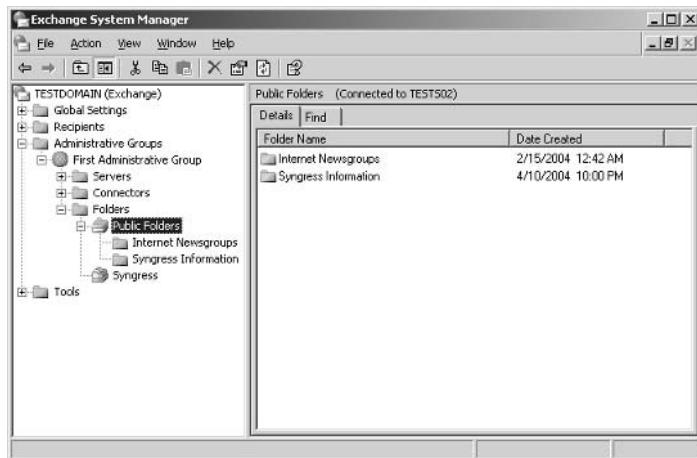
REALITY CHECK...

Before proceeding with the next set of steps, you should enable the Display Administrative Groups option. This makes it easier to administer Public Folders in the Exchange organization and is as well a requirement in creating new Public Folders through the Exchange System Manager. You enable this feature by opening the **Exchange System Manager**, then right-clicking the **Exchange organization** object (globe with envelope) and selecting **Properties**. Put a check mark in **Display Administrative Groups**, and then click **OK**. Though you're informed to exit and restart the Exchange System Manager, this is not necessary. If you want to see the changes immediately, just press **F5** or click **Refresh** in either the menu or the toolbar.

Now that the Administrative Groups container is visible, we can continue:

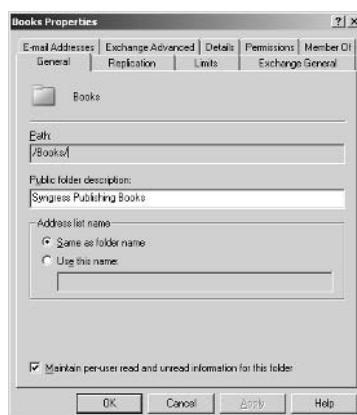
1. In the **Exchange System Manager**, expand, then select the **Public Folders** object (see Figure 3.20).

Figure 3.20 Navigating Down to Public Folders in Exchange System Manager



2. Right-click the **Public Folders** container, then select **New | Public Folder**.
3. Give the folder a name (and maybe a description), then click **OK**.
4. Right-click the new **Public Folder**, and select **Properties** (see Figure 3.21).

Figure 3.21 Public Folder Properties Through Exchange System Manager



- As you can see, there are several tabs to choose from, but since we're only interested in the security-related stuff, click the **Permissions** tab (see Figure 3.22).

Figure 3.22 The Public Folder Properties Permissions Tab Through Exchange System Manager



- Start by clicking the **Client permissions** button. You'll see a screen like the one in Figure 3.23.

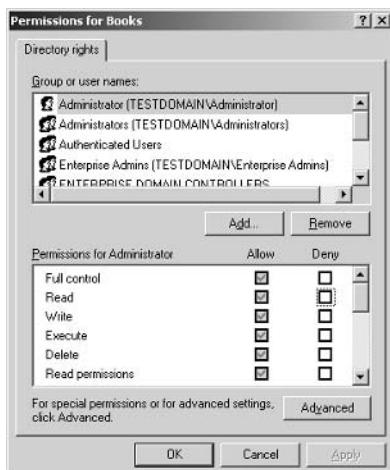
Does this screen look familiar? Compare it to Figure 3.19. We agree that there is no reason that we should go through these permissions and permission level roles again.

Figure 3.23 Setting User Permissions on Public Folders Through the Exchange System Manager



- Click **OK**, then click the **Directory rights** button. You'll see a screen like the one shown in Figure 3.24.

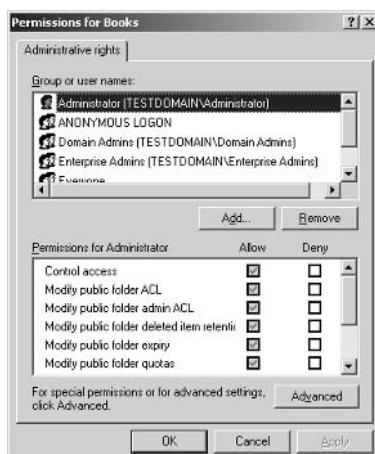
Figure 3.24 Directory Rights Under the Permissions Tab in Public Folder Properties



Here you grant or deny permissions to change mail-related attributes of a mail-enabled Public Folder. These attributes are stored in Active Directory just like most other Exchange permissions. Windows 2000/2003 users accounts can be granted or denied permission to read, write, or perform administrative tasks on the e-mail-related attributes.

- Click **OK**, then click the last button, **Administrative rights**. You'll see the screen shown in Figure 3.25.

Figure 3.25 Administrative Rights Under the Permissions Tab in Public Folder Properties



Here you can specify the users and/or groups that can use the Exchange System Manager to change the replication, limits, and other settings for the current Public Folder. When a user has been selected, you can either grant or deny administrative permissions.



REALITY CHECK...

You can also create new Public Folders through OWA 2003, but you cannot set specific permission-level roles or other permissions on the Public Folder. These will be created with the default permissions, which you then can change through either the Exchange System Manager or Outlook 2003.

Setting Permissions on Top-Level Public Folders in Exchange System Manager

Besides specifying different permission level roles and other permission-related options directly on each individual Public Folder, it's also possible to set permissions on a top-level Public Folder. This is done by choosing Properties of the top-level Public Folder, then clicking the Security tab. Setting permissions on the top-level folder means that all Public Folders below it will inherit the permission, which can be a good idea if you want one or more superusers or people on the help desk to administer all Public Folders beneath a top-level Public Folder.

Your A** Is Covered If You...

- Examine the default Exchange 2003 permissions.
- Know how to delegate permissions using the Exchange Administration Delegation Wizard.
- Know how to grant access to mailboxes using either Outlook or Active Directory Users and Computers.
- Know how to grant access to Public Folders using either Outlook or the Exchange System Manager.

Chapter 4

SMTP Security

In this Chapter

Even though Exchange 2003, out of the box, is the most secure version of Exchange released to date, we still need to keep an open eye on Exchange services such as the Simple Mail Transfer Protocol (SMTP), which is one the most compromised services in Exchange 2003. The primary reason is that SMTP servers are quite insecure because they are configured in such a way that communication with other SMTP servers is done using anonymous connections.

This chapter covers the following topics:

- Securing the SMTP service
- SMTP relaying
- E-mail address spoofing
- Internet mail headers

As you read this chapter, you will first be introduced to the SMTP basics, and then you will learn what SMTP relaying is all about and why it's vital to protect your SMTP server against relaying. We will also touch on topics such as e-mail address spoofing. Last but not least, you will be shown the information included in an Internet mail header.

Securing the SMTP Service

To understand the material in the rest of this chapter, it's mandatory that you know how SMTP servers communicate with each other. It's also vital that you have the proper knowledge of the various security-related options under an Exchange 2003 SMTP virtual server.



BY THE BOOK...

Simple Mail Transfer Protocol (SMTP) is the Internet standard for transporting and delivering electronic messages. SMTP is based on specifications in request for comment (RFC) 2821 and RFC 2822. Microsoft SMTP Service is included in the Windows 2000 and Windows 2003 operating systems.

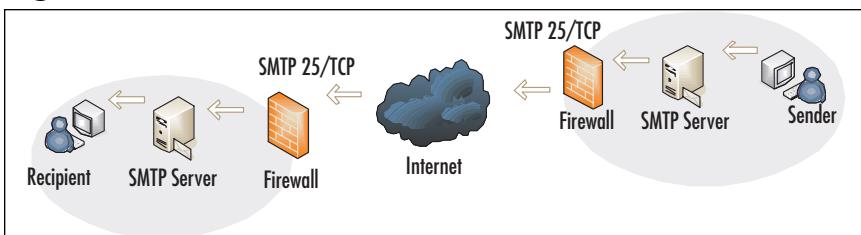
The Exchange 2003 Server expands Microsoft SMTP Service, enhancing the basic delivery functions of the protocol without compromising its compatibility with other messaging systems. Exchange gives administrators greater control over the routing and delivery of messages and provides secure access and channels for managing the service.

Because SMTP is a very popular choice to hack (through SMTP hijacking, DoS attacks, and so on) and given that by default it is quite insecure, it typically needs to be protected by restricting its settings on the Exchange server itself, but also by securing the messaging environment using perimeter networks, with additional servers acting as advanced firewalls, SMTP gateways, and the like.

SMTP Basics

When a mail-enabled user located on your Exchange 2003 server sends an e-mail message to a business contact in another company (in other words, a user located on another SMTP server belonging to another domain), the e-mail message is typically sent over the Internet using SMTP (port 25/TCP). Figure 4.1 describes this concept graphically.

Figure 4.1 SMTP Connection Between Two SMTP Servers

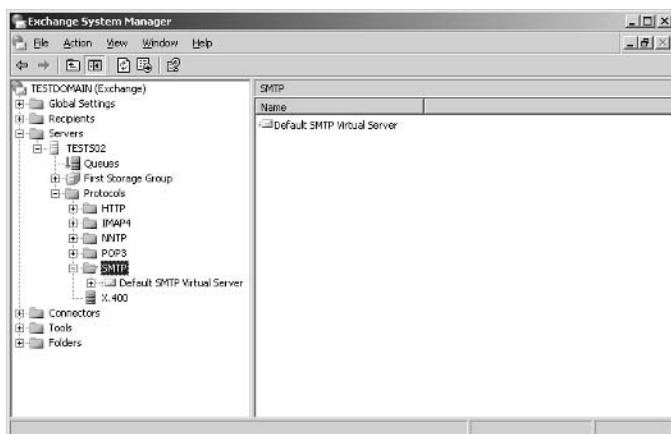


Note: Because Figure 4.1 is just a very basic example, we haven't included any perimeter networks (DMZs) containing additional SMTP servers.

By default, all SMTP servers can connect to each other via an *anonymous connection*. This means that any SMTP server on the Internet can connect to your Exchange 2003 server without needing to authenticate to it first (in other words, an account name or password is not required). To see where this specific setting is located, do the following:

1. Open **Exchange System Manager**.
2. Drill down to **Servers | Server | Protocols | SMTP** (see Figure 4.2).

Figure 4.2 Default SMTP Virtual Server in Exchange System Manager



3. Right-click **Default SMTP Virtual Server** and choose **Properties**.
4. Click the **Access** tab, then the **Authentication** button. You will be presented with the screen shown in Figure 4.3.

Figure 4.3 Default SMTP Virtual Server Authentication Settings

Even though anonymous access seems like quite a security risk, you would rarely change this setting. You might be tempted to make the SMTP connection more secure by removing the check mark in **Anonymous access** so that any SMTP server trying to establish a connection with your Exchange 2003 server would have to validate first. But it's important that you understand this wouldn't work, because all SMTP servers delivering e-mail messages to your server would need to configure a valid user account/password at their end, making the Exchange administration even more complex. Try to imagine configuring a valid username and password for each mail domain with which your users communicate via e-mail. It would be an absolute nightmare, so in the end, you will have to accept this "vulnerability." Luckily, there are several ways to limit it. One is to set restrictions on the Exchange Default Virtual SMTP Server itself. Another is to use a combination of firewalls, perimeter networks, SMTP gateways, and so on.



REALITY CHECK...

Typically, one SMTP virtual server would be sufficient, but if you're hosting multiple domains and would like to provide your users with more than one domain, you need to create additional SMTP virtual servers. Each will require its own unique IP address/TCP port combination. But you do have the possibility of setting up multiple aliases to one IP address. In addition, as long as the DNS server is configured properly, you could also "wild-card" the SMTP domain *.com, so the server will accept incoming

mail for all domains ending in .com, regardless of the IP address. If you have multiple SMTP virtual servers, remember that you need to set authentication settings on each.

SMTP Authentication Settings

Let's take a look at each of the authentication settings available under an Exchange 2003 SMTP virtual server (refer back to Figure 4.3):

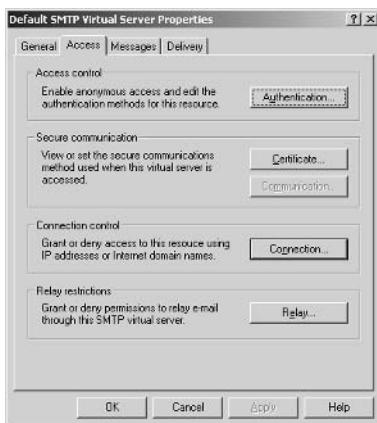
- **Anonymous access** As we mentioned, this setting allows users to connect to the SMTP virtual server without supplying a valid Windows 200x username and password. It's important to note that when this check box is selected, users will have the option to log on anonymously, even though other authentication methods have been configured.
- **Resolve anonymous e-mail** Though not an authentication setting, this setting is used to resolve anonymous e-mails to their display names. By default, Exchange 2003 prevents *spoofing*, or forging identities, by requiring authentication before a sender's name is resolved to its display name in the global address list (GAL). But if you would like to change this behavior, select the **Resolve anonymous e-mail** check box. You must keep in mind that there is a possibility for unauthorized users to send e-mail with a forged address of a legitimate user. Because the default setting works in such a way that e-mail messages now resolve to their display name in the GAL, it's more difficult to distinguish a legitimate sender from a forged address. We will talk more about e-mail spoofing later in the chapter.
- **Basic authentication** Select the **Basic authentication** check box if your users should be allowed to connect to this default SMTP virtual server by verifying their usernames and passwords in clear text. When using this setting, you should enable encryption of usernames and passwords by selecting the **Require TLS encryption** check box and/or the **Integrated Windows Authentication** check box.
- **Require TLS encryption** Transport Layer Encryption (TLS) is used to encrypt usernames, passwords, and just as important, the message data. Keep in mind that only mail clients (such as Outlook Express) supporting the TLS feature can relay through

the default SMTP virtual server if you select the check box. Note that you must have enabled a certificate on the SMTP virtual server for this feature to work.

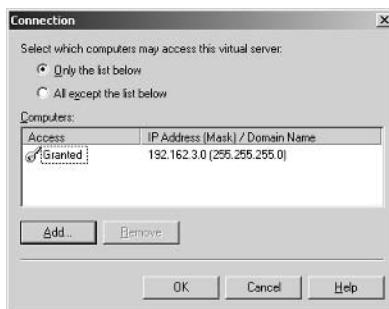
- **Default domain** In this text box you can specify the default domain to which the mail clients should authenticate. If you use a shared hosting model or similar setup and are using multiple SMTP virtual servers, specifying the default domain can be a good idea. If a user from a domain other than the one specified needs to authenticate to this SMTP virtual server, fortunately that's still possible—the user need only enter his or her username in the following format: *domain\username*.
- **Integrated Windows Authentication** If you want to only allow access to users with a valid Windows user account, select this check box. Because this authentication method uses the Windows NT LAN Manager (NTLM) mechanism, usernames and passwords are encrypted, but the message data is not.
- **Users** Note that this button is grayed out because we the **Anonymous access** check box is selected. You need to disable **Anonymous access** to use this feature, which gives you the possibility to grant or deny submit permissions to specific users or groups. Note that this feature is rarely used.

Secure SMTP Communication

Let's move on to the next option, which is Secure Communication (see Figure 4.4). We will not go into detail about this option, but briefly, you should know that it is used to set up security certificates and encryption. For example, to use TLS encryption on an SMTP virtual server, you need to set up an SSL certificate by running the Web Server Certificate Wizard. When you have installed the SSL certificate, you can require that SMTP clients use TLS encryption to connect to the virtual server.

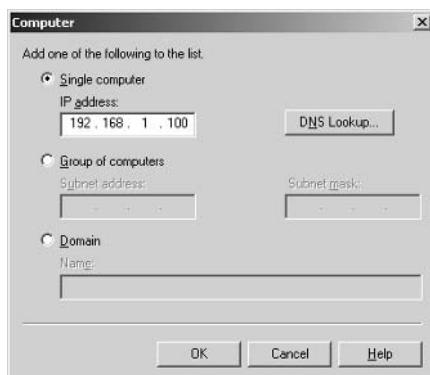
Figure 4.4 Access Tab Under Default SMTP Virtual Server Properties

You can allow and deny access by clicking the **Connection** button in the **Connection control** section, which brings up the screen shown in Figure 4.5.

Figure 4.5 Restricting Access to the SMTP Virtual Server

Note: Don't confuse the Connection Control feature with the Relay Restriction feature.

The primary goal of the Connection Control feature is to prevent specific computers from connecting to our SMTP virtual server. This can be done by specifying a single computer (IP address), groups of computers (subnet address, which is a range of IP addresses), or domains (see Figure 4.6).

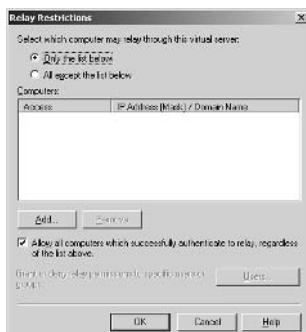
Figure 4.6 Specifying Computers, Groups of Computers, or Domains

Note: Specifying a domain can increase server load because the server would need to do a lookup on each IP address trying to establish a session to the SMTP virtual server.

Setting Relay Restrictions

The Relay Restrictions feature is one of the more interesting ones. It's important that you understand each setting this feature offers. By default, Exchange 2003 allows only authenticated computers to relay, which is a good default setting because it means that our SMTP virtual server is closed for relaying if the given host's IP address isn't listed under Computers (when only the list below is selected) or if a valid username and password can't be provided. As is the case with the Connection Control option, the Relay Restrictions option allows you to specify a single computer (IP address), a group of computers (subnet address, which is a range of IP addresses) or domains to have implicit access to relay through the SMTP virtual server.

When you click the **Relay** button (refer back to Figure 4.4), the screen shown in Figure 4.7 will appear.

Figure 4.7 SMTP Virtual Server Relay Restrictions

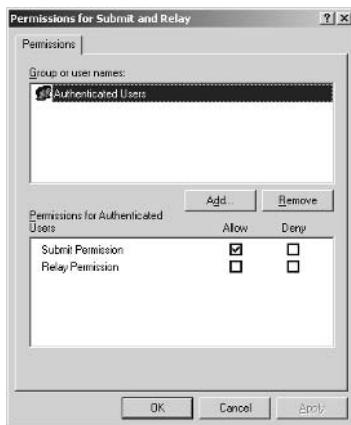


REALITY CHECK...

You should be very careful when experimenting with the relay restriction feature, because you can easily create a huge mess. For example, suppose you decide to select the **All except the list below** option because you want to deny access to a list of IP addresses, which you then specify. Your goal of blocking specific computers from relaying through your SMTP virtual server will be accomplished, but chances are you also granted relay access to anybody else except the users the specified list. This is the case if the **Anonymous access** check box under **Access | Authentication** is selected. If it is, you have just created what is known as an *open relay*. If you don't know what open relays are all about, don't worry—we will cover them later in this chapter.

As the observant reader might have noticed in Figure 4.7, there's also a grayed-out button labeled **Users**. If you deselect the **Allow all computers which successfully authenticate to relay, regardless of the list above** check box, the **Users** button will become active. When you click it, you will be presented with a screen similar to the one in Figure 4.8.

Figure 4.8 Permissions for Submit and Relay



Here you can grant or deny relay permissions to specific users and groups. If a user or a group is granted the Relay permission, the user or the group is allowed to submit mail to the SMTP virtual server and thereby send it to a mail user outside your organization—to put it another way, a user belonging to a mail server that is part of another

domain. You can also explicitly deny access to specific users or groups. (Remember, the *deny* permission always overrules *allow*.)

Note: For a user to relay through the SMTP virtual server, he or she must be granted both *submit* permission and *relay* permission!



REALITY CHECK...

It's important that you are aware that relay settings can only be set per SMTP virtual server (or SMTP connector, which we will talk about next). In Exchange 2003, there is no way to apply relay settings on the Exchange organization itself. In short, you must configure each SMTP virtual server's (or connector's) relay settings individually.

SMTP Connectors and Relaying

Even though SMTP connectors are relatively rarely used, we thought it a good idea to include them here, at least so you know what they are used for, but also for the benefit of readers who actually use or plan to use them in the future. The difference between an SMTP virtual server and an SMTP connector is basically that the latter provides many more features. An SMTP connector can be used between Exchange 2003 and other SMTP-compatible messaging systems such as UNIX SendMail or other SMTP hosts on the Internet. With an SMTP connector, you are able to link one or more bridgehead servers directly to a smart host or even to a remote server on which recipient addresses are stored.



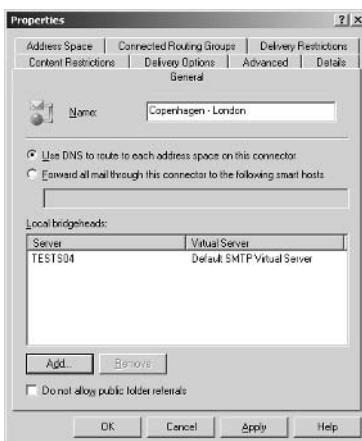
REALITY CHECK...

Many Exchange admins think they need to create an SMTP connector in order for e-mail messages to flow in and out of the Exchange servers, but this is far from true. You don't need to create an SMTP connector to have your Exchange server receive and deliver e-mail messages to and from other Exchange organizations or the Internet. That's all taken care of by your SMTP virtual servers. All you need for mail to flow is an Internet connection and a Mail Exchanger (MX) record pointing at your Exchange server. An *MX record* indicates which computer is responsible for handling the mail for a particular domain. If you don't have your own public DNS server, this record is typically set on an Internet service provider's (ISP's) DNS.

You create an SMTP connector the following way:

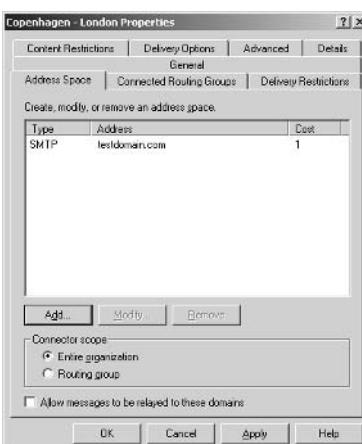
1. In the **Exchange System Manager**, right-click **Connectors**, then select **New | SMTP Connector**.
2. Give the new SMTP connector a sensible name (such as <local site> – <remote site>).
3. Specify whether you want to use DNS routing or a specified smart host (see Figure 4.9).

Figure 4.9 Creating a New SMTP Connector



4. Select a local bridgehead by clicking the **Add** button.
5. Click the **Address Space** tab, then click **Add** (see Figure 4.10).

Figure 4.10 Adding an Address Space



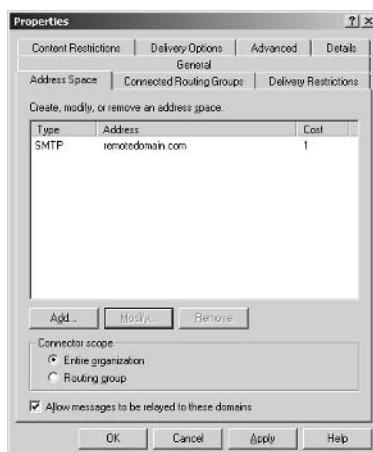
6. Select SMTP type, then click **OK**.
7. Specify the **E-mail domain** and **Cost** (see Figure 4.11).

Figure 4.11 Specifying Domain and Cost of the SMTP Connector



8. Click **OK**.
9. Put a check mark next to **Allow messages to be relayed to these domains** (see Figure 4.12).

Figure 4.12 SMTP Connector Address Space



When you enable the **Allow messages to be relayed to these domains** option on your local SMTP server, it can act as relay server for the remotedomain.com, meaning that POP3 clients, IMAP4 clients, and the remotedomain.com SMTP server can use this server to send and deliver any outgoing mail.



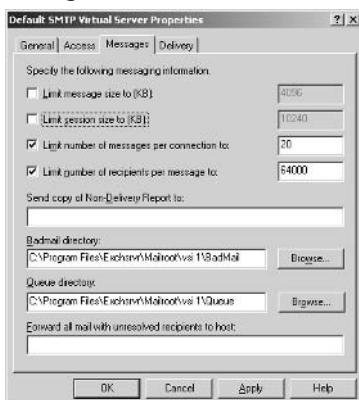
REALITY CHECK...

Because we have only briefly touched on the topic of SMTP connectors, we recommend that if you plan to use them, you do a search for *SMTP connector* on Microsoft Technet. Microsoft has published quite a few Knowledge Base articles on this topic.

Setting Mailbox Message Limits

We have reached the Messages tab (see Figure 4.13), under which you configure limits for such things as messages, sessions, number of messages per connection, and number of recipients per message.

Figure 4.13 The Messages Tab Under SMTP Virtual Server



“What do these settings have to do with security?” you might ask. The answer is, a lot. Besides controlling the various message limits of your users, this is one of the places where you actually can set specific settings to prevent your Exchange server against things such as DoS attacks. When an Exchange server is targeted for a DoS attack, one of the most widespread ways of accomplishing it is to inundate the messaging system with large messages (often more than 20MB each!). Such types of attack will bring even the heaviest Exchange server to its knees because it’s forced to move large blocks of data, which will impact the server input/output (I/O) to the extent that mail service is delayed or interrupted completely.

To prevent DoS attacks, Exchange 2003 message limits (or to be more accurate, session limits) have by default been set to 10MB (10240KB), which in most cases should be a sufficient size. Note that the

10MB (10240KB) limit has in Exchange 2003 not only been set on the default SMTP virtual server, but it also includes messages sent and received by the Exchange organization and messages posted to public folders. (Actually, the SMTP virtual server inherits the setting from the Exchange organization by default, as you can see in Figure 4.13.)



REALITY CHECK...

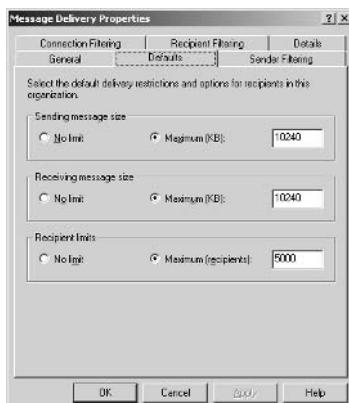
It's important to keep in mind that if you have completed an in-place upgrade from Exchange 2000 to 2003, Exchange will not change the message size limit already specified in Exchange 2000. So, if you want to follow Exchange 2003 default limits, you should specify this limit manually after the upgrade. There is one exception, though: If the settings of the limit are set to **No Limit**, the Exchange setup will impose these settings with the new one.

Setting Mailbox Message Limits Globally

To adjust the message size limits on an Exchange organization level, meaning that the specified setting will not only affect a given SMTP virtual server but all SMTP virtual servers in the entire organization, do the following:

1. In the **Exchange System Manager**, expand **Global Settings**.
2. Right-click the **Message Delivery** object, then select **Properties**.
3. Click the **Defaults** tab (see Figure 4.14).

In Figure 4.14, you can see that the Sending and Receiving message sizes are set to 10MB (10240KB) by default.

Figure 4.14 Message Delivery Properties

Configuring Internet Message Formats

Although they're not part of the security-related features of the SMTP virtual server, you should be aware of the different Internet Message Format options, since some of them are related to SMTP security. These options are set under the **Advanced** tab of the default **Internet Message Format**. To get to this tab, do the following:

1. In the **Exchange System Manager**, expand **Global Settings**.
2. Single-click **Internet Message Format**, then right-click **Default** in the right pane and select **Properties**.
3. Click the **Advanced** tab. You'll be presented with the screen shown in Figure 4.15.

Figure 4.15 Default Properties of Internet Message Formats

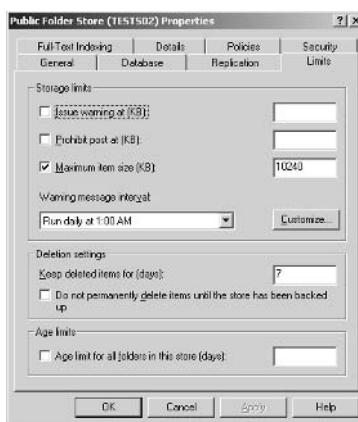
On this tab are three options related to security:

- **Allow out of office responses** This check box allows out-of-office responses to be sent outside the organization. Typically it's not a good idea to select this check box, since it could allow malicious users to learn when users are out of their offices. In other words, this option should only be allowed internally in the organization. Leave this check box cleared unless you have a very special need for selecting it.
- **Allow automatic replies** Selecting this check box makes it possible for your users to configure their mailboxes to make automatic replies. You should keep this check box cleared because it's generally not a good idea to send out automatic replies to external mailboxes.
- **Allow automatic forward** Selecting this check box allows your users to, for example, create a rule that forwards all internal (typically considered confidential) mail to an external account (such as Hotmail). Many organizations have security policies against this practice. Therefore, leave the check box cleared unless you have special needs that require you to select it.

Setting Public Folder Limits

To configure the sending and receiving message limits for public folders, do the following:

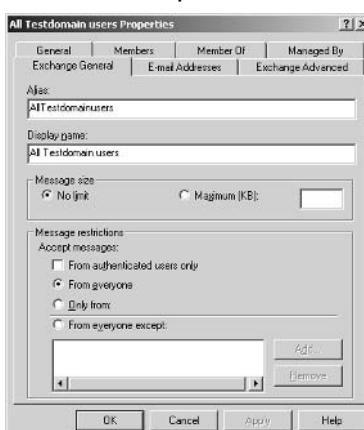
1. In the **Exchange System Manager**, drill down to **Servers | Server | First Storage Group**.
2. Right-click the **Public Folder Store** object, then select **Properties**.
3. Click the **Limits** tab (see Figure 4.16).

Figure 4.16 Public Folder Store Message Limits

As you can see in Figure 4.16, the maximum item size is, by default, set to 10MB (10240KB).

Protecting Mail-Enabled Groups

It's not only user mailboxes we have to worry about. Improperly configured mail-enabled groups (also known as *distribution lists*) can be a security threat to your organization. Because a mail-enabled group can receive mail just like any user, it is also vulnerable to threats such as spam, virus attacks, and DoS attacks. What can we do to protect our mail-enabled groups? We have a few simple but effective configuration settings we can change. Even though Exchange 2003 in general is quite secure (because of Microsoft's trustworthy computing initiative), oddly enough, a mail-enabled group is, by default, rather insecure (see Figure 4.17).

Figure 4.17 Mail-Enabled Group's Default Settings

As you can see in Figure 4.17, a mail-enabled group, by default, doesn't have a message size limit, but this setting should definitely be restricted.

Then we have the message restrictions (see Figure 4.17), which have two important options. By default, Exchange 2003 accepts e-mail messages from everyone. If the mail-enabled groups are only for internal use, we recommend you restrict the groups by putting a check mark in the **From authenticated users only** box. This will typically block all spam and DoS attacks against the mail-enabled group.

Note: When you enable the **From authenticated users only** option, any user sending a message to the mail-enabled group must have been validated, through either Outlook or OWA or to the SMTP virtual server.

The last two security-related options for dealing with mail-enabled groups are the **Only from** and **From everyone except**. With **Only from**, we can restrict our mail-enabled group even further by specifying which users actually can send messages to it. We can also choose to specify it the other way around by specifying that everyone (authenticated or not) can send e-mail messages to the group and then create a special exception from list, with which we can exclude either users or other mail-enabled groups.

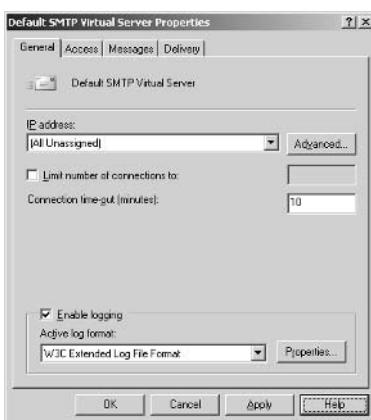
Enabling SMTP Protocol Logging

It's strongly recommended that you enable SMTP protocol logging, because protocol logs can be used to track the commands that the SMTP virtual server receives from SMTP clients. They can also be used to track outgoing SMTP commands. When enabling the SMTP protocol logging option, you need to choose the logging format Exchange should use to log the information. You can choose between ASCII-based formats and Open Database Connectivity (ODBC) database. The ASCII logs can be read in a text editor such as Notepad but are typically loaded into some kind of report-generating software tool. As the name indicates, ODBC logging format can be logged in an ODBC-compliant database (such as Access, MSDE, or SQL). For most, it should be sufficient to use the W3C extended log file format for SMTP logging.

The following steps show you how to enable the SMTP protocol logging option:

1. In the **Exchange System Manager**, drill down to **Servers | Server | Protocols | SMTP**.
2. Right-click the **Default SMTP virtual server**, then select **Properties**.
3. Put a check mark next to **Enable logging** (see Figure 4.18).

Figure 4.18 Enabling SMTP Virtual Server Logging

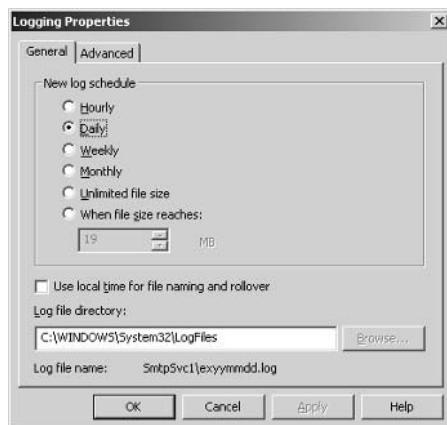


4. Select the appropriate type of log format, then click **OK**.

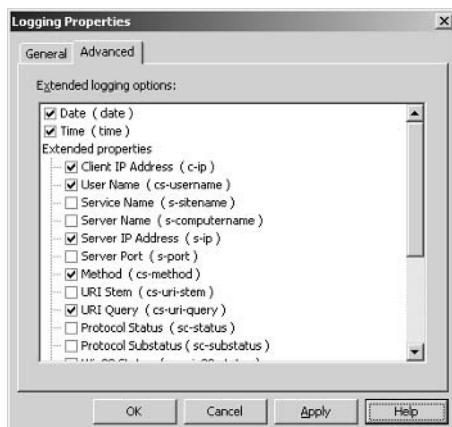
Now that the logging feature has been enabled, we need to choose the log format. In this example, we will use the W3C extended log file format.

5. Select **W3C Extended Log File Format**, then click **Properties**.

Under the General tab (see Figure 4.19), we can specify the type of log schedule; daily (the default) should be sufficient in most situations. As you can see, it's also possible to specify a log file directory. Again, leave the defaults if you have no specific requirements for changing this setting. Also note the filename displayed right under the **Log file directory** box. This name is determined by the log file format and the criterion used for starting new log files.

Figure 4.19 Logging Properties of an SMTP Virtual Server

6. Click the **Advanced** tab (see Figure 4.20). This tab is probably the most interesting because this is where we specify the type of information we want to log.

Figure 4.20 The SMTP Protocol Logging Advanced Tab

As you can see, quite a few extended logging options are available, but if you're dealing with SMTP virtual servers, we recommend you log things such as:

- **Date** Record the date where activity occurred.
- **Time** Record the time where activity occurred.
- **Client IP address** Record the IP address of the client accessing your SMTP virtual server.

- **Username** Record the name of the authenticated user who accessed your SMTP virtual server. It's important to note that this doesn't include anonymous users, who are represented by a hyphen.
- **Method** Record the action the client tried to perform.
- **URI Query** Record the query the client tried to perform.
- **Time Taken** Record the length of time the action took to complete.

Notes from the Underground...

Consider Using a Third-Party SMTP Protocol Logging Product

Most of you have probably tried to read different types of logging files in Notepad (or another favorite text editor) and know how difficult it can be to read a log file's content through a text editor. The same is true for reading SMTP protocol logs. If you're really serious about reading these log files (maybe because your organization's security policy demands it), we suggest you use a third-party product, which can create nice reports.

Some of the most popular log-reporting products are:

- **Promodag** www.promodag.com
- **MessageStats** www.quest.com/messagestats
- **E-nspect** www.e-nspect.co.uk/e2v2.htm
- **Sawmill** www.sawmill.net

Modifying the SMTP Banner

As part of securing your SMTP service, you have the option of modifying the default SMTP banner so that any malicious person can't find out the type of system you're running. As mentioned earlier, anyone, by default, has access to make a connection to port 25/TCP (SMTP). So if a malicious person on the Internet, preparing for some kind of attack, wants to retrieve the SMTP version of your system, it could be done in seconds. The following steps demonstrate how this is accomplished.

(Remember to make a backup of the metabase before changing this information on any production servers.)

Do the following:

1. From a client, open a command prompt (click **Start** | **Run** and type **CMD**).
 2. Type **telnet <servername_or_IP> 25**.

If you Telnet an Exchange 2003 Server, you will get output similar to the following:

220 tests02.testdomain.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at Sat, 27 Mar 2004 17:25:19 +0100

You might wonder why the previous example says Version: 6.0.3790.0, when as of this writing Exchange 2003 Server is at Version 6.5 (Build 6944.4). This is because it's the SMTP version (and not the Exchange version) that is informed.

If you would like to change the SMTP banner, you need to do some metabase editing. The following steps show you how to change the SMTP banner on an Exchange 2003 Server:

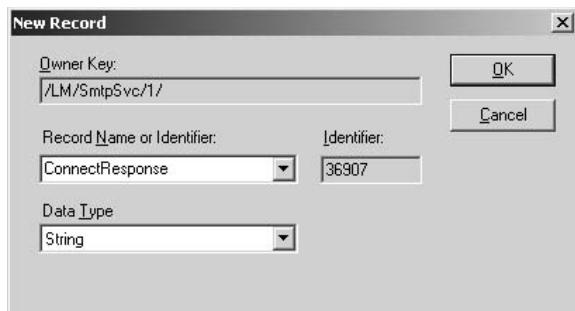
1. Grab a copy of the IIS 6.0 Resource Kit from www.microsoft.com/downloads/details.aspx?familyid=56fc92ee-a71a-4c73-b628-ade629c89499&displaylang=en.
 2. Install the IIS 6.0 Resource Kit on your Exchange 2003 server.
 3. Click **Start | Run | All Programs | IIS Resources | Metabase Explorer | Metabase Explorer**.
 4. Expand **LM | SmtpSvc** (see Figure 4.21).

Figure 4.21 SmtpSvc in Metabase Explorer

IIS Metabase Explorer							
	ID	Name	Date Type	Data	Attributes	Bytes	UserType
TESTS02 (local)							
[+]	LM	1002	KeyType	String	IisSslpServer	none	26
[+]	DS3MB	1013	ConnectionString	DWORD	500	4	Server
[+]	EventManager	1014	MaxConnections	DWORD	200000000	none	4
[+]	ISADMIN	1015	ServerComment	String	Default SMTP Virtual Server	4	Server
[+]	IMAP4SVC	1016	ServerStat	DWORD	2	54	Server
[+]	1017	ServerAutoStart	DWORD	1	4	Server	
[+]	Logging	1023	ServerBindings	MultiString	25:	4	Server
[+]	MimeMap	1025	ClusterEnabled	DWORD	0	8	Server
[+]	NNTPSVC	1093	Vin32Error	DWORD	0	4	Server
[+]	POP3SVC	38871	MaxBatchedElements	DWORD	20	4	File
[+]	resvc	38875	QueueDirectory	String	C:\Program Files\Exchsvr\Mailroot\1\queue	none	52
[+]	SinkSvcs	38880	PublishDirectory	String	C:\Program Files\Exchsvr\Mailroot\1\httpd\up	none	54
[+]	Info	38881	Path	String	C:\Windows\System32\netm\route.dll	4	Server
[+]	resvc	38884	EndLabelReverse	DWORD	0	4	Server
[+]	W3SVC	38896	HotCount	DWORD	30	4	Server
[+]	38897	MaxMessageSize	DWORD	0	4	Server	
[+]	38892	MaxSessionSize	DWORD	0	4	Server	
[+]	38894	MaxOutConns	DWORD	1000	4	Server	
[+]	38895	MaxReplies	DWORD	64000	4	Server	
[+]	38905	SmallHostType	DWORD	0	4	Server	
[+]	38908	DefaultDomain	String	testdomain.com	20	Server	
[+]	38909	BadMailDirectory	String	C:\Program Files\Exchsvr\Mailroot\1\BadMail	56	Server	
[+]	38913	DiskQuotaDeode	DWORD	0	4	Server	
[+]	38914	RemoteSmtpPort	DWORD	25	4	Server	
[+]	38918	ErrDays	DWORD	12	4	Server	

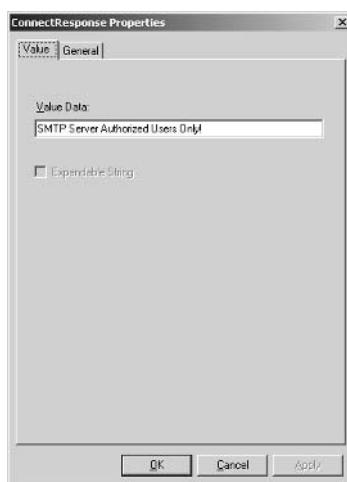
5. Right-click 1 (Virtual Server number), then select **New | String Record**.
6. In the drop-down text box under **Record Name or Identifier**, choose **ConnectResponse** (see Figure 4.22).

Figure 4.22 New Metabase String Record



7. Click **OK**.
8. Double-click the new identifier in the right pane.
9. In the **Value Data** field, type the text you want displayed when people connect to the SMTP service (see Figure 4.23).

Figure 4.23 ConnectResponse Properties



10. Click **OK** and close the Metabase Explorer.
11. Stop and then restart the SMTP service so that the changes take effect.

Try to Telnet the Exchange server on port 25 again. You should now see text similar to the following:

```
220 tests02.testdomain.com SMTP Server Authorized Users Only! Sat,  
27 Mar 2004 18:34:00 +0100
```

You might have tried to change the SMTP banner in Exchange 2000. If so, you probably remember that you used the MetaEdit utility to do this. However, we advise against using this utility on IIS 6.0, because it is designed for IIS 4.0 and 5.0 only! If you have installed Exchange 2003 on a Windows 2000 server, you could still use the old utility; see Microsoft KB article 281224, “XCON: How to Modify the SMTP Banner,” at www.support.microsoft.com/?id=281224 for specific instructions on using MetaEdit.

If you make a Telnet connection to the server after this change, the output will look similar to the following:

```
220 tests02.testdomain.com Authorized Users Only! Sat, 27 Mar 2004  
20:26:52 +0100
```

If you would also like to change the fully qualified domain name (FQDN), you do this in the Exchange System Manager as follows:

1. Open the **Exchange System Manager**.
2. Expand **Servers** | **Server** | **Protocols** | **SMTP**.
3. Right-click **Default SMTP Virtual Server**, then select **Properties**.
4. Click the **Delivery** tab, and then click the **Advanced** button.
5. In the **Fully qualified domain name** box, enter the FQDN you would like to have displayed in the SMTP banner.



REALITY CHECK...

If you change the SMTP banner, you should also consider changing the banner for POP3 and IMAP4 (if you use the protocols). Unfortunately, this cannot be done using the previous method. Instead, you need to follow the step-by-step instructions in the MS KB article 303513, “XCON: How to Modify the POP or IMAP Banner,” at www.support.microsoft.com/?kbid=303513.

Note that the article assumes that you have a copy of the `smtpmd.exe` utility. To get that copy, you need to call Microsoft Product Services because you cannot download it from any Microsoft Web site.

Configure a Corporate Legal Disclaimer

We recommend that you configure a corporate legal disclaimer (also called a *footer*) on a global level in your Exchange organization. Configuring a disclaimer will add a small piece of text in the footer of each user's outgoing messages. The concept of using a disclaimer has been around for years, typically attached to ads, company slogans, and other text to ensure that an approved corporate message is consistently communicated. But increasing numbers of court decisions have been clear and unequivocal in establishing the principle that a corporation is responsible for the content of its employees' e-mail messages, even if the message is very different from the corporate organization's beliefs and positions. This means that for everything sent from a corporate e-mail system—no matter whether it's sent between mailboxes on the company server or to the outside world—the organization can be held responsible for all content. Primarily because of these court decisions, organizations need to protect themselves by means of legal disclaimers.

You can configure a disclaimer in several ways. One of them is to use a so-called SMTP Transport Event Sink; this would be considered the complex method. For instructions, see Microsoft KB article 317327, "How to Add a Disclaimer to Outgoing SMTP Messages in Visual Basic," at www.support.microsoft.com/?id=317327.



REALITY CHECK...

Be aware that Microsoft KB article 317327, "How to Add a Disclaimer to Outgoing SMTP Messages in Visual Basic" (www.support.microsoft.com/?id=317327) we refer to only works with either pure Windows 2000 SMTP servers or Exchange 2000 and 2003 Exchange servers running on Windows 2000. Said in another way, no SMTP Transport Event Sink script currently exists for pure Windows 2003 SMTP servers or Exchange 2003 servers running on Windows 2003. Therefore, we recommend that you configure the SMTP Transport Event Sink on an SMTP gateway in your organization.

The other method is to use one of the many third-party products offering a disclaimer feature either as part of another product or as a single utility. Though a few freeware versions exist, you will need to pay for most of these products. Table 4.1 lists some of the most popular products that include the disclaimer feature.

Table 4.1 Disclaimer Products

Product	Web Site URL	Comments
GFI MailEssentials	www.gfi.com/mes	Disclaimer feature included in the freeware version
MxClaim	www.customermag-netism.co.uk	Not free but relatively inexpensive
eXclaimer	www.exclaimer.co.uk	Not free but relatively inexpensive
Policy Patrol	www.policypatrol.com/ PolicyPatrolDisclaimers.htm	Not free but relatively inexpensive, depending on amount users

SMTP Relaying

When it comes to Exchange servers (or mail servers in general), one of the most important tasks is to keep the SMTP relay as secure as possible. Organizations that don't use the SMTP relaying feature should consider disabling it completely.



BY THE BOOK...

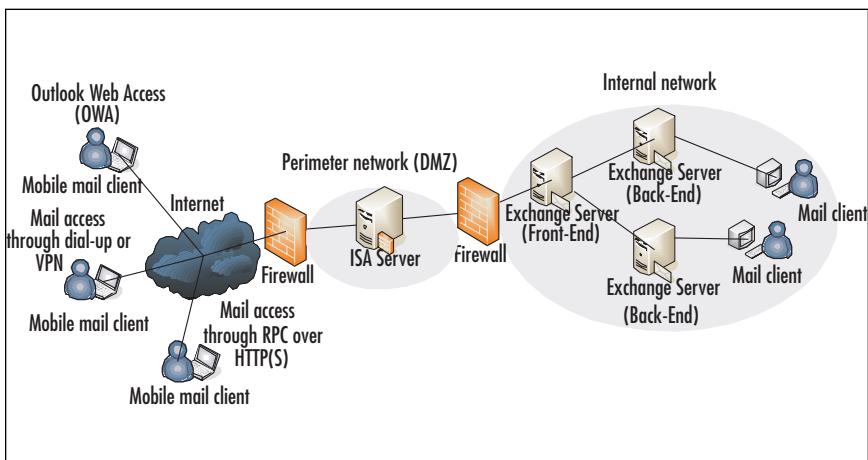
A SMTP relay server can best be described as a server that accepts mail from other SMTP servers (Exchange, SendMail, Lotus Notes, and the like) and SMTP clients (Outlook, Outlook Express, Eudora, Netscape Communicator, and so on). When the mail is received, the SMTP relay server forwards it on to nonlocal recipients at a nonlocal domain. What we mean by nonlocal recipients and domains is mail-enabled users located at a domain not belonging to our organizations messaging environment.

A SMTP relay server is a very common type of server among ISPs and other application service providers (ASPs) for two reasons. One, these organizations often have a huge number of customers that use the ISP's SMTP relay server to send mail messages to their friends, families, and colleagues, but also because many smaller organizations that have bought a relatively cheap broadband connection aren't allowed to route port 25 (SMTP) traffic to destinations other than the ISP's SMTP relay server, or *smart host*, as it's often referred to in the Exchange world. The reason that many ISPs choose to block port 25 (SMTP) traffic is to avoid having their IP blocks ending up on different

real-time block lists (RBLs) because of customers either sending out spam on purpose or simply having configured their mail servers improperly. ISPs often also offer a so-called SMTP backup service, which basically means that the ISP's SMTP server will accept and process a given customer's mail, in case his or her primary mail server goes down for some reason. This is done with the help of a secondary MX record pointing to the ISP's SMTP server, in addition to your primary MX record.

"Do I need an SMTP relay?" you might ask. Well, that depends. If you strictly have internal users using Outlook and maybe a few users who are sometimes on the road connecting directly to your Exchange environment with OWA, RPC over HTTP(S) or a dialup or virtual private network (VPN) connection to connect to your organization to send and receive mail with the Outlook client, the answer would be no, you don't need an SMTP relay. Figure 4.24 shows an Exchange messaging environment in which you wouldn't need the SMTP relay feature.

Figure 4.24 Exchange Messaging Environment Without an SMTP Relay Server



If your Exchange environment includes a SMTP gateway, it has to be configured to relay mail, but only for your own domain! Why do we emphasize this? Because we have seen and heard of all too many improperly configured SMTP relay servers, which often end up acting as so-called open relay servers.



REALITY CHECK...

An *open relay* is an SMTP server that has been (mis)configured in such a way that it allows any anonymous (unauthenticated) sender to send his or her mail through it to any destination he or she likes. If you configure an SMTP server as an open relay, it's a matter of days (or maybe even hours) before it will be found by an evil spammer, who will use it to send out spam and other unsolicited e-mail. We have seen several open relay servers that were sending out thousands of e-mail messages an hour.

Besides slowing down your messaging environment and taking up a huge load of disk space, system resources (such as CPU load), and bandwidth, there's another very negative side effect. If you don't have the open relay closed at the speed of light, your IP address or domain will certainly end up on one or more RBLs because all the mail users who receive the spam from your open relay will of course see the spam originating from your IP address or domain. If the Exchange admins haven't already found out you sent spam to their users, a frustrated user will certainly tell them. When your IP address or domain ends up on one or more RBLs, your users will suddenly be unable to send mail to users located behind mail servers that use RBLs to filter spam server-side. If all this weren't enough, if you end up on an RBL, it's often a big pain to get your IP address or domain erased from it after you actually have closed your open relay. So be careful when experimenting with your SMTP server's relay settings.

Notes from the Underground

Exchange 5.5 and SMTP Relaying

The Exchange 5.5 product was actually developed in such a way that it (or more specifically, the Internet Message Connector, also known as IMS) by default was installed as an open relay—no, we're not kidding! So you can probably imagine that Exchange servers were a kind of paradise for spammers in the past. Fortunately, this rather big design flaw was corrected in Exchange 2000, so today, Exchange by default allows only authenticated users to relay through it.

Due to customer demand, Microsoft recently released (some would say a little late) Microsoft KB article 836500, "Relaying and unsolicited commercial e-mail in Exchange Server

Continued

5.5," at <http://support.microsoft.com/?kbid=836500>, which talks about open relaying and how you can protect your Exchange 5.5-based messaging environment. The KB article is definitely worth a read, even for all you Exchange admins who are no longer using Exchange 5.5.

Open Relay Test Methods

At some point you will check your Exchange server to see whether it acts as an open relay. If you find one of your Exchange servers is configured as an open relay, we guess you would like to check which RBLs it's listed on. Here we'll show you how to do both.

You can check your Exchange server for open relays manually by issuing a few SMTP commands to it using Telnet, or by using one of the many sites offering a Web-based solution (the easiest method).

Let's start with the Telnet method. Let's try to relay an e-mail through our tests02.testdomain.com server:

1. Open a command prompt.
2. Type **telnet tests02.testdomain.com 25** (substitute *tests02.testdomain.com* with your own FQDN).

If the SMTP server is running, we get following answer:

```
220 tests02.testdomain.com Microsoft ESMTP MAIL Service,  
Version: 6.0.3790.0 ready at Tue, 30 Mar 2004 21:00:05  
+0200
```

The SMTP server on tests02.testdomain.com issues a 220 response code, indicating that the connection was successful and that the extended SMTP (ESMTP) server is ready to accept SMTP mail commands. This code is then followed by the FQDN of the server (tests02.testdomain.com) as well as the Exchange SMTP server version (6.0.3790.0) and the current date, year, and time.

3. Type **HELO spamking.spamnest.com**.

The server responds with:

```
250-tests02.testdomain.com Hello [192.168.1.221]
```

First we specify the type of language our SMTP client speaks—in this example, HELO, which is standard SMTP. (It could as well have been EHLO, which is a newer standard than HELO and makes the server advertise additional features.) When we present our SMTP client to the server, it acknowledges the *HELO* command with the 250 response code, which

means OK. Then the server “greets” the client with “Hello [local IP address].”

- Type **MAIL FROM: spamking@spamnest.com.**

The server responds with:

```
250 2.1.0 spamking@spamnest.com....Sender OK
```

With the *MAIL FROM* command, we tell the server who the sender (or originator) is, and the server then responds with a response code 250 2.1.0, which, in humans language, means “OK User not local but will accept mail anyway.”

- Type **RCPT TO: henrik@testdomain.com.**

```
550 5.7.1 Unable to relay for henrik@testdomain.com
```

We get the response code 550 5.7.1. which in this example means “Relaying not permitted.” If you get this response code, your Exchange server is most likely a closed relay and everything is as it should be, but if you instead get a 250 2.1.5 henrik@testdomain.com response, chances are you have an open relay, and it is recommended that you examine and correct the configuration error.

Figure 4.25 shows the steps we have been through in action.

Figure 4.25 Open Relay Test Using Telnet

```
cn> Telnet tests02.testdomain.com
220 tests02.testdomain.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at Tue, 30 Mar 2004 22:23:38 +0200
HELO spamking.spamnest.com
250 tests02.testdomain.com Hello [192.168.1.221]
MAIL FROM: spamking@spamnest.com
250 2.1.0 spamking@spamnest.com....Sender OK
RCPT TO: henrik@exchange-faq.dk
550 5.7.1 Unable to relay for henrik@exchange-faq.dk
```

As we mentioned, there are many Web-based services that will help you examine whether your (or somebody else’s) server is an open relay. Table 4.2 lists some of these sites.

Table 4.2 Popular Open Relay Test Sites

Provider	Web Site URL
Open Relay Database (ORDB)	www.ordb.org/submit
Network Abuse Clearinghouse	www.abuse.net/relay.html
Open Relay Test	members.iinet.net.au/%7Eremmie/relay
Relay Check	www.relaycheck.com/test.asp
SpamLArt Open Relay Testing	spamlart.homeunix.org
Msv.dk	msv.dk/ms009.asp
Open Relay Tester	www.mob.net/~ted/tools/relaytester.php3

Notes from the Underground...

A Few Words About Open Relay Testers

No open relay testers—or any tools you’re likely to find—can provide an exhaustive test. If you test a given server and it’s referred to as safe, it merely means that the open relay tester encountered none of the vulnerabilities that it tests for. It’s safe to assume that there are other vulnerabilities that were not detected and that a given server is in fact still open.

E-Mail Address Spoofing

A common way of attacking an e-mail messaging environment is to use e-mail address spoofing. In short, spoofing means that a person is pretending to be any other person without leaving any kind of traces. There’s currently not very much you can do to protect your e-mail messaging environment against e-mail address spoofing, but fortunately, Exchange 2003 provides a functionality to help minimize it.



BY THE BOOK...

E-mail messages can be considered *spoofed* if the e-mail address in the From field is not identical to the original sender’s address. The e-mail address of an innocent victim can be hijacked, so that e-mail messages containing spam or viruses can look as though they came from the innocent victim instead of the actual sender.

of the mail. But e-mail address spoofing can also be used to persuade another user (perhaps a business partner of the innocent victim) to provide the malicious sender with, for example, corporate confidential information, in that spoofed e-mail could purport to be from someone in a position of authority, asking for sensitive data. As you can see, this type of threat can be extremely dangerous for an organization, especially those that deal on a day-to-day basis with highly confidential information. Unfortunately, it's not very hard to spoof e-mail, but on the other hand, it's also fairly easy to detect—at least for an Exchange admin, that is.

Since e-mail spoofing often can be categorized as a threat, why is it allowed by default in Exchange 2003 and on many other SMTP servers? That's because of SMTP. As we touched on earlier in this chapter, SMTP, by default, allows anonymous connections to port 25. This means anyone with the requisite knowledge can connect to an SMTP server and thereby use it to send messages. To send spoofed e-mail messages, the malicious sender typically inserts special commands in the Internet headers that will alter the e-mail message information.

We will show you how to configure Exchange 2003 to help minimize e-mail address spoofing in your messaging environment. But before we do that, we need to straighten out some basic concepts.

Authentication and Resolving E-Mail Addresses

By default, when Exchange 2003 receives an e-mail message from an authenticated client (Outlook, Outlook Express, OWA, or the like), the server verifies that the sender is in the GAL, and if the sender's name is present, the user's display name (in the From field) on the message is resolved. If the message has been sent without authentication, Exchange 2003 will mark the e-mail message as unauthenticated. This means that the e-mail address of the sender won't be resolved to the display name (for example, Henrik Walther) found in the GAL. Instead, it will be shown in its SMTP format (for example, henrik@exchange-faq.dk). So, it's important to understand that if a user in your organization receives an e-mail message from another user who is a member of the same active directory domain, and this e-mail message's From line displays the sender's full SMTP address instead of his or her GAL display name, chances are it's a spoofed e-mail message.

Note: To see where you enable/disable the **Resolve anonymous e-mail** feature, look back at Figure 4.3.



REALITY CHECK...

It's very important to educate the users in your organization so that they always keep an open eye on the From line in any e-mail messages they receive. You should tell them to be very careful in replying to messages where the From line contains the full SMTP address of a colleague instead of the GAL display name, because if this is the case they are most likely dealing with a spoofed e-mail message. If they reply, the message will end up in the in-box of a malicious sender's mail client, not the colleague's.

Notes from the Underground...

Exchange 2000 and E-Mail Address Spoofing

You should be aware that Exchange 2000 does resolve e-mail messages submitted anonymously. As you can imagine, this makes it quite difficult (especially for an ordinary user) to judge whether an e-mail message is spoofed. If you're dealing with any Exchange 2000 servers, we highly recommend you change this behavior. This can be accomplished by adding a registry key on the Exchange server, but because this book is about Exchange 2003 only, we won't cover the step-by-step instructions here. Instead, we suggest you read Microsoft KB article 288635, "XIMS: ResolveP2 Functionality in Exchange 2000 Server," at www.support.microsoft.com/?id=288635 to obtain further information.

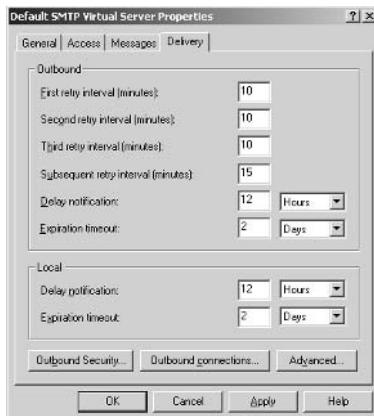
Reverse DNS Lookup

Another Exchange 2003 feature (disabled by default) that you should consider enabling to prevent against e-mail address spoofing in your organization is the reverse domain name system lookup feature, which is found under the Default SMTP virtual server.

You enable the DNS reverse lookup feature the following way:

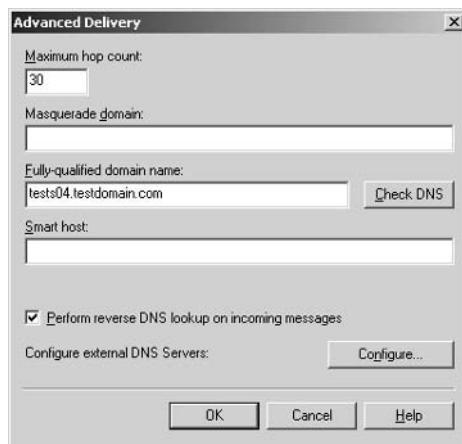
1. Open the **Exchange System Manager**.
2. Drill down to **Servers | Server | Protocols | SMTP**.
3. Right-click the default SMTP virtual server, then select **Properties**.
4. Click the **Delivery** tab (see Figure 4.26), then click the **Advanced** button.

Figure 4.26 The SMTP Virtual Server Delivery Tab



5. On the screen that appears (see Figure 4.27), put a check mark in the **Perform reverse DNS lookup on incoming messages** box.

Figure 4.27 Enabling the Reverse DNS Feature



By enabling the reverse DNS lookup feature on your Exchange 2003 server, you ensure that the sending e-mail message server's IP address (and its FQDN) matches the message sender's domain name, and if a record cannot be found, the message is denied. The downsides are that organizations that are trying to send you legitimate mail will be excluded if they don't have a pointer or reverse record (PTR), which unfortunately many organizations still don't, but should, have. The reverse lookup feature also increases the load on your Exchange Server computer (the server has more work in resolving every inbound connection back to a name using DNS) and requires that your Exchange Server computer can contact the reverse lookup zones for the sending domain.

Internet Mail Headers

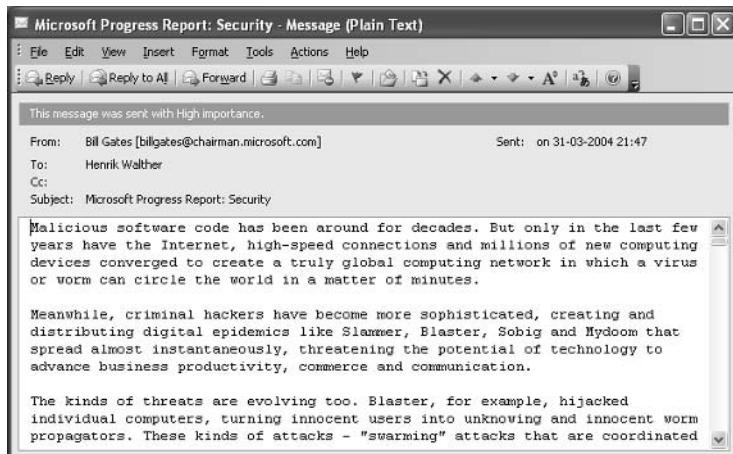
As an Exchange admin, you should know what an Internet mail header is all about. Every Internet e-mail message is made up of two parts: the header and the message body. The header contains valuable information on the path the message took to reach you. Knowing how to check an Internet header can come in handy—for example, if you're tracing the original sender of a spoofed e-mail message, or just to see if a given e-mail message actually is spoofed. Knowing how to check an Internet Mail Header can also come in handy during other kinds of troubleshooting issues.



BY THE BOOK...

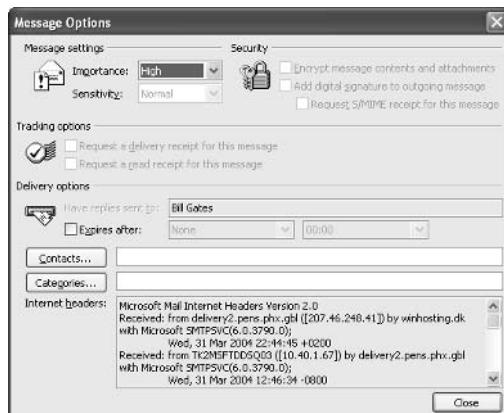
Every received e-mail has an Internet header. A valid Internet e-mail header provides a detailed log of the network path the message took between the mail sender and the mail receivers. This Internet mail header can sometimes be quite long, depending on the network path between sender and receiver.

Your e-mail client program will usually hide the full header or display only a few of its lines, such as From, To, Date, and Subject. Figure 4.28 shows an example of the default headers that are visible when you open an e-mail message in Outlook 2003.

Figure 4.28 Default Header Shown in an Outlook E-Mail Message

An e-mail's complete Internet header can have 20 lines or more showing all kinds of information about the message, such as which servers the e-mail has traveled through and when (although spammers sometimes forge some of a header to disguise the e-mail's actual origin). Your e-mail program can also display the "full" header of an e-mail, though it might not be obvious how. The following steps show you how this is done in an Outlook 2003 client:

1. Start **Outlook 2003**.
2. Open an e-mail message—for example, by double-clicking on it.
3. In the menu, select **View | Options**. You'll now see the screen shown in Figure 4.29.

Figure 4.29 Internet Header in Outlook 2003

In the bottom of the figure, you can see the Internet header, but because the header is too big for us to be able to see it in the Internet header box, we show the complete header here:

```
Microsoft Mail Internet Headers Version 2.0
Received: from delivery2.pens.phx.gbl ([207.46.248.41]) by
winhosting.dk with Microsoft
SMTPSVC(6.0.3790.0);
Wed, 31 Mar 2004 22:44:45 +0200
Received: from TK2MSFTDDSQ03 ([10.40.1.67]) by
delivery2.pens.phx.gbl with Microsoft SMTPSVC(6.0.3790.0);
Wed, 31 Mar 2004 12:46:34 -0800
Reply-To: "Bill Gates"
<10_132_KNZiMBwjgiRqfK8bWmPT0w@newsletters.microsoft.com>
From: "Bill Gates" <billgates@chairman.microsoft.com>
To: <henrik@exchange-faq.dk>
Subject: Microsoft Progress Report: Security
Date: Wed, 31 Mar 2004 12:46:33 -0800
Message-ID: <e95f401c41761$40ce6070$4301280a@phx.gbl>
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
```

When reading a header in Outlook 2003, you have to start from the bottom and read upward. Most of the lines are pretty logical, but to get a thorough understanding of what happens when an e-mail is sent from one e-mail client to another, we recommend that you read the following article, which does a great job of explaining all you ever want to know about Internet Mail headers: “Reading E-mail Headers,” at www.stopspam.org/email/headers.html.

Notes from the Underground...

Never Trust an Internet Mail Header 100 Percent

Unfortunately, sophisticated spammers and other malicious people know how to falsify most of the header information before you receive it. Since they can use a false name, a false From address, a false IP origination address, and a false Received from line in the header, this means that every single element that should be traceable in the header could be false and is therefore useless in identifying the spammer. This makes the header unreliable for determining the network path and difficult or impossible to use to determine the true sender. How can this

Continued

happen? When these rules for mail transfer were developed in the early 1980s, we lived in a more trusting world.

Luckily, several initiatives are on the horizon to solve problems such as faked headers. One of these is the .mail domain antispam initiative, which you can read more about at the Anti-Spam Community Registry site at www.ascregistry.org (remember to check out the FAQ!). This is a very exciting initiative that any serious Exchange admin should examine further.

Your A** Is Covered If You...

- Take your time examining how the SMTP protocol works when sending e-mail between SMTP servers.
- Examine what authentication method SMTP uses by default.
- Set strict policies for mailbox sizes on your users' mailboxes and mail-enabled groups.
- Know how to test whether your Exchange server has an open relay, either manually using Telnet or by using a Web-based open relay tester.
- Know what e-mail spoofing is all about, and educate your users to prevent e-mail spoofing attacks.
- Know how to read an Internet mail header.

Chapter 5

Securing the Outlook Web Access Server

In this Chapter

With OWA 2003, your organization's users can access their mailboxes using a Web browser. OWA 2003 has come a long way since Exchange 5.5 and 2000; it now looks and feels very similar to the full Outlook 2003 client. If we were to describe all the new, cool features of OWA 2003, we would end up writing several hundred pages, but because this book is about the security aspects of Exchange 2003 and Outlook Web Access, this chapter focuses strictly on OWA security:

- OWA authentication
- Enabling SSL on OWA
- Restricting user access
- Allowing password changes through OWA
- Redirecting HTTP to HTTPS

By the time you reach the end of this chapter, you will have gained a proper understanding of the different authentication methods available in OWA as well as insight into how to secure the OWA 2003 server by enabling SSL, how to control user access, and how to allow users to change their passwords through the OWA interface. To finish the chapter, we show you a little trick on how to redirect HTTP requests to HTTPS. For readers who wonder why we don't have a section on the new and exciting forms-based authentication feature, refer to Chapter 7.

What are we waiting for? Let's get started!

OWA Authentication

To begin, let's look at each of the authentication methods available in OWA 2003.



BY THE BOOK...

The OWA virtual directories (also called *HTTP virtual servers*) allow you to support a collaborative authoring environment. For example, when you collaborate on confidential material, it is important to control who has access to the data. However, if you also want users outside your organization to access public information, you can enable anonymous connections on a separate HTTP virtual server. To restrict user access, you can use several authentication methods, but normally a combination of anonymous access, Integrated Windows authentication, and basic authentication is sufficient.

When you install Exchange 2003, several virtual directories are created under the Default Web Site in Internet Information Services (IIS). By default, the OWA (Exchange) Virtual Directory is configured with basic authentication (no default domain/realm specified) and integrated Windows authentication as the authentication methods. If for some reason you need to change or edit these authentication methods, you should always strive to change any settings through the Exchange System Manager and not through the IIS Manager. If authentication method changes are made in the IIS Manager, Exchange changes them back to the configurations set in the Exchange System Manager every 15 minutes or after a reboot.

OWA Virtual Directories

Before examining each of the available authentication methods, which can be set on the OWA virtual directories, we thought it would be a good idea to give you a short description of each default virtual OWA directory:

- **Exadmin** This directory provides Web-based administration of the HTTP Virtual Server. Among other things, it's used to administer public folders from within the Exchange System Manager. It's also possible to make custom third-party applications communicate with the Exadmin folder. This folder is only

configured for Integrated Windows authentication access (see Figure 5.1).

Figure 5.1 The Exadmin Folder



- **Exchange** The Exchange directory provides mailbox access to OWA clients. By default, this folder is configured with Basic and Integrated Windows authentication access. The Active Directory (AD) domain name is also specified (see Figure 5.2).

Figure 5.2 The Exchange Folder



- **ExchWeb** The ExchWeb folder provides most of the OWA control functionalities. By default, this folder has anonymous

access enabled, but don't let this setting fool you. The subfolder BIN that contains the controls is set to basic and Integrated Windows authentication (see Figure 5.3). Also note that this folder is viewable through only the IIS Manager and not the Exchange System Manager.

Figure 5.3 The ExchWeb Folder



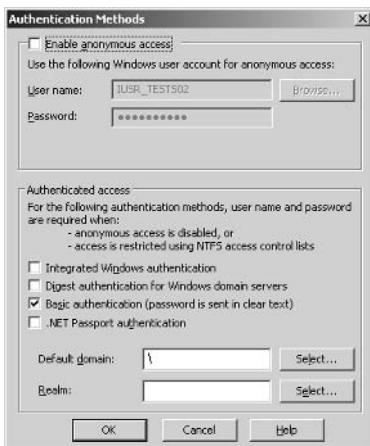
- **Microsoft-Server-Activesync** This directory provides support for wireless synchronization (Activesync) by Microsoft Pocket PCs, smartphones, and the like. The folder is by default set to basic authentication and the default AD domain (see Figure 5.4).

Figure 5.4 The Microsoft-Server-Activesync Folder



- **OMA** The OMA folder provides Web-based mailbox access to Pocket PCs, smartphones, and the like. The folder is set by default to basic authentication and default domain \ (see Figure 5.5).

Figure 5.5 The OMA Folder



- **Public** The Public folder provides users with access to the Public folders. This folder is set by default to basic and Integrated Windows authentication and the default AD domain (see Figure 5.6).

Figure 5.6 The Public Folder



Authentication Methods

By default, the authentication method for accessing OWA is basic and/or Integrated Windows authentication, but actually there are five different authentication methods that can be used to validate your OWA users:

- **Anonymous access** Enabling anonymous connections allows HTTP clients to access resources without specifying a Microsoft Windows 200x user account. Passwords for anonymous accounts are not verified; the password is only logged in the Windows 200x Event Log. By default, anonymous access is not enabled. The server creates and uses the account IUSR_computername.
- **Integrated Windows authentication** The Integrated Windows authentication method is enabled by default (except on front-end servers). This authentication method also requires HTTP users to have a valid Windows 200x user account and password to access information. Users are not prompted for their account names and passwords; instead, the server negotiates with the Windows 2000 security packages installed on the client computer. This method allows the server to authenticate users without prompting them for information and without transmitting unencrypted information across the network.
- **Digest authentication** Digest authentication works only with Active Directory accounts. It's quite secure because it sends a hash value over the network rather than a plaintext password, as is the case with basic authentication. Digest authentication works across proxy servers and other firewalls and is available on Web Distributed Authoring and Versioning (WebDAV) directories. To use this form of authentication, your clients must use Internet Explorer 5.0 or later.
- **Basic authentication** Basic authentication transmits user passwords across the network as unencrypted information. Although this method allows users to access all Exchange resources, it is not very secure. To enhance security, it is strongly advised that you use SSL with basic authentication to encrypt all information. We will show you how to enable Secure Socket Layer (SSL) on your OWA virtual directories in the next section.
- **.NET Passport authentication** .NET Passport authentication allows your site's users to create a single sign-in name and password for easy, secure access to all .NET Passport-enabled

Web sites and services. .NET Passport-enabled sites rely on the .NET Passport central server to authenticate users rather than hosting and maintaining their own proprietary authentication systems. However, the .NET Passport central server does not authorize or deny a specific user's access to individual .NET Passport-enabled sites. It is Web site's responsibility to control user permissions. Using .NET Passport authentication requires that a default domain be defined. You probably know the .NET Passport authentication method from services such as Microsoft's MSN Hotmail and Messenger. Note that this authentication method can be set only through the IIS Manager, not the Exchange System Manager.

As you can see in Figures 5.7 and 5.8, you can set all types of authentication methods on either the HTTP Virtual folders in the exchange System Manager and/or on the OWA virtual directories under the Default Web Site in the IIS Manager. As a general rule, you should set the authentication methods through the Exchange System Manager whenever possible, and through the IIS Manager only as a last resort.

Figure 5.7 Setting Authentication Methods Through Exchange



Figure 5.8 Setting Authentication Methods Through IIS

REALITY CHECK...

Before you start experimenting with OWA configuration options, it's vital that you know the ins and outs of the DS2MB process. DS2MB stands for *Directory Service to Metabase*, a method by which Exchange configuration information in Active Directory is synchronized to the metabase. The function of the DS2MB synchronization process is to transfer configuration information from Active Directory to the local metabase. DS2MB is a one-way process, meaning that you always should make any changes to your OWA directories through the Exchange System Manager and not the IIS Manager. Any changes you make to the Exchange and Public virtual directories via the IIS Manager will be lost once the System Attendant service is restarted (such as after a reboot) or when the DS2MB process kicks in, which is normally every 15 minutes. The reason is that the DS2MB process always overwrites the settings in IIS Manager with the settings that exist in Exchange System Manager.

Read, Write, Browse, and Execute Permissions

In addition to the available authentication methods we've discussed, you can set Read, Write, Browse, and Execute permissions on the various HTTP virtual folders in the Exchange System Manager (see Figure 5.9).

In general, you'll rarely have reason to change the default settings. We will therefore not go into further detail about them in this book, but instead suggest you take a look at the Exchange Help files for any information you require.

Figure 5.9 Read, Write, Browse, and Execute Permissions Through ESM



Connection Limits

By default, an HTTP virtual server accepts an unlimited number of inbound connections (or more precisely, 1000—the default limit set in IIS), but to prevent an Exchange server from becoming overloaded, it's possible to specify a limited number of simultaneous connections. This is done the following way:

1. Open the **Exchange System Manager**.
2. Drill down to **Servers | Server | Protocols | HTTP**.
3. Open the **Properties** of the respective HTTP virtual server.
4. Under the **General** tab, put a check mark in **Limit Number of Connections**.
5. Specify the amount of allowed connection, then click **OK**.



REALITY CHECK...

For some reason, it's not possible to enable the limited number of inbound connections on the default HTTP virtual server in the Exchange System Manager. You can only enable this feature on

additionally created HTTP virtual servers. If you need to set it on the default one, you need to use an identical feature in IIS (more specifically, by right-clicking the **Default Web Site**, then choosing the **Performance** tab).

You can also limit the length of time that idle connections remain logged on to the server, also specified under the General tab. If you don't use forms-based authentication, it could be a good idea to do this to reduce the risk of a malicious person accessing your messaging environment through a running OWA session that a user forgot to disconnect on a kiosk machine or similar.

Notes from the Underground...

OWA 2003 Security Flaw

In November 2003, the NTBugTraq mailing list found a security flaw in OWA 2003. Users who use OWA for Exchange Server 2003 to access their mailboxes could connect to another user's mailbox. An attacker seeking to exploit this vulnerability could not predict which mailbox they would connect to or if they would connect to another user's mailbox at all. The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed through OWA. This behavior occurs when OWA is used in an Exchange front-end server configuration and when Kerberos (the preferred Windows authentication protocol, used whenever possible, and the default protocol used by Exchange Server 2003 between front-end and back-end Exchange servers for OWA) is disabled as an authentication method for the IIS Web site that hosts OWA on the back-end Exchange servers. By default, Kerberos authentication is used as the HTTP authentication method between Exchange Server 2003 front-end and back-end servers.

This vulnerability is exposed only if the Web site that is running the Exchange Server 2003 programs on the Exchange back-end server has been configured not to use Kerberos authentication and OWA is using NTLM authentication. This configuration change can occur when Microsoft Windows SharePoint Services are installed on a Windows Server 2003 server that also functions as an Exchange Server 2003 back end.

Read more about this security issue in Microsoft Security Bulletin MS04-002 at: www.microsoft.com/technet/security/bulletin/MS04-002.mspx.

Enabling SSL on OWA

If you have OWA clients accessing the organization's Exchange 2003 server from an external network, you normally use the basic authentication method, but by default this method transmits all traffic (including user-names and passwords!) between the server and the client in cleartext. Therefore, it's highly recommended that you encrypt the traffic using SSL. In this section, we show you step by step how to create and implement your own SSL certificate using your own certificate authority (CA). Instead of creating your own SSL certificate, you could buy a third-party certificate from a provider such as VeriSign, Thawte, or InstantSSL. If you choose the latter option, the third-party certificate provider typically has the necessary instructions for you install its specific certificate.



BY THE BOOK...

By implementing SSL on your OWA virtual directories, you encrypt the communication between the client browser and the OWA server itself. This means that your OWA users can safely access their mailboxes without you having to worry that either passwords or confidential information in e-mail messages will be intercepted and used by third parties for malicious purposes. If you use the basic authentication method and don't implement SSL, all data transmitted between the client browser and the OWA server will be sent in cleartext and unencrypted, meaning that anyone with a sniffer program could retrieve all information transmitted. As you might guess, this would be quite a security hole. Another benefit of enabling SSL is your users' option to change their passwords through the OWA interface.

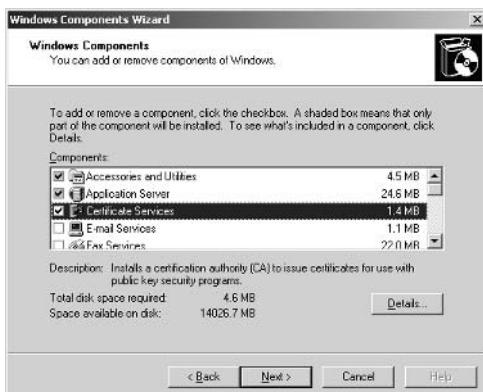
The first thing to do is to decide what server should hold the CA role. This could be any server, but it's recommended that you use at least a member server of your Active Directory domain/forest. Many Exchange admins in small to midsize organizations choose to install it on one of the Exchange servers, which is absolutely fine, especially if you use the Certificate Authority Web Enrollment component, which requires IIS to be installed on the server.

Installing the Microsoft Certificate Service

To install the CA component, log on to the server that's going to hold the CA service, and then do the following:

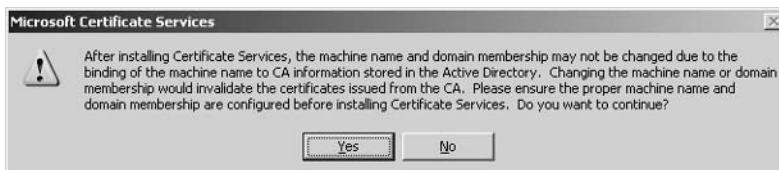
1. Click **Start | Control Panel | Add or Remove Programs**.
2. Select **Add/Remove Windows Components**.
3. Put a check mark in the **Certificate Services** box (see Figure 5.10).

Figure 5.10 Windows Component Wizard



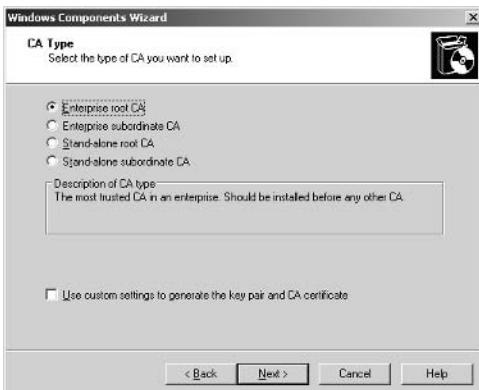
A Microsoft Certificate Services warning dialog box will appear (see Figure 5.11). The box informs you that you cannot change the machine name or the domain membership of the machine while it acts as a certificate server. Read and take note of this message; otherwise, you could end up in quite a mess.

Figure 5.11 Microsoft Certificates Services Warning box



4. Click **Yes**, then click **Next**.
5. Select **Enterprise root CA** (recommended when you have an AD), then click **Next** (see Figure 5.12)

Figure 5.12 Choosing the CA Type



REALITY CHECK...

When dealing with OWA environments, you should typically choose to install an enterprise root certificate service unless a standalone root certificate service is specifically required. We won't go into detail on the differences between the types of CA in this book, but if you want to read more about them, we suggest you take a look at the following two links at Microsoft Technet:

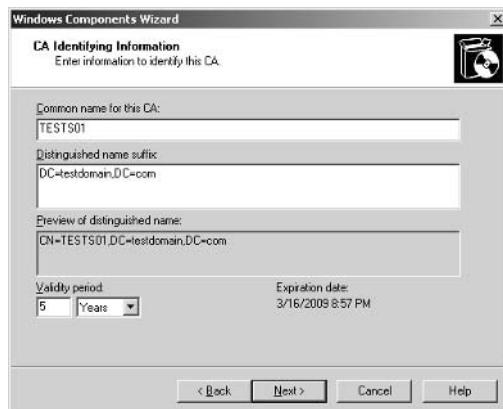
- **Enterprise certification authorities**
[www.microsoft.com/resources/documentation/Windows
Serv/2003/standard/proddocs/en-us/sag_
CSEnterCA.asp?frame=true](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_CSEnterCA.asp?frame=true)
- **Stand-alone certification authorities**
[www.microsoft.com/resources/documentation/Windows
Serv/2003/standard/proddocs/en-
us/sag_CSStandCA.asp?frame=true](http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_CSStandCA.asp?frame=true)

Alternatively, check your CA server's Help file.

In the screen that appears (see Figure 5.13), type in a common name for this CA. The common name of the CA is typically the DNS host name or NetBIOS name (computer

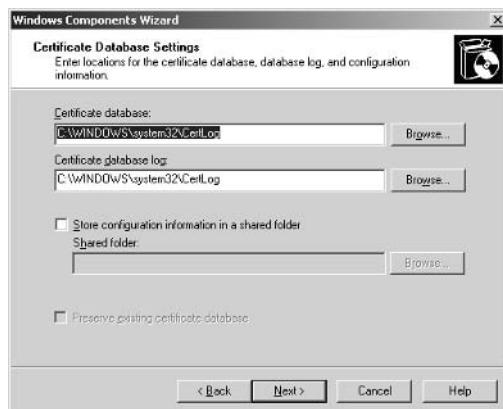
name) of the server running the certificate services. In this specific example, the name of the machine is TESTS01, so we will enter **TESTS01** in the **Common name** field. The default Validity Period of the CA's self-signed certificate is five years, which in most cases should be sufficient, so leave this setting at the default. Click **Next**.

Figure 5.13 Common Name for this CA



6. On the **Certificate Database Settings** page (see Figure 5.14), use the default locations for the Certificate Database and Certificate Database Log. Note that when the server is part of an Active Directory, it's typically not necessary to store configuration information in a shared folder. Click **Next**.

Figure 5.14 Certificate Database and Log Settings



7. Another warning dialog box will appear (see Figure 5.15). This time it informs you that to complete the installation, the IIS must be stopped temporarily. Click **Yes**.

Figure 5.15 Warning Dialog Box



REALITY CHECK

If you haven't enabled Active Server Pages (ASPs) during the IIS installation, a dialog box will notify you that you need to do so if you wish to use the Certificate Services Web enrollment site. The dialog box will then give you the choice of enabling ASPs immediately. If you want to use the enrollment site, click **Yes**.

8. The wizard will now complete the installation of the Certificate Authority Services. Click **Finish** (see Figure 5.16).

Figure 5.16 Completing the Windows Component Wizard



9. Close the **Add or Remove Components** window.

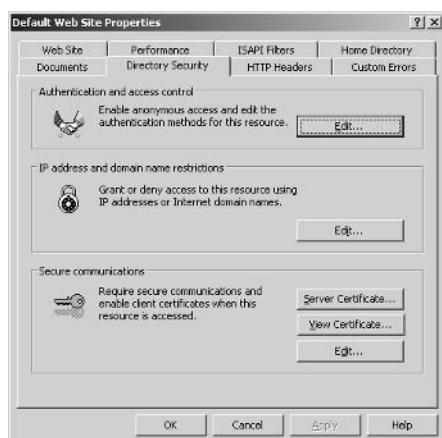
The CA is now installed, and we can issue the necessary SSL certificate to our OWA virtual directories.

Creating the Certificate Request

Now that we have installed the online Certificate Authority Service, it's time to create the Certificate Request for our Exchange 2003 server's default Web site. Do the following:

1. Click **Start | Administrative Tools | Internet Information Services (IIS) Manager**.
2. Expand **Web Sites**, right-click **Default Web Site**, and select **Properties**.
3. Click the **Directory Security** tab (see Figure 5.17).

Figure 5.17 The Directory Security Tab



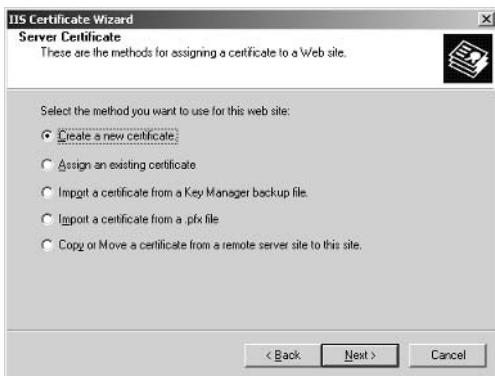
4. Under **Secure Communications**, click the **Server Certificate** button. You will be presented with the Web Server Certificate Wizard screen shown in Figure 5.18. Click **Next**.

Figure 5.18 Web Server Certificate Wizard



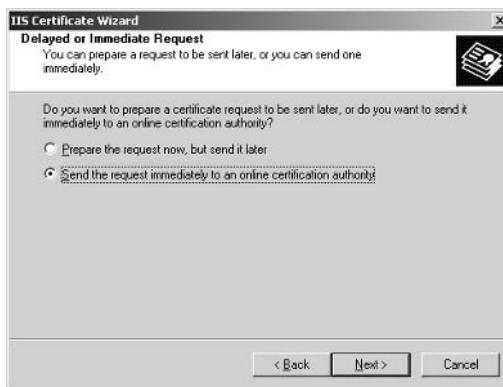
5. Because we are going to create a new certificate, leave this screen to with its default settings (see Figure 5.19). Click **Next**.

Figure 5.19 Create a New Certificate



6. Because we're configuring an online enterprise authority, select the **Send the request immediately to an online certificate authority** option from the **Delayed or Immediate Request** screen (see Figure 5.20). Click **Next**.

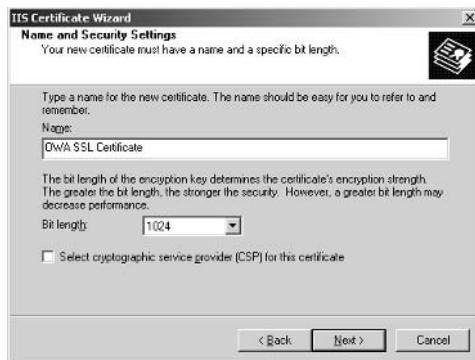
Figure 5.20 Delayed or Immediate Request



7. In the next screen that appears, enter a name for the certificate in the **Name** text box (see Figure 5.21). This is only a descriptive name, meaning it doesn't affect the functionality of the certificate in any way, so enter something that describes the certificate. Because the default bit length key in most situations is sufficient, leave it at its default value of 1024. (This bit length

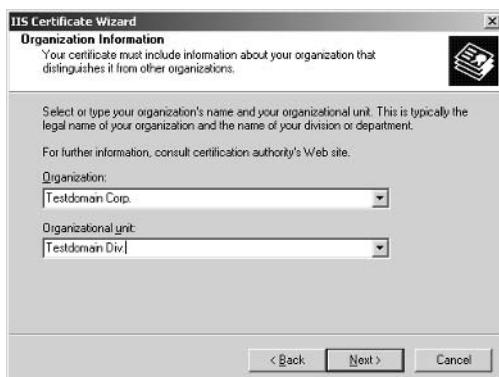
is capable of generating 128-bit encryption, which is what we're going to use.) Click **Next**.

Figure 5.21 Name and Security Settings



8. We now have the option of specifying our organization and organizational unit. Using the defaults is just fine (see Figure 5.22). Click **Next**.

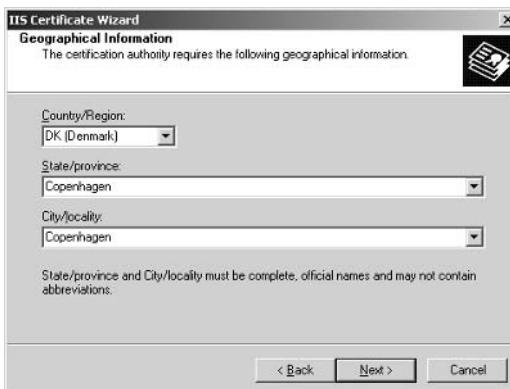
Figure 5.22 Organization Information



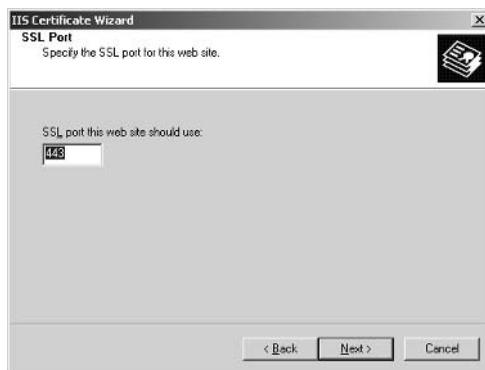
9. In the screen that appears (see Figure 5.23), we need to pay extra attention, since the common name reflects the external fully qualified domain name (FQDN). This is the address external users have to type in their browsers to access OWA from the Internet. If this common name doesn't match the name (FQDN) that the OWA clients connect to, the client will see an error message. Type your site's FQDN in the **Common name** field. Click **Next**.

Figure 5.23 Your Site's Common Name

10. Type your information in the **Country/Region**, **State/province**, and **City/locality** boxes (see Figure 5.24). Click **Next**.

Figure 5.24 Entering Your Geographical Information

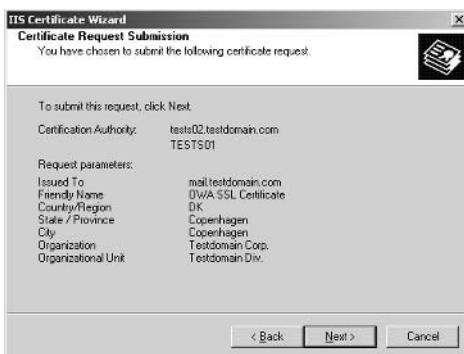
11. We now have the option of specifying the SSL port for the Web site (see Figure 5.25). Because SSL typically uses port 443, leave the defaults. Click **Next**.

Figure 5.25 Choosing the SSL Port

12. In Figure 5.26, select the respective certification authority. Since we only have one in this example, leave the defaults. Click **Next**.

Figure 5.26 Choosing a Certification Authority

13. We now have a chance to review the information we specified throughout the IIS Certificate Wizard. If you find you made a mistake, this is your final chance to correct it. Carefully review the information in the Certificate Request Submission screen (see Figure 5.27), and if you're satisfied, click **Next** and then click **Finish**.

Figure 5.27 Certificate Request Submission

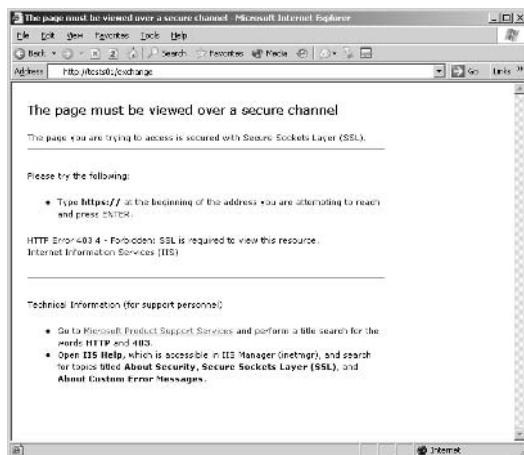
Note: Because the SSL certificates were created using an online CA, SSL has been enabled automatically (see Figure 5.28). If you used a third-party certificate or an offline CA, you would have to manually put a check mark in Require secure channel (SSL) and Require 128-bit encryption.

Figure 5.28 Secure Communications

SSL has now been enabled on our default Web site using our own Enterprise Certificate Service. Let's see if it works as it's supposed to.

14. From a client, launch **Internet Explorer**, then type **http://exchangeserver/exchange**. You should see an error message like the one shown in Figure 5.29.

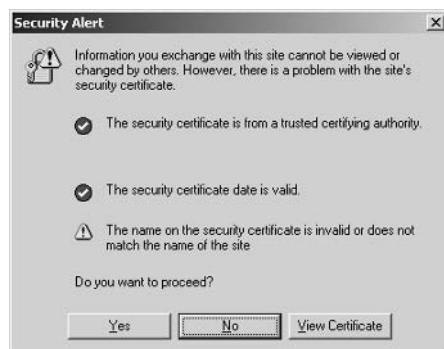
Figure 5.29 This Page Must Be Viewed Over a Secure Channel Error Message



15. Now type **https://tests01/exchange** instead. You will be presented with a Security Alert box like the one shown in Figure 5.30.

Note: The yellow warning icon tells us The name on the security certificate is invalid or does not match the name of the site. This is expected, since during this little test we aren't accessing the site via its common name (mail.testdomain.com).

Figure 5.30 Security Alert Box



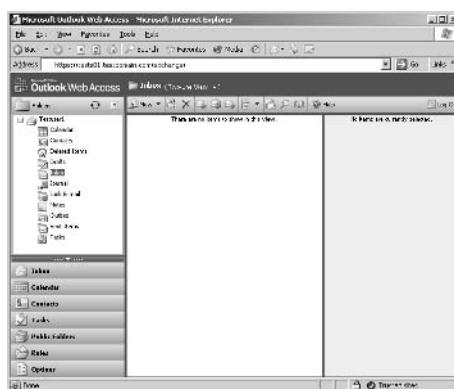
16. Click **Yes**. You will now be prompted for a valid username/password, as shown in Figure 5.31.

Figure 5.31 User Validation Box



17. Enter a valid username and password, and your OWA session will load (see Figure 5.32).

Figure 5.32 Outlook Web Access Session



Notice the little yellow lock icon in the lower-right corner of the screen; this indicates we're viewing a secure site, so fortunately our SSL-enabled OWA site works correctly.

Notes from the Underground...

SSL in a Front-End/Back-End Scenario

Although it's possible to implement SSL on a front-end (FE) server, resulting in all transmitted data between the FE and your client browsers being encrypted, you should be aware that you can't use SSL between any FE and back-end (BE) servers—it simply doesn't work. This means that if your FE server is placed in a perimeter network (also known as a *demilitarized zone*, or DMZ), all traffic between the FE and BE would be unencrypted. So if you're planning such a scenario, consider using IPSec between the FEs and BEs. More and more organizations place their FEs directly on their private networks (and instead place an ISA server or similar in the DMZ), which eliminates this security risk. We will talk more about FE/BE scenarios in Chapter 6.

Third-Party Certificates

In this section so far, we've focused strictly on using certificates issued by our own certificate services authority, but it's important to mention that you also have the opportunity to buy a certificate from a third-party provider such as VeriSign, Thawte, and InstantSSL. In regard to OWA, the primary benefit of buying a third-party certificate instead of creating your own is that it automatically will be trusted by your browser clients, which means the users won't get the dreaded security warning box, similar to the one we saw back in Figure 5.30. You also have the option of having your private certificate trusted by your browser clients, which is done by installing the certificate on each client. If you go that route, you won't get the security warning box either; therefore, third-party certificates are mostly only of interest for service providers and other similar organizations. But keep in mind that if you work in a big corporate OWA environment, it could be a good idea to consider a third-party certificate to decrease support costs, since the security warning box can generate lots of help desk calls.

Restricting User Access

By default, any mail-enabled user in your Exchange organization is allowed access to his or her mailbox using OWA 2003. Depending on the type of organization you have to deal with, you might want to restrict who has access and who doesn't. You might even want to go as

far as disabling the OWA feature completely. In this section we look at the various options available for restricting OWA access.



BY THE BOOK...

Although all users have permissions to access their mailbox through OWA by default, you might run into situations where your organization would want to restrict access. This can be accomplished in several different ways: You can disable access for specific users or by stopping the HTTP virtual server on the Exchange server. In addition, you can go as far as to limit what OWA features should be available to your users. This is done through what is known as *OWA segmentation*.

Disabling OWA Access for a Specific User

Disabling OWA access for a specific user is done through the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in. The following procedure will show you how:

1. Click **Start | Administrative Tools | Active Directory Users and Computers**.
2. Choose **Properties** of a mail-enabled user account.
3. Select the **Exchange Features** tab (see Figure 5.33).

Figure 5.33 Exchange Features Tab



4. Under **Protocols**, click **Outlook Web Access**.
5. Click **Disable** near the bottom of the screen (refer back to Figure 5.33).

You have now disabled OWA for this particular user. Now when this user tries to access his or her mailbox through OWA, he or she will see an “HTTP Error 403—Forbidden” message (see Figure 5.34).

Figure 5.34 HTTP Error 403—Forbidden



Notes from the Underground...

Disable OWA Access on Users in Bulk

Suppose you need to disable OWA access for 500 user accounts. You wouldn't want to do this manually, would you? Don't worry—the nifty little graphical user interface (GUI)-based ADMModify tool comes to the rescue. With ADMModify you can make bulk changes to the attributes for user accounts in your AD forest/domain, and to your advantage, one of the options is to disable HTTP access for them. When you disable HTTP access for a user, that user can no longer access OWA. You can download ADMModify directly from Microsoft Exchange Product Support Services FTP site from the following URL: <ftp://ftp.microsoft.com/PSS/Tools/Exchange%20Support%20Tools/ADMModify>.

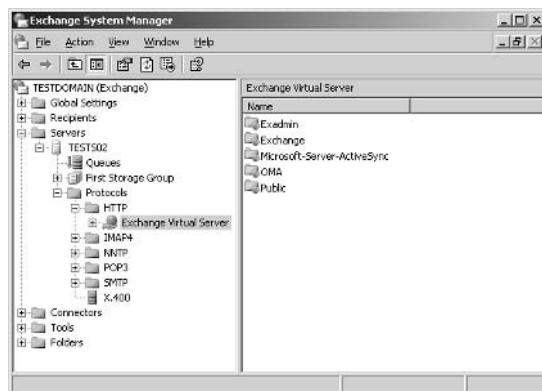
Note: The Microsoft Exchange Product Support Services FTP site contains a lot of other brilliant Exchange utilities, so it's highly recommended that you check out its main FTP folder: <ftp://ftp.microsoft.com/PSS/Tools/Exchange%20Support%20Tools>

Disabling OWA Access for a Server

You might find yourself in situations where your organization doesn't want to allow its users to connect to their mailboxes through OWA at all. If this is the case, the easiest way to accomplish this goal is to stop the HTTP Exchange Virtual Server, as follows:

1. Click **Start | All Programs | Microsoft Exchange | System Manager**.
2. Expand **Servers | Server | Protocols | HTTP** (see Figure 5.35).

Figure 5.35 HTTP Exchange Virtual Server



3. Right-click **Exchange Virtual Server**, then select **Stop**.

A red cross will now appear over the Exchange Virtual Server icon, indicating it has been stopped. Any user will from now on receive a “The Page Cannot Be Displayed” error message when trying to access his or her mailbox through OWA.

OWA Segmentation

With OWA segmentation, it's possible to modify the features that are available in OWA 2003. You could, for example, hide the Tasks, Contacts, or Public folders from the user's OWA interface. OWA segmentation can be done on a per-server or a per-user basis. Per-server segmentation requires that you modify the Windows registry on the Exchange computer. Per-user segmentation requires that you modify an Active Directory attribute.

- **Per-server segmentation** Per-server segmentation in OWA determines the features that are available for all OWA users who are hosted on a particular server that is running Microsoft Exchange Server 2003.
- **Per-user segmentation** Per-user segmentation in OWA determines the features that are available for a particular OWA user or group. Per-user segmentation settings override the per-server value that you configure on the Exchange 2003 server.

We will not go into detail on how you configure OWA segmentation in your Exchange 2003 environment in this book, but instead suggest you read the following Microsoft KB article on this subject: 833340: “How to modify the appearance and the functionality of Outlook Web Access by using the segmentation feature in Exchange 2003,” which you will find at: support.microsoft.com/default.aspx?scid=kb;en-us;833340.

Allowing Password Changes Through OWA

In this section you will learn how to enable the Change Password functionality in OWA 2003.



BY THE BOOK...

Because of Microsoft’s Trustworthy Computing initiative, one of the OWA 2003 things that is disabled by default is the user’s option to change his or her account password through the OWA 2003 interface. As you might remember, this option was enabled by default in Exchange Server 2000, but many organizations actually disabled the feature because, before Windows 2000 Service Pack 4, it was considered quite insecure. Before Microsoft released Windows 2000 Service Pack 4, the technology for changing passwords through OWA (or more specifically, through IIS) was based on HTR files and an ISAPI extension (lsm.dll), which potentially exposes the Web server to quite a security risk because the ISAPI extension (lsm.dll) needed to run under the security context of System. This basically means that if the system is compromised, a hacker could get full control over the local machine.

Now the Change Password functionality has been modified to use Active Server Pages (ASPs), which makes the functionality more secure, since it is run under the configurable security context of the current process (such as DLLHost, which uses the user, IWAM_<MachineName>, by default).

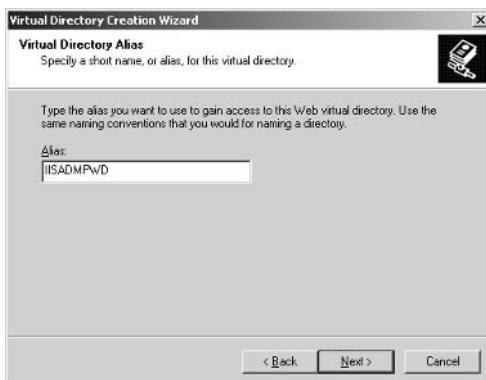
Before adjusting the Change Password functionality in OWA 2003, you first need to implement SSL on your OWA server, as shown earlier in this chapter.

Creating the IISADMPWD Virtual Directory

We first need to create a new virtual directory in the IIS Manager, you should therefore do the following:

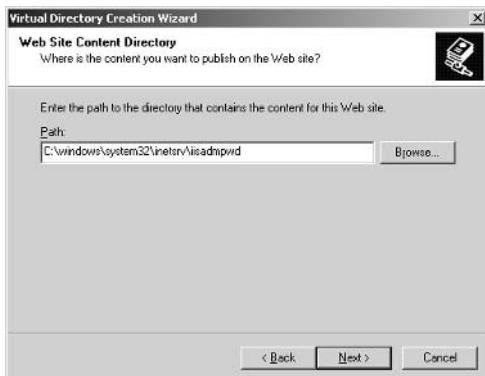
1. Log on to the **Exchange server**.
2. Click **Start | All Programs | Administrative Tools | Internet Services Manager**.
3. Expand **Local Computer | Web Sites**.
4. Right-click the **Default Web Site** and point to **New**, then click **Virtual Directory**.
5. The Virtual Directory Creation Wizard is launched. Click **Next**.
6. In the Virtual Directory Creation Wizard, type **IISADMPWD** in the Alias box, then click **Next** (see Figure 5.36).

Figure 5.36 Virtual Directory Creation Wizard



7. You now need to specify the directory path. Type **C:\windows\system32\inetsrv\iisadmpwd** (see Figure 5.37), then click **Next**.

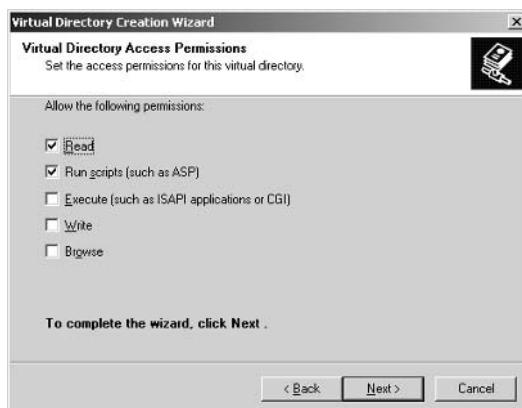
Figure 5.37 Web Site Content Directory



8. Verify that only the **Read** and **Run scripts** (such as ASP) check boxes are set, as shown in Figure 5.38, then click **Next** and then **Finish**.

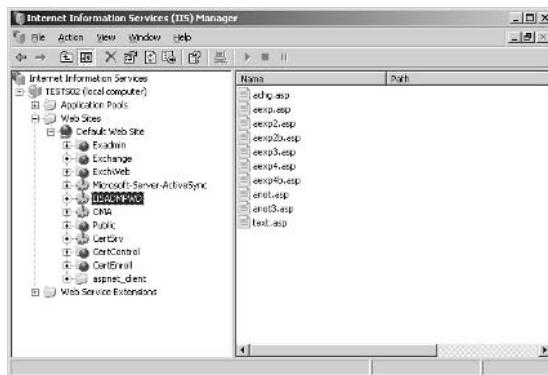
Note: It's important you only give Read and Run Scripts permissions in Step 8. Giving write permissions would allow a potential hacker to replace the scripts with his own versions!

Figure 5.38 Virtual Directory Access Permissions



As you can see in Figure 5.39, we now have a IISADMPWD virtual directory under our default Web sites.

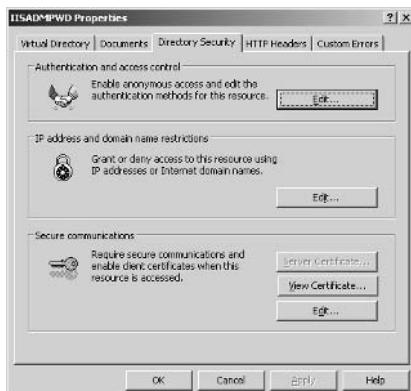
Figure 5.39 IISADMPWD Virtual Directory



We now have to verify that the IISADMPWD virtual directory has anonymous access enabled. Otherwise, we can end up in situations where the client and server go into a so-called *endless loop* when you attempt to authenticate users who are prompted to change an expired password. You can read more about this issue in MS KB Article 275457: “IIS 5.0 May Loop Infinitely When A User Is Forced to Change Their Password,” at: support.microsoft.com/?id=275457.

9. Right-click the **IISADMPWD** virtual directory, then select **Properties**.
10. Select the **Directory Security** tab, and then under **Authentication and access control**, click **Edit** (see Figure 5.40).

Figure 5.40 Directory Security Tab



- Put a check mark in the **Enable anonymous access** box, as shown in Figure 5.41.

Figure 5.41 Authentication Methods



- Click **OK** twice and close the IIS Manager.

If you are running Exchange Server 2003 on a Windows Server 2000-based machine, there is one more thing to do: You need to reset the *PasswordChangeFlags* flag in the IIS 5.x Metabase to zero. This is done the following way:

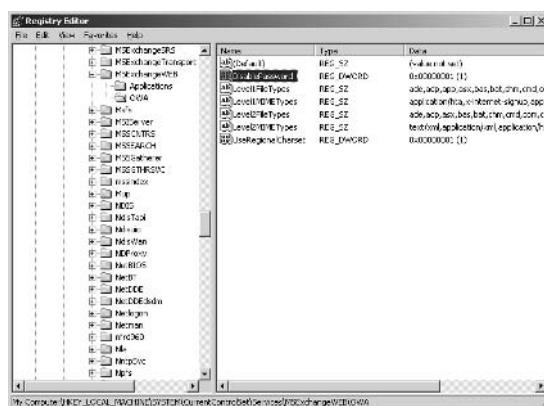
- Click **Start | Run**, and type **CMD**.
- Change to the C:\Inetpub\Adminscripts directory by typing **cd c:\inetpub\adminscripts**, and type **adsutil.vbs set w3svc/passwordchangeflags 0**.

Enabling the Change Password Button in OWA

Now it's time to make the Change Password button visible in OWA. You do this in the registry of the Exchange 2003 server:

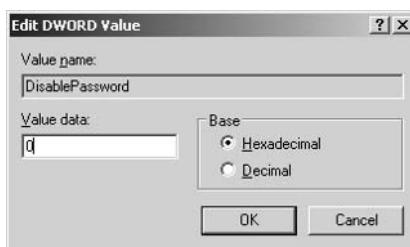
- On the Exchange server, click **Start | Run** and type **Regedt32**.
- Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSEexchangeWEB\OWA** (see Figure 5.42).

Figure 5.42 Enable Change Password in Registry Editor



3. Change the value of **DisablePassword** REG_DWORD from 1 to 0 (see Figure 5.43)

Figure 5.43 Edit DWORD Value



4. Close the registry editor.
 5. Restart the IIS Services—for example, by opening a command prompt and typing **IISRESET**.

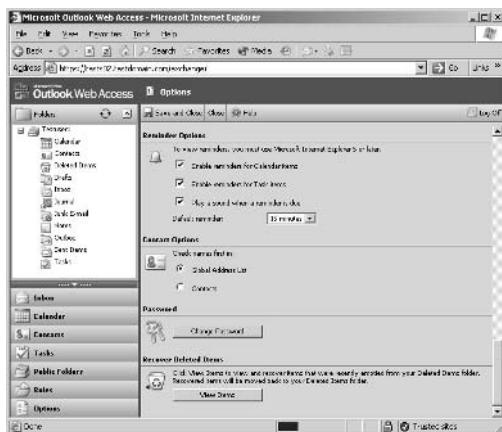
Testing the Change Password Feature in OWA

We now need to check to see if the Change Password option is available, and last but not least, working as it's supposed to:

1. Launch **Internet Explorer**.
 2. Enter the URL to OWA—in this example, **https://mail.test-domain.com**.

3. Log on with your username and password.
4. Click the **Options** button.
5. In the Options window, scroll all the way to the bottom, and click the now visible **Change Password** button under **Password** (see Figure 5.44).

Figure 5.44 Change Password Button



If it works, you will be presented with the window shown in Figure 5.45.

Figure 5.45 Internet Service Manager



6. To test if we are able to actually change a password, fill out the fields with a valid user account, as shown in Figure 5.44, then click **OK**. You should now see a message stating that your password was changed successfully.

Depending on your organization's specific setup, you might experience what is known as *lag time* (delayed change) when users change their passwords. This is especially true if your domain controllers are located at another site than the OWA servers.



REALITY CHECK...

Be aware that if you have installed Exchange Server 2003 on a Windows Server 2000 machine (with SP3 or earlier), on which you also have run the Urlscan 2.5 security tool, you will get an error message when trying to change your password through OWA. The reason is that by default, the Urlscan 2.5 security tool blocks files with the .HTR extension. (Remember, Windows 2000 SP3 and earlier uses the HTR technology for changing passwords.) To resolve this problem, remove .htr from the Deny Scripts section of the urlscan.ini file (by default located in C:\WINDOWS\system32\inetsrv\urlscan). If you plan to install the Urlscan 2.5 security tool on your Exchange 2003 server, there are quite a few things you should take into consideration, so it's highly recommended that you read MS KB article 823175, "Fine-Tuning and Known Issues When You Use the Urlscan Utility in an Exchange 2003 Environment," at <http://support.microsoft.com/?kbid=823175>.

Note: If OWA is installed on a Windows Server 2000 with Service Pack 4 applied or on a Windows Server 2003-based computer, OWA uses the IIS 6.0 ASP Change Password program. Therefore, OWA is not affected by .htr files that are not enabled.

Redirecting HTTP Requests to SSL Requests

Now that we have enabled SSL on our OWA server, your phone is glowing with calls from frustrated users who can no longer access their mailboxes through OWA. What do you do? Make the SSL implementation invisible to your users, of course. In this section we show you how it's possible to automatically redirect HTTP requests to SSL requests, simply by creating a small Web page containing a few snippets of ASP code.



BY THE BOOK...

When using OWA 2003, it's recommended that you require SSL to encrypt or secure the data to ensure that all data is hidden from malicious users. We already discussed how to enable SSL on your OWA site. However, when you configure OWA 2003 to require SSL for all incoming requests, and a request comes in using non-SSL such as `http://mail.testdomain.com`, OWA (or more specifically, IIS) will respond with the following error message similar to the "HTTP 403.4—Forbidden" message: "SSL required Internet Information Services." You know that no matter how much you try to educate your users to type `HTTPS://` instead of `HTTP://`; there will always be some who just don't understand the difference. Therefore, you might want to create an automatic redirection page that translates all HTTP requests (`HTTP://`) to SSL requests (`HTTPS://`).

To accomplish our goal, we need to perform the following steps:

1. Start **Notepad**.
2. Insert the text shown in Figure 5.46 into your Notepad window.

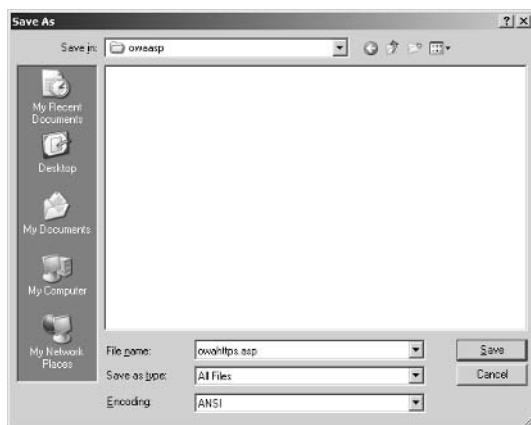
Figure 5.46 Redirect Script in Notepad

```
<% If Request.ServerVariables("SERVER_PORT")=80 Then
    Dim strSecureURL
    strSecureURL = "https://"
    strSecureURL = strSecureURL & Request.ServerVariables("SERVER_NAME")
    strSecureURL = strSecureURL & "/exchange"
    Response.Redirect strSecureURL
End If
%>
```

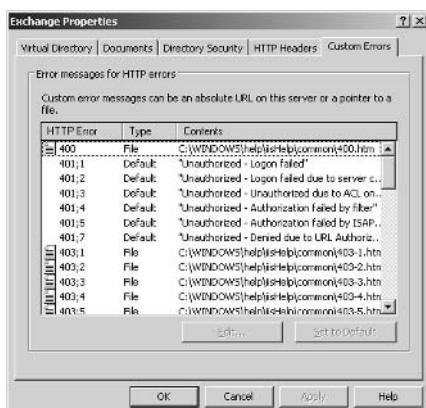
Note: The *SERVER_PORT* and *SERVER_NAME* in this code should not be replaced with an actual server port or server name. They are variables, and the code snippet should be entered as it is shown without modification.

3. Save the Notepad file in your C:\Inetpub\wwwroot\owaasp directory (create the owaasp directory) as owahttps.asp or some other meaningful name (see Figure 5.47).

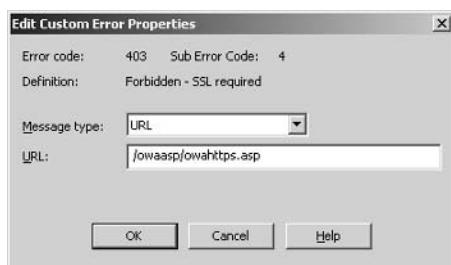
Figure 5.47 Save OWAHTTPS.ASP Page



4. Click Start | Administrative Tools | Internet Information Services (IIS) Manager.
5. Expand Local Computer | Web Sites | Default Web Site.
6. Right-click the Exchange Virtual Directory, then click Properties.
7. Select the Custom Errors tab (see Figure 5.48).

Figure 5.48 The Custom Errors Tab

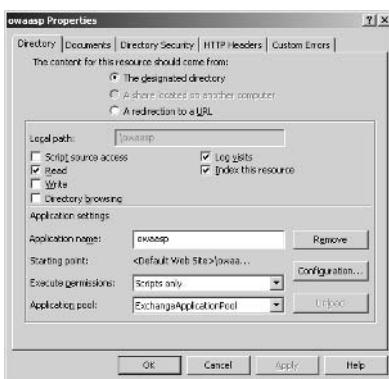
8. Select the **403;4** HTTP error, then click **Edit**. You will now be presented with the box shown in Figure 5.49.

Figure 5.49 Error-Mapping Properties

9. In **Message type**, select **URL**, then type **/owaasp/owahttps.asp** (or whatever you called the ASP page back in Step 3) in the URL text box. Click **OK**.

If you have installed Exchange Server 2003 on a Windows Server 2000-based machine, you only have one thing left to do, and you can jump directly to Step 12. But if you are running Exchange Server 2003 on a Windows 2003 Server, you have an additional task to complete.

10. In the IIS Manager, choose the **Properties** of the **OWAASP** folder.
11. Under **Application Settings**, click **Create**, then select **ExchangeApplicationPool** under the **Application Pool** drop-down box (see Figure 5.50).

Figure 5.50 Select Application Pool

12. Restart IIS, as was shown earlier, by opening a command prompt and typing **IISRESET**.

We can now type **http://mail.testdomain.com** in a Web browser and automatically be redirected to **https://mail.testdomain.com**.

Your A** Is Covered If You...

- Have a general understanding of OWA authentication and permissions
- Enable SSL on your OWA virtual directories
- Know what options you have in regard to restricting user access to OWA
- Set up an automatic OWA redirect page

Chapter 6

OWA Front-End/Back-End Deployment Scenarios

In this Chapter

With Exchange 2000, Microsoft introduced the front-end and back-end (FE/BE) topology, which basically means you have one or more FE servers placed in front of your BE servers. The FE servers' job is to proxy mail client requests to the BE servers. An FE/BE scenario provides your organization with several benefits. To use an FE/BE topology, your organization would typically need to be of a certain size, because the FE/BE topology primarily focuses on organizations with at least two Exchange servers in addition to one or more FE servers—overkill for many small organizations. In this chapter we cover the following topics:

- Deploying a single-server scenario
- Deploying a front-end/back-end scenario
- Securing the front-end server(s)
- Exchange 2003 behind an ISA Server 2000

By the time you reach the end of this chapter you will have a good understanding of the possible scenarios for deploying Exchange in your organization. You will know the benefits and drawbacks of each of the possible deployment scenarios. In addition, you will be shown how to sufficiently secure your FE/BE servers. To finish the chapter, we take a closer look at how introducing an Internet Security and Acceleration (ISA) server to your environment could benefit your Exchange messaging system.

Deploying a Single-Server Scenario

Because many small organizations don't have the budget to invest in an FE/BE solution, most of them still use a so-called single-server scenario, which unfortunately means that these smaller organizations often are more vulnerable than bigger ones—simply because they don't have the same options for securing their Exchange environments.

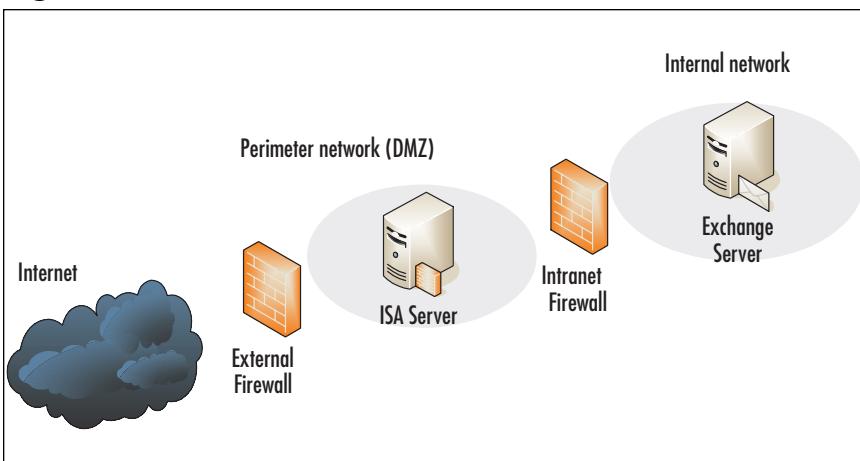


BY THE BOOK...

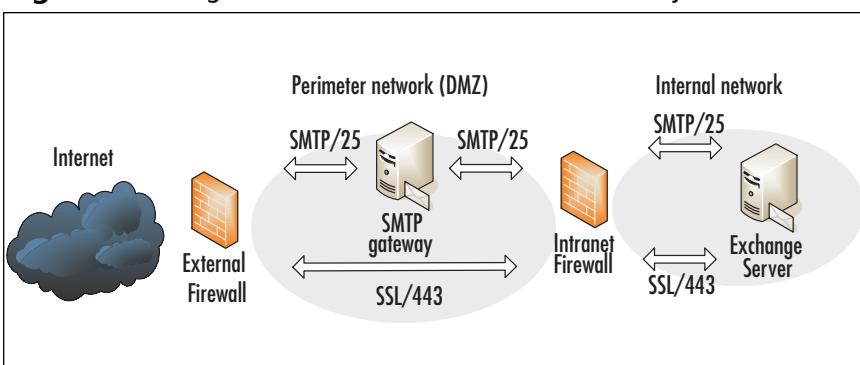
In a single-server scenario, only one Exchange server is involved. This means that users typically connect directly to the Exchange server to access their mailboxes through OWA. This is typically the kind of scenario used by small organizations. The only benefits are that it's the cheapest and easiest solution to implement.

If you plan to deploy a single-server scenario, you should place the server on your internal network. In other words, never deploy the Exchange server directly in the perimeter network (the DMZ) or so it's exposed directly to the Internet. Why not, you might ask? For several reasons: First, since this is the only Exchange server in your organization, it holds all Mailbox and Public folder stores. Second, because the Exchange server must communicate with your Active Directory (AD) domain to process user validation and so on, you would have to open several ports in your intranet firewall to allow access to the domain controllers and Global Catalog servers on your internal network.

The optimal way to deploy your single-server scenario is to place the Exchange server on the internal network and then place an ISA Server in your perimeter network. This way you could publish OWA and all other required mail protocols directly on the ISA server itself (see Figure 6.1).

Figure 6.1 Single-Server Scenario with ISA Server

Because ISA Server is a relatively expensive product in which small organizations often don't have the budget to invest, this scenario is realistic for only a limited number of small organizations. What should the rest do? Because the important thing is to limit the number of exposed ports on the internal Exchange server, you could set up an SMTP gateway in your perimeter network. It doesn't need to run Exchange (it would be overkill to just forward mail); a Windows 2000 or 2003 server would be sufficient, since they both have native SMTP support. You could also set up a UNIX (or UNIX variant, such as FreeBSD or Linux) mail server or something similar; the choice is yours. When implementing an SMTP gateway in a single-server setup, you need to expose only one port on your Exchange server directly to the Internet—port 443 (SSL) or port 80 (HTTP)—if you haven't secured your OWA site with SSL (not recommended, as explained in Chapter 5). This would be required for your external clients to access OWA. Such a setup would look like the one shown in Figure 6.2.

Figure 6.2 Single-Server Scenario with SMTP Gateway

Deploying a Front-End/Back-End Scenario

You have many things to consider when deploying a FE/BE scenario; one of the most important tasks is to decide what type of FE/BE scenario you want to use. Should the FE server be located in the perimeter network (DMZ)? If so, should you use IPSec to properly secure it? Or should you place the FE server on your internal network and then put an advanced firewall such as an ISA Server in your perimeter network (DMZ)? These are some of the issues we look at in this section.



BY THE BOOK...

Deploying Exchange 2003 using an FE/BE topology provides your organization with several benefits. The basic idea is to have FE servers that accept proxies' client requests to the BE servers for processing. An FE/BE topology is recommended specifically for big organizations using multiple Exchange servers and that want to provide OWA (and POP3, IMAP4, etc.) access for their users over the Internet. Besides better security, an FE/BE topology gives us several other benefits such as single namespace, offload processing, and better scalability. As a general rule, one FE server is reasonable for every four BE servers. However, keep in mind that this number is suggested practice, not a rule. It's recommended to use an advanced firewall such as an ISA server in conjunction with an FE/BE topology, but it's not required.

HTTP Authentication

In creating an FE/BE scenario, you have to make several important decisions. One is whether you want to let the FE server authenticate the OWA users or if it should forward the authentication requests to the BE server(s). No matter which method you choose, the BE server(s) will always be involved in authenticating the users. Microsoft recommends that you use *dual authentication*, meaning that both the FE and BE server(s) authenticate the users. This makes sense because when you use this method, users won't be allowed access to the BE server(s) unless they already have authenticated themselves to an FE server. If you choose to implement dual authentication, you must enable basic authentication both on the FE and BE server(s). However, this is true only if the FE

server(s) are located in the perimeter network; if they are located on your internal network, this isn't necessary.

If you don't allow Remote Procedure Call (RPC) traffic from your perimeter network to travel through your intranet firewall, you are forced to forward the authentication requests directly to your BE server(s). This is known as *pass-through authentication*. Needless to say, you should use pass-through authentication only if you don't have the choice of using dual authentication. The reason is that it's considered more secure to allow RPC traffic through your intranet firewall than it is to allow anonymous requests to go directly to the BE servers. If your security policy doesn't allow RPC through the intranet firewall from the perimeter network, you should reevaluate that policy. Some may ask why we advise to allow RPC traffic through the intranet firewall rather than allowing anonymous requests to go directly to the BE servers. Well, think about it: If you allow anonymous requests directly to the BE server(s), anybody—including malicious people—would have direct access to the BE server(s), meaning it would be much easier to hack your network.

Another important thing worth noting is that client authentication by FE servers only supports the Basic authentication method. This is also true between FE and BE servers. Therefore, it's absolutely mandatory to use SSL encryption between the clients and the FE server. If you don't, anybody with a network packet sniffer utility attached to your Internet firewall could sit and watch the content of your inbound/outbound e-mail messages sent via the OWA client. The intruder could also see any usernames and password sent between the client and the FE server.

Using Dual Authentication

To use dual authentication, you need to enable basic authentication on the FE server(s). The following step-by-step instructions show you how to enable basic authentication on an FE server:

1. Open the **Exchange System Manager**.
2. Drill down to **Servers | Server | Protocols | HTTP | Exchange Virtual Server**.
3. Right-click the **Exchange** virtual folder, then choose **Properties**.
4. Click the **Access** tab, then click **Authentication**.
5. Enable **Basic authentication (password sent in clear text)**, as shown in Figure 6.3.

Figure 6.3 Authentication Settings of the Exchange Virtual

6. Click **OK** twice and close the Exchange System Manager.

As you can see in Figure 6.3, it's possible to specify a default domain. It's recommended that you type in your default domain in this field; this will let your users log on to OWA without specifying the domain name, typically by typing **domain\username**. Or you could let your users log in with their user principal names (UPNs) instead. In that case, you would need to type a backslash (\) in the Default domain field. When UPN login has been configured, users are able to log in by typing **user@domain.com** in the Username field.

Note: When you use UPN logins, users can still log in using the format *domain\username*.

If you enabled the new Exchange 2003 feature forms-based authentication, UPN logins will be automatically enabled.

Using Pass-Through Authentication

To configure an FE server to forward the authentication requests directly to your BE server(s)—a process known as *pass-through authentication*—you need to do the following:

1. Open the **Exchange System Manager**.
2. Drill down to **Servers | Server | Protocols | HTTP | Exchange Virtual Server**.
3. Right-click the **Exchange** virtual folder, then choose **Properties**.
4. Click the **Access** tab, then click **Authentication**.

5. Enable **Anonymous access**, then remove the check mark in **Basic authentication** (see Figure 6.4).

Figure 6.4 Configuring a Front End to Use Pass-Through Authentication



6. Click **OK** twice and close the Exchange System Manager.

Securing a Front-End Server

There are several security related tasks to complete when you're securing an FE server. This is especially true if it's going to be placed in the perimeter network, as this makes it more vulnerable than if placing it on the internal network.



BY THE Book...

An Exchange FE server is just a normal Exchange 2003 server that has been designated as an FE server. This is done via Properties of the server in the Exchange System Manager, enabling the **This is a Front-End server** option. Because an FE server typically doesn't have user information stored on it, it provides your organization with an additional layer of security. You can also configure the FE server to authenticate users before they are proxied to the respective BE servers, protecting the BE server from denial-of-service and other attacks. As you'll probably remember, formerly only an Exchange 2000 Enterprise version could be designated as an FE server; this has changed with Exchange 2003. Now you can also dedicate an Exchange 2003 Standard version as a front end, which means that even more small organizations can afford to invest in an FE/BE scenario.

Disabling Unnecessary Front-End Services

After an Exchange server has been configured as an FE server, quite a few services are no longer required to run. Stopping and disabling any unnecessary services is recommended to reduce the number of processes on the FE server and to harden the server against attacks. This is especially true if the server resides on a perimeter network.

Table 6.1 shows you which Exchange services, depending on specific environment, are required or not on an FE server. All other Exchange services except the RESvc (Microsoft Exchange Routing Engine) service can be disabled.

Table 6.1 Exchange 2003 Front-End Services

Service	Conditions under which it can be disabled
Hypertext Transfer Protocol (HTTP)	For OWA to work, the W3SVC (World Wide Web Publishing) service must be running, but no Exchange services require this service.
Simple Mail Transfer Protocol (SMTP)	If hosting Mailboxes/Public folders or using the FE as an SMTP gateway, the Microsoft Exchange Information Store (MSExchangeIS) and Microsoft Exchange System Attendant (MSExchangeSA) services must be running. If you're offering POP3 and/or IMAP4 to your clients, SMTP is also required.
Post Office Protocol version 3 (POP3)	For POP3 access, the POP3 and MSExchangeSA services must be running. Keep this option disabled if you don't have any POP3 clients.
Internet Message Access Protocol version 4 (IMAP4)	For IMAP access, the IMAP4 and MSExchangeSA services are required. Keep this option disabled if you don't have any IMAP4 clients.
Network News Transfer Protocol (NNTP)	Keep this option disabled if you don't offer NNTP (newsgroups) to your users. Note that the service must be enabled during an upgrade.

If you're running the Front-End server on a Windows 2003 server, due to Microsoft's trustworthy computing initiative quite a few services (compared to Windows 2000) are disabled by default. But there are still a few Windows services you might want to disable, such as the Computer Browser, DHCP Client, Distributed File System, Error Reporting, Indexing, File Replication, Help and Support, and Print Spooler.

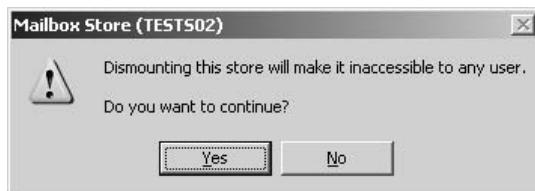
Note: If you're running Exchange 2003 on a Windows 2000 server, there are far more services you should consider disabling. We won't go into detail here on which ones to disable, but instead refer you to the Glossary of Windows 2000 Services on the Microsoft site: www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp, which should be able to assist in your decision.

Dismounting and Deleting the Mailbox Store

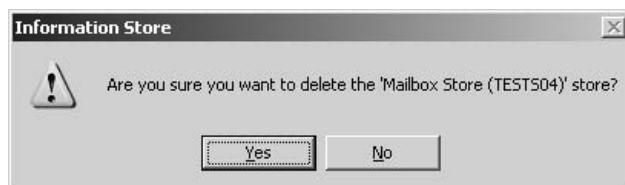
Before placing an FE server in your production environment, it's often a good idea to dismount and delete any Mailbox Store present on it. There are several reasons that you would want to disable a Mailbox Store. First, doing so will make the FE server less vulnerable to attack and will, in most situations, increase server performance. You should dismount and delete the Mailbox Store only if the SMTP service isn't running (or more specifically, used) on the FE server. If you use the SMTP service (for example, if the FE also acts as an SMTP gateway), a mounted Mailbox Store is required, but it doesn't do any harm deleting any mailboxes it contains.

The following step-by-step instructions show you how to dismount and delete the Mailbox Store on an FE server:

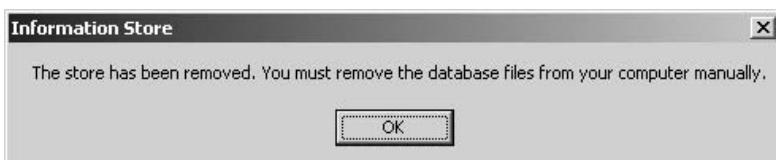
1. Open the **Exchange System Manager**.
2. Drill down to **Servers | Server | First Storage Group**.
3. Check to see whether the Mailbox Store is mounted. If it is, right-click it and select **Dismount Store**.
4. Click **Yes** to message on the screen shown in Figure 6.5.

Figure 6.5 Mailbox Store Warning

5. After the dismount, right-click the **Mailbox Store** and select **Delete**.
6. Click **Yes** (see Figure 6.6), then click **Yes** again (see Figure 6.7).

Figure 6.6 Deleting the Mailbox Store Information Store Warning Box**Figure 6.7** Deleting the Mailbox Store Confirmation Box

7. Click **OK** (see Figure 6.8). The Mailbox Store has been removed.

Figure 6.8 Mailbox Store Removed Information Box

Dismounting and Deleting the Public Folder Store

As is the case with the Mailbox Store on an FE server, it's also a good idea to dismount and remove the Public Folder Store, but again, if your SMTP is running on the FE server, you shouldn't delete the Public Folder Store. The reason is that SMTP depends on the Public Folder Store to provide reliable routing for e-mail messages destined for BE Server Public folders. If you don't have SMTP on the FE server, you can follow these step-by-step instructions, which shows you how the Public Folder Stores are deleted:

1. Open the **Exchange System Manager**.
2. Drill down to **Servers | Server | First Storage Group**.
3. Check to see whether the Public Folder Store is mounted. If it is, right-click it and select **Dismount Store**.
4. You will be presented with the message shown in Figure 6.9. Make note of the information, then click **Yes**.

Figure 6.9 Public Folder Store Replica Warning



5. Click **Yes** in the **Are you sure you want to delete the Public Folder Store** warning box.
6. You receive a screen similar to the one shown in Figure 6.8. Click **OK**.

When you have disabled both the Mailbox Store and the Public Folder Store, you can also stop and disable the Information Store service, but you should bear in mind that if the Information Store service is stopped, you won't be able to do any configuration changes in the IIS Manager. This means that if, for example, you need to configure SSL on the default Web site, you should do so before stopping and disabling this service.

Note: When you have dismounted and deleted any Mailbox Store and Public Folder Store plus stopped and disabled the Information Store,

you might be tempted to deleted the whole Storage Group, but don't! If you do, you will not be able to start the Information Store service if that should ever become necessary.

Front-End Servers in the Perimeter Network

If you decide to place the FE server(s) in the perimeter network (the DMZ), you should be aware that this involves or more specifically requires you to open a fairly large number of ports on your intranet firewall (see Table 6.2). Opening these ports is necessary in order for the FE server(s) to communicate with the domain controllers (DCs), Global Catalog (GC), and Exchange BE server(s) located on the internal network.

Table 6.2 Exchange and Active Directory Ports Required to Be Open on the Intranet Firewall

Ports	Protocol
80/TCP	HTTP. Why port 80? Because even though your OWA clients communicate with the FE server(s) over port 443/TCP (SSL), FE and BE servers don't use SSL to communicate with each other—they communicate over port 80
143/TCP	IMAP4
110/TCP	POP3
25/TCP	Simple Mail Transfer Protocol (SMTP)
691/TCP	Link State Algorithm Routing
389/TCP/UDP	LDAP to Directory Service
3268/TCP	LDAP to Global Catalog Server
88/TCP/UDP	Kerberos authentication
53/TCP/UDP	DNS Lookup

No matter if your FE server(s) are located on in the perimeter network (DMZ) or the internal network, the ports listed in Table 6.3 must be opened on the firewall facing the Internet, also known as the Internet firewall. Of course, this depends on which mail services your clients are using.

Table 6.3 Exchange Ports Required to Be Open on the Internet Firewall

Ports	Protocol
443/TCP	SSL to make secure connections to the FE server(s). If you for some reason haven't implemented SSL, you should instead open port 80/TCP (not recommended!)
993/TCP	SSL Secured IMAP; if IMAP isn't secured you should instead open port 143/TCP
995/TCP	SSL Secured POP3; if POP3 isn't secured you should instead open port 110/TCP
25/TCP	SMTP

Allowing RPC Traffic Through the Intranet Firewall

As mentioned earlier, it's a very good idea to allow RPC traffic through your intranet firewall, since this makes it possible to use dual authentication, meaning that no anonymous users are forwarded directly to the BE server(s). To allow RPC access from the FE server(s) to the Active Directory, you must open two ports, the RPC portmapper and either 1024 and higher/TCP or the single port you specify (see Table 6.4).

Table 6.4 RPC Ports Needed for Authentication Through the Intranet Firewall

Port	Protocol
135/TCP	RPC port endpoint mapper
1024 and higher/ TCP	All service ports

If you don't like the idea of opening port 1024 and all ports above, you have the option of configuring your DCs, GC and any BE server(s) to use a single port for all RPC traffic instead. To restrict Active Directory replications over RPC, do the following:

1. Start the **Registry Editor**.
2. Navigate down to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters**.

3. Modify the TCP/IP port value on each server that the FE servers may contact using RPCs to a specific port such as port 1600.

Note: Even though you specify a specific port for the RPC traffic, port 135 is still required.

Disallowing RPC Traffic Through the Intranet Firewall

When FE server(s) reside in the perimeter network (DMZ) and you choose not to let the intranet firewall allow RPC traffic, you should configure the DSAccess component in such a way that the FE server(s) contact specific DCs and GCs. In order to improve performance, you should as well disable the NetLogon service and Directory Access ping. DSAccess connects to Active Directory servers to check available disk space, time synchronization and replication participation by using the NetLogon service with RPC. If you do not allow RPC traffic over the Intranet firewall, the NetLogon check should be disabled. This is done by creating a *DisableNetLogonCheck* and an *LdapKeepAliveSecs* registry key on the FE server(s).

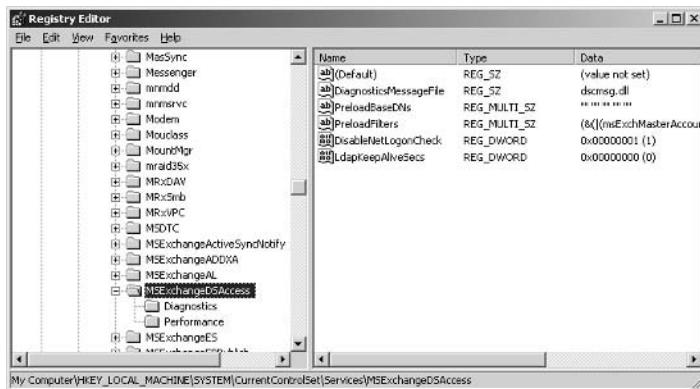


REALITY CHECK...

If your organization doesn't allow RPC traffic to travel through your intranet firewall, you won't be able to support POP3 and IMAP4 clients. The reason here fore is that these two protocols require SMTP to run on the FE server in order to send e-mail. If RPC traffic is blocked it isn't possible to have the MSEchangeIS and the MSEchangeSA services running on the FE server. And as you might know SMTP is dependent on these two services.

To create the *DisableNetLogonCheck* REG_DWORD registry key do the following:

1. **Start the** Registry Editor
2. Navigate down to: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSEchangeDSAccess** (see figure 6.10).

Figure 6.10 *DisableNetLogonCheck* Registry Key

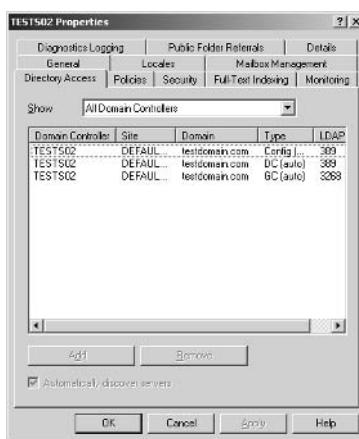
3. In the menu, select **Edit | New | DWORD Value**.
4. Name it **DisableNetLogonCheck**. Make sure to enable it by changing the **0** to **1** in the **Data value** field.

To create the *LdapKeepAliveSecs* *REG_DWORD* registry key, do the following:

1. Start the **Registry Editor**.
2. Navigate down to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\MSExchangeDSAccess** (see Figure 6.10).
3. In the menu, select **Edit | New | DWORD Value**.
4. Name it **LdapKeepAliveSecs**. Make sure **0** is specified in the **Data value** field.

To configure your FE server(s) to use specific DCs and GC servers, do the following:

1. Open the **Exchange System Manager**.
2. Expand **Servers**, right-click the server, then choose **Properties**.
3. Select the **DSAccess** tab (see Figure 6.11).

Figure 6.11 DSAccess Tab in the Exchange System

4. Specify the DCs and GC servers.
5. Click **OK** and close the Exchange System Manager.

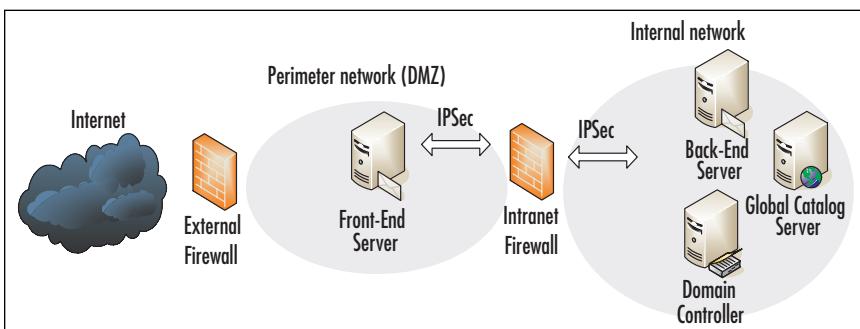
Using IPSec

Any traffic (whether HTTP, POP3, or IMAP4) sent between the FE server(s) in the perimeter network (DMZ) and any server (DC, GC, or BE) with which it communicates are not encrypted. Even though we typically talk about traffic traveling from the perimeter network (DMZ) through the intranet firewall to your internal network, this might be against your organization's corporate security policy. If this is the case, you have the option of implementing IP Security (IPSec), an Internet standard that allows a server to encrypt almost any kind of IP traffic.

Implementing IPSec prevents internal users from sniffing packets and viewing information. If you don't use IPSec, it would actually be possible for an internal user who knows how to use a network packet sniffer to read the CEO's e-mail, which wouldn't be very good—especially because we know who would be blamed if the CEO found out somebody else was reading his or her e-mail.

In Figure 6.12 you can see an example of how an IPSec scenario might look.

Figure 6.12 IPSec Between the Front-End Server and Any (DC, GC, BE) Servers on the Internal Network



You can use two different types of protocols to encrypt IP traffic. Those protocols are:

- **Authentication Header (AH)** AH doesn't encrypt packets; rather, it adds a checksum to each IP packet. The nice thing about AH is that it guarantees a given packet came from the expected host, meaning that it was not impersonated in any way and wasn't modified in transit. AH uses IP protocol 51.
- **Encapsulating Security Payload (ESP)** Opposite AH, ESP encrypts the content of IP packets. ESP uses IP protocol 50.

By implementing IPSec using AH or ESP, you get a reliable and—at least as important—a very secure, trusted communication channel. To allow IPSec communication across your intranet firewall, depending on which protocols you use, you need to open the ports listed in Table 6.5.

Table 6.5 Ports Required to Be Open When Using IPSec

Port	Protocol
IP protocol 51	AH
IP protocol 50	ESP
500/UDP	Internet Key Exchange (IKE)
88/TCP	Kerberos (authentication method used by IPSec)
88/UDP	Kerberos(authentication method used by IPSec)

IPSec uses the standard Internet Key Exchange (IKE) for IPSec negotiations between the servers. Note that IKE uses UDP and not TCP.

Because Kerberos is the preferred security protocol for IPSec, you also need to grant access to port 88/TCP/UDP.

For more detailed information on IPSec, we suggest you read the Microsoft Online Book *Using Microsoft Exchange 2000 Front-End Servers*, which can be download from www.microsoft.com/exchange/techinfo/deployment/2000.

URLScan

You might already be familiar with URLScan (part of IIS Lockdown Tools). If not, we can inform you that URLScan is a small but very efficient utility used to screen all incoming HTTP requests to an IIS server. With URLScan you can improve security on any FE server(s) located in the perimeter network (DMZ) by specifying specific rules and filter requests based on their length, character set, content, and several other factors. You should strongly consider installing URLScan on your FE servers in the perimeter network.

You can download a copy of URLScan from www.microsoft.com/technet/security/tools/urlscan.mspx.

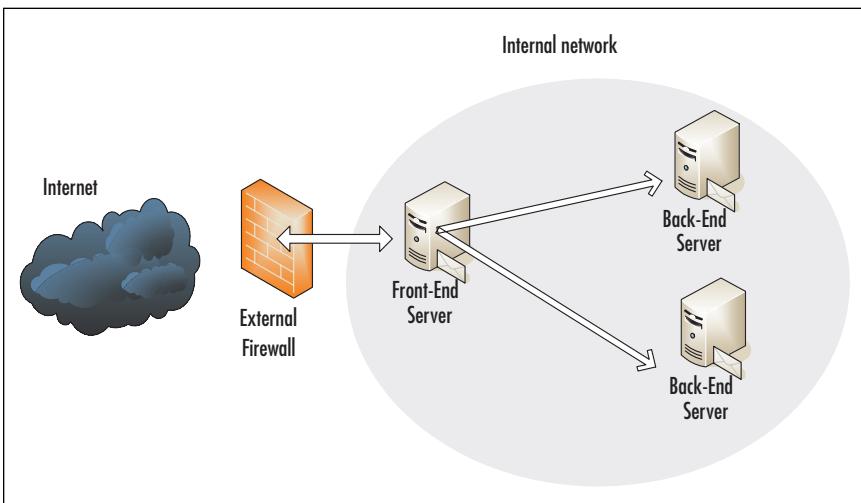
To see specific details on how to tweak URLScan and secure your FE servers even more, we recommend you read the Microsoft Exchange Technical article “Exchange Server 2003 Security Hardening Guide,” which can be found in the Microsoft Exchange 2003 Technical Documentation Library at www.microsoft.com/technet/prodtechnol/exchange/2003/library/default.mspx.

Front-End Servers on the Internal Network

We typically have two scenarios when dealing with an FE server located on the internal network. Figures 6.13 and 6.14 show these scenarios graphically.

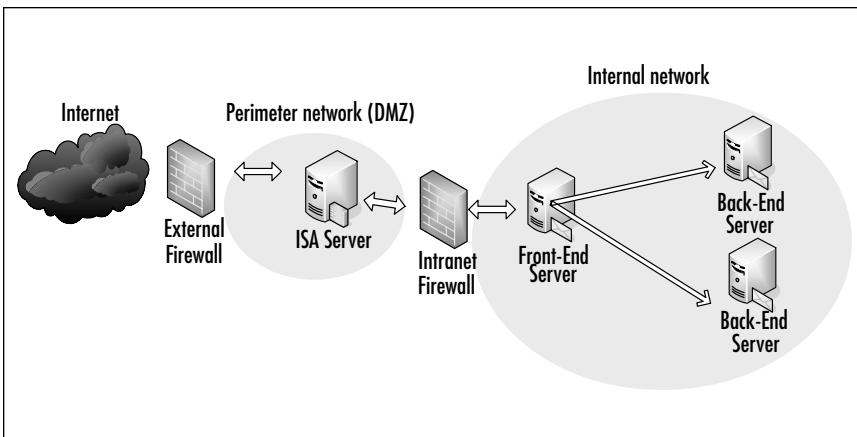
The scenario in Figure 6.13 is one of the most simple to configure. The reason is that all servers are located on the internal network, meaning that you don’t have to worry about RPC traffic. Other benefits of this scenario are the cost savings of not having to maintain a perimeter network (DMZ). But don’t forget, this scenario brings a major drawback as well: If your firewall is compromised, your whole network is exposed. It’s understandable that many small organizations choose this scenario, because they don’t have the budget to invest in two firewalls and maintenance of the perimeter network. But if you can, you should generally avoid this scenario.

Figure 6.13 Front-End Server on Internal Network Behind a Single Firewall



Then we have the scenario in which the FE server is located on the internal network, behind an intranet firewall and facing a perimeter network (DMZ) containing an advanced firewall—in this example, an ISA Server (see Figure 6.14). This is probably the most secure scenario available today. Instead of just doing basic forwarding of mail protocol ports (the way most traditional firewalls do), ISA Server has the ability to inspect and evaluate the communications going on between the e-mail clients and the Exchange 2003 Server(s). This is done through a process known as *application layer filtering*, which involves examining the content of each packet moving between the e-mail clients and the servers. Other security-related benefits of this scenario are protection against unauthorized access and the possibility of configuring alerting of administrators, should an attack occur. You can also restrict access by allowing specific users, groups, application types, time of day, content type, and destination sets.

Figure 6.14 Front-End Server on Internal Network Behind Perimeter Network (DMZ) with ISA Server



Exchange 2003 Behind an ISA Server 2000

This book does not go into detail or provide any step-by-step instructions on how you, using a combination of Exchange 2003 and ISA Server, can provide your organization with an even more secure messaging environment than provided by the traditional FE/BE approach, where the FE server(s) are placed directly in the perimeter network (DMZ). Other good books have been written on this subject, such as Dr. Tom Shinder's *ISA Server and Beyond*, which is also published by Syngress Publishing (ISBN 1931836663). However, we felt it was a good idea to make you aware of the possibilities offered by deploying an ISA Server in your Exchange environment.



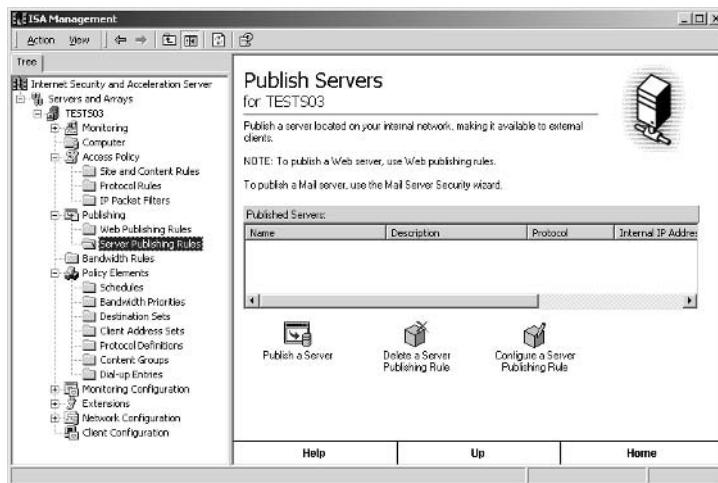
BY THE BOOK...

To provide your organization with a more secure messaging environment, Exchange 2003 has been designed to work better with ISA Server than has been the case with previous versions of Exchange. ISA Server is an advanced firewall that controls Internet traffic entering your internal network and outbound communication from your messaging environment. With ISA Server firewalls, it's possible to allow secure remote access to Exchange Server services on the internal network. An ISA Server protects Exchange Servers on your internal network using several

unique features that you won't find on any other firewall. All inbound Internet traffic destined to your Exchange 2003 servers (such as OWA, RPC over HTTP(S) , OMA, POP3, IMAP4) is processed by the ISA Server. This means that when the ISA Server receives a request from an Exchange server on the internal network, it proxies the requests to the appropriate Exchange server(s). The internal Exchange server(s) then returns the requested data to the ISA Server, and then ISA Server sends the information to the client through the Internet.

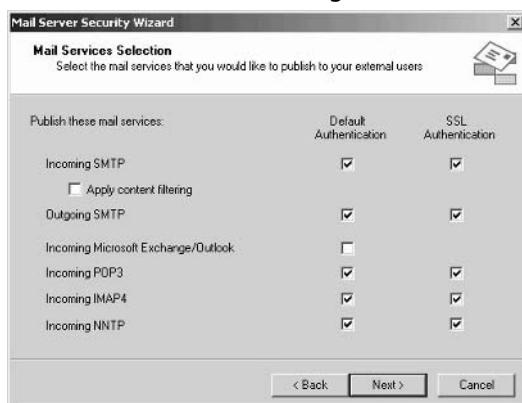
ISA Server is an advanced filtering firewall that can be used in many different ways (see Figure 6.15), but in this section we focus on only a few of the Exchange-related ones.

Figure 6.15 ISA Server Management Console



Publishing the Exchange 2003 Services

ISA Server includes what is known as the Secure Mail Server Publishing Wizard, which allows you to publish all the different Exchange 2003 protocols available (see Figure 6.16).

Figure 6.16 The Secure Mail Publishing Wizard

As you can see in the figure, it's possible to publish SMTP, RPC (MAPI), POP3, IMAP4, and NNTP services. (Notice that you can publish them with SSL authentication.) We can enable **Apply content filtering**, which is an application filter that intercepts all SMTP traffic that arrives on port 25 of the ISA Server computer. The filter accepts the traffic, inspects it, and passes it on only if the rules allow it. The SMTP filter can filter incoming mail based on source user or domain and can generate an alert if mail is received from specific users. The SMTP filter can filter messages based on recipient. (The filter maintains a list of rejected users from whom mail messages are not accepted.)

Message Screener

If you enable the SMTP filter, you can go even further and install what is known as a *message screener*. If you install the message screener, you can even configure the SMTP filter to check for specific attachments or keywords. You can go so far as to specify the size, name, or type of content that should be held, deleted, or forwarded to the administrator. You can also specify that one of those three actions be taken if a keyword is found. In addition, the SMTP filter can check for buffer overrun attacks. A buffer overrun occurs when an SMTP command is specified with a line length exceeding a specific value. The SMTP filter can be configured to generate an alert when a buffer overrun attack is attempted.

OWA 2003 Publishing

As you might have noticed, the Secure Mail Publishing Wizard didn't have any option of publishing OWA. This is because OWA is published in a slightly different way than is the case with the rest of the Exchange

services. To publish OWA, instead of using the Server Publishing rule you have to use the Web publishing rule. After publishing OWA, you will also have to create a Web Listener, among other things.

Notes from the Underground...

ISA Server 2004 Just Around the Corner

You should note that the next generation of ISA Server is in its final stages, which means that at the time of this writing it exists in a beta version. ISA Server 2004, as it's surprisingly been named, provides us with several improvements, such as:

- Unlimited multiple networks and types
- Per-network policies
- Stateful inspection on all network traffic
- Performance-optimized, multilayered filtering engine
- All-new user interface

If you would like a closer look at ISA 2004 and even download a copy of the beta version, be sure to visit the following site: Microsoft Internet Security & Acceleration Server: ISA Server 2004 Beta at www.microsoft.com/isaserver/beta/default.asp.

More ISA Server Information

For more information about ISA Server, we recommend you read the Microsoft Technical article, "Using ISA Server 2000 with Exchange Server 2003," which can be found in the Microsoft Exchange 2003 Technical Documentation Library: www.microsoft.com/technet/prodtechnol/exchange/2003/library/default.mspx.

You should also be sure to visit www.isaserver.org, which contains just about anything you want to know about ISA Server installations, configurations, and the like. One of the regular contributors to the site is Dr. Thomas Shinder, who has written several books on ISA and can be described as a true ISA Server guru.



REALITY CHECK...

Deploying an ISA Server is a rather expensive solution (even though it exists in both a standard and Enterprise version), so unless you are using, for example, a Premium version of Small Business Server (SBS) which includes ISA Server 2000 as well, keep in mind that ISA Server is primarily for midsize to large organizations.

Your A** Is Covered If You...

- Work for a small organization without the budget to invest in an FE server and/or an ISA Server and strongly consider using an SMTP gateway.
- Take your time and examine each type of OWA deployment scenario carefully to choose the scenario that fits your organization best.
- Consider using dual authentication if your organization has one or more FE servers in the perimeter network (DMZ).
- Secure any FE server(s) very tightly, especially if they're located in the perimeter network (DMZ).
- Depending on your organization's size, consider deploying an ISA Server in your environment.

Chapter 7

Outlook Web Access

Client Security Features

In this Chapter

Now that we have Outlook Web Access (OWA) 2003 correctly configured and secured on the server side, it's time to focus on the security features contained in the new OWA 2003 client. OWA has come a long way since its predecessors. The Web mail client introduces several new or enhanced security features such as:

- S/MIME support
- Junk e-mail filter
- Web beacon blocking
- Enhanced attachment blocking
- Forms-based authentication (also known as cookie-based authentication)

The OWA client has finally reached a reasonable security level, which will allow even more organizations to offer Web-based mailbox access to their users.

By the time you reach the end of this chapter, you will have a basic understanding of each new or enhanced security feature included in the OWA client. It will then be up to you to decide which of these features you want to take advantage of in your organization's Exchange environment.

S/MIME Support

OWA now supports Secure/Multipurpose Internet Mail Extensions (S/MIME), which secures Internet e-mail by digitally signing the messages as well as encrypting them. S/MIME for OWA 2003 uses ActiveX controls, which make it possible for clients running Microsoft Internet Explorer 6 with Service Pack 1 (SP1) or later to send and receive S/MIME messages.

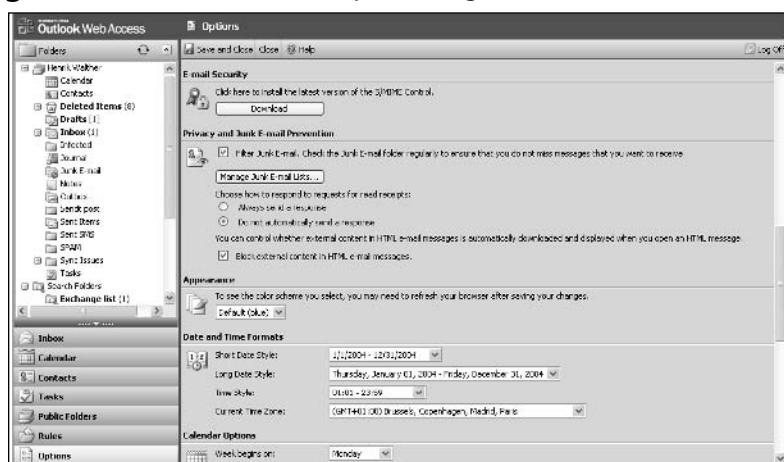


BY THE BOOK...

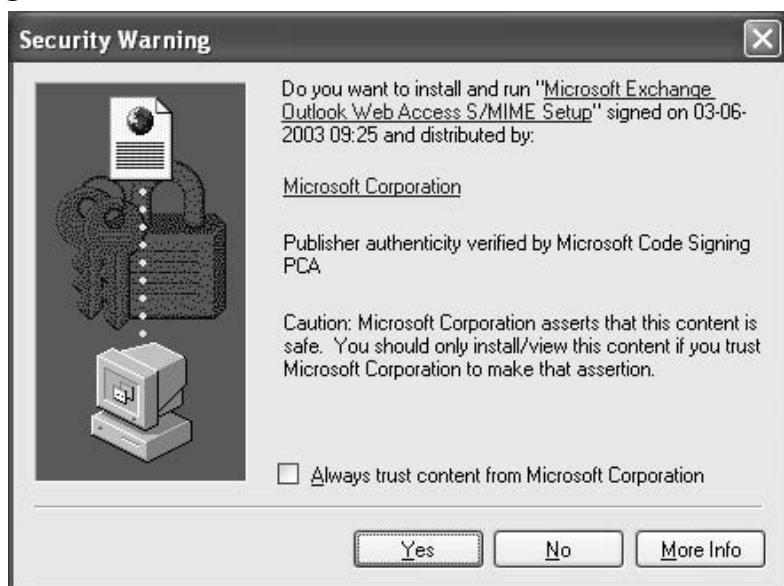
In order for OWA users to use S/MIME, you would either need to use an Enterprise Public Key Infrastructure (PKI) or get a third-party certificate. We will not go into detail on how to install and configure a PKI but will solely go through how we enable the S/MIME option in our OWA client. For specific details on how to deploy a fully functional S/MIME system, read the Microsoft technical article *Quick Start for SMIME in Exchange Server 2003*, which can be found in the Microsoft Exchange Server 2003 Technical Documentation Library at www.microsoft.com/technet/prodtechnol/exchange/exchange2003/proddocs/library/default.asp.

To enable S/MIME in the OWA client, we need to perform the following steps:

1. Launch **Internet Explorer**. Type the URL to OWA, which would normally be something like **www.yourdomain.com/exchange** or **https://mail.yourdomain.com**. Note the *s* in *https*; this is important because we are connecting to a Secure Socket Layer (SSL) secured site.
2. Log on to OWA by entering the username/password of a mail-enabled user account.
3. In the OWA navigation pane, click the **Options** button in the lower-left corner (see Figure 7.1).

Figure 7.1 The OWA 2003 Options Page

4. In the Options page under E-mail Security, click **Download**. You will be presented with a few Security Warning boxes (see Figure 7.2) in which you should click **Yes**.

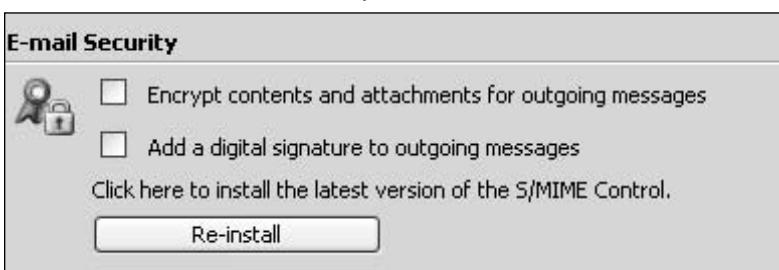
Figure 7.2 S/MIME Security Warning Box

5. Now OWA will start downloading the required DLLs to enable S/MIME on the client (see Figure 7.3).

Figure 7.3 Progress of S/MIME Client Installation

After a few seconds, all the required DDL files will be downloaded and installed, and you will have an S/MIME enabled client machine. The reason we say *client machine* is that S/MIME now is enabled for all OWA users using this specific machine. If a user wanted to log on to OWA on another machine and take advantage of the S/MIME feature, he or she would need to install the S/MIME ActiveX controls again.

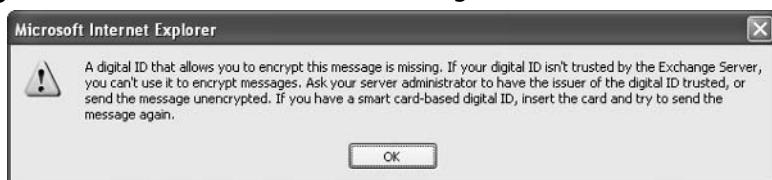
Now that we have properly installed S/MIME, let's look at two new options that have been added under E-mail Security on the OWA Options page (see Figure 7.4).

Figure 7.4 Two New S/MIME Options

If we enable these two options, all outgoing messages sent through OWA from this particular client machine will be encrypted as well as having a digital signature added. If we don't enable the options, there will still be an option of enabling them manually in each new e-mail message. This is done by single-clicking the two buttons to the left of **Options...** before sending the e-mail message (see Figure 7.5).

Figure 7.5 S/MIME Encryption and Digitally Signed E-Mail Message

As mentioned in the beginning of the chapter, you must have a working PKI or install a third-party certificate to take advantage of S/MIME in OWA. If not, you will receive an error message similar to the one in Figure 7.6 when you try to send an e-mail message.

Figure 7.6 S/MIME E-Mail Error Message

REALITY CHECK...

There are still relatively few organizations that encrypt or digitally sign every single e-mail message leaving their messaging environment, but more and more organizations dealing with very confidential information are beginning to require this security measure. Before you decide to implement S/MIME, you should carefully consider whether your organization really needs to encrypt or digitally sign each and every outbound e-mail message.

Junk E-Mail Filter

OWA 2003 finally includes a junk e-mail filter that helps us manage all the spam and other unsolicited e-mail we receive today. The new OWA junk e-mail filter is quite basic and very similar to the one included in the full Outlook 2003 client. The biggest difference between the two clients is that OWA doesn't include the Microsoft SmartScreen-based filtering technology. This means that we, in OWA, have the option of categorizing SMTP addresses as safe senders, safe recipients, or blocked senders.

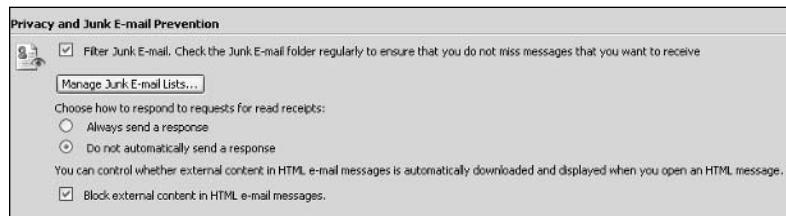


BY THE BOOK...

By enabling the OWA 2003 e-mail junk filter, you will be able to either allow or block specific SMTP addresses. All e-mail filtered by the e-mail junk filter will be moved to a special junk mail folder. A nice benefit of the OWA junk e-mail filter is that it shares its lists with Outlook 2003, so you only have to maintain one junk e-mail filter, even though you use both OWA and Outlook 2003 to access your mailbox.

Follow these steps to manage the OWA junk e-mail filter:

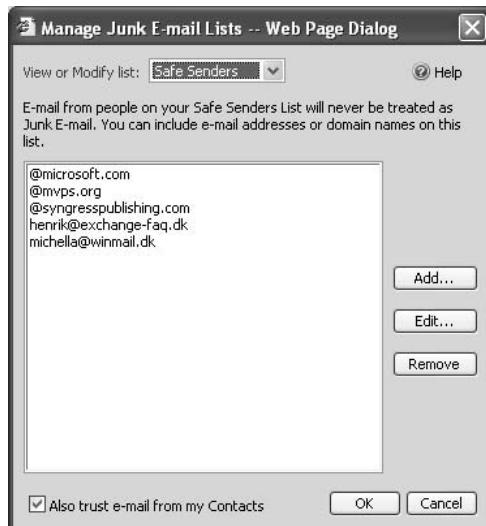
1. Launch **Internet Explorer**.
2. Type the URL to OWA, which would normally be something like **www.yourdomain.com/exchange** or **https://mail.yourdomain.com**.
3. Log on to OWA by entering the username/password of a mail-enabled user account.
4. In the OWA navigation pane, click the **Options** button in the lower-left corner (refer back to Figure 7.1).
5. Under **Privacy and Junk E-mail Prevention** on the Options page, put a check mark in the box next to **Filter Junk E-mail**. **Check the Junk E-mail folder regularly to ensure that you do not miss messages that you want to receive** (see Figure 7.7).

Figure 7.7 Privacy and Junk E-Mail Prevention Options

When you enable the junk e-mail filter, you also activate the **Manage Junk E-mail Lists** button.

6. Click the **Manage Junk E-mail Lists** button.

This choice presents us with the Manage Junk E-mail Lists screen. Notice the **View or Modify list** drop-down box shown in Figure 7.8; this is where you'll choose the appropriate list to be managed.

Figure 7.8 Junk E-Mail Safe Senders List

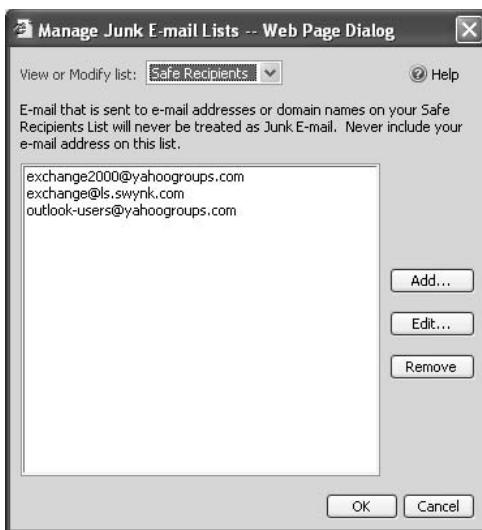
Safe Senders

Safe senders are people and/or domains you want to receive e-mail messages from. E-mail addresses and domains on the Safe Senders list will never be treated as junk e-mail. You can see the Safe Senders option in the View or Modify list drop-down box in Figure 7.8.

Safe Recipients

Safe recipients are distribution or mailing lists that you are a member of and want to receive e-mail messages from. You can also add individual e-mail addresses to your Safe Recipients list. For example, you might want to allow messages that are not only sent to you but also to a particular person. Figure 7.9 shows the Safe Recipients option in the View or Modify list drop-down box.

Figure 7.9 Junk E-Mail Safe Recipients List



Blocked Senders

Blocked senders are people and domains you don't want to receive e-mail messages from. Messages received from any e-mail address or domain on your Blocked Senders list are sent directly to your junk e-mail folder. Figure 7.10 shows the Blocked Senders option selected in the View or Modify list drop-down box.

Figure 7.10 Junk E-Mail Blocked Senders List

When any incoming messages are checked, each junk e-mail filter list gives an e-mail address precedence over domains. For example, suppose that the domain syngresspublishing.com is on your Blocked Senders list (of course, this would never be the case in real life) and the address editor@syngresspublishing.com was on your Safe Senders list. Message from the address editor@syngresspublishing.com would then be allowed into your inbox, but all other messages from e-mail addresses with the syngresspublishing.com domain would be sent to your junk e-mail folder.

Notes from the Underground...

Consider Using a Server-Side Antispam Solution

Even though OWA and Outlook 2003 contain an e-mail junk filter, that is rarely be enough to keep the wolves at bay. If you really want to fight spam effectively, you should, depending on the size of your organization, deploy multiple lines of protection. An efficient way to fight spam is to configure an SMTP gateway and then install an antispam software package on it. If you work for a small organization, you could, as a second option, install the antispam software directly on the Exchange server. You could also use Exchange 2003's built-in connection-filtering feature, but this tool is very limited in functionality, so

we advise you spend some money on a third-party antispam solution. (Server-side antispam solutions are covered in depth in Chapter 9.)

Web Beacon Blocking

OWA 2003 makes it more difficult for spammers sending out junk e-mail to use Web beacons to retrieve valid e-mail addresses. Most spam today is sent out as HTML messages containing one or more embedded beacons. The beacon is often a transparent .gif image embedded in a Web page or an e-mail message's HTML code. The spammer's purpose of using Web beacons is to retrieve valid e-mail addresses. In this section, we take a closer look at how the OWA Web beacon-blocking feature prevents this from happening on your system.



BY THE BOOK...

The OWA 2003 Web beacon-blocking feature helps eliminate the amount of spam you receive by blocking attempts to retrieve valid e-mail addresses through embedded beacons in HTML messages or an e-mail message's HTML code. The Web beacon-blocking feature is enabled by default, just as in the full Outlook 2003 client.

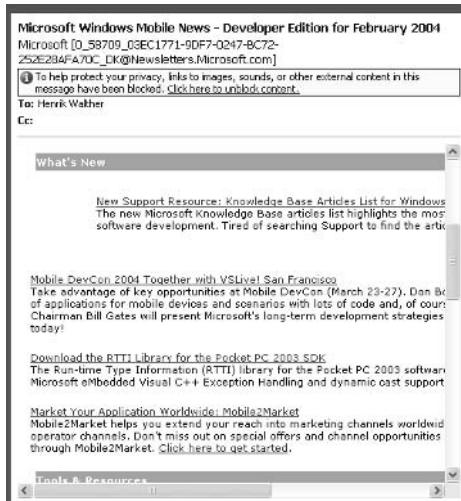
These steps will show you how to enable and disable the OWA Web beacon-blocking feature:

1. Launch **Internet Explorer**.
2. Type the URL to OWA, which is normally something like **www.yourdomain.com/exchange** or **mail.yourdomain.com**.
3. Log on to OWA by entering the username/password of a mail-enabled user account.
4. In the OWA navigation pane, click the **Options** button in the lower-left corner (refer back to Figure 7.1).
5. Scroll down to **Privacy and Junk E-mail Prevention**.
6. Under **You can control whether external content in HTML e-mail messages is automatically downloaded and displayed when you open an HTML message**, activate the Web beacon-blocking feature by putting a check mark

in the box next to **Block external content in HTML e-mail messages** (refer back to Figure 7.6).

Let's look at the Web beacon-blocking feature in action. Figure 7.11 shows a screen dump of a newsletter e-mail message we received. As you can see in the header, the e-mail newsletter contained one or more embedded Web beacons, which the screen shows were blocked.

Figure 7.11 Example of a Blocked Web Beacon Contained in an E-Mail Message



As you can see, it's possible to click the option to **Click here to unblock content** to see the content that was blocked. The Web beacon-blocking feature is a client-side configuration option, but should you need to customize it even further, this would have to be done through a few registry settings on the Exchange server. However, this topic is outside the scope of this book.



REALITY CHECK...

As part of their "secure by default" initiative, Microsoft enabled the Web beacon-blocking feature by default, and there would rarely be a valid reason for this setting to be changed. The feature greatly reduces the amount of received spam because it makes it even harder for spammers to retrieve valid e-mail addresses by embedding Web beacons in a Web page or an e-mail message's HTML code.

Enhanced Attachment Blocking

OWA 2003 also provides an enhanced attachment-blocking feature. We say it's enhanced because this feature in a simpler form has existed in the full Outlook client since Outlook 98 Service Pack 2 (SP2). The feature was introduced in OWA when the Exchange 2000 Service Pack 2 (SP2) was launched.



BY THE BOOK...

Because most viruses today are spread via e-mail worms containing malicious code (such as Bagle and Netsky), it's vital to have a strict attachment-blocking policy. Of course, you should teach your users not to open suspicious e-mail attachments, but as many of us know, no matter how hard you try, there will always be a few users who cannot resist the temptation.

All configuration of the OWA attachment-blocking feature is done on the server side—more specifically, under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWEB\OWA registry subkey (see Figure 7.12).

Figure 7.12 The Attachment-Blocking Option Values in the Registry Editor

Name	Type	Data
ab\{Default\}	REG_SZ	(value not set)
ab\DisablePassword	REG_DWORD	0x00000001 (1)
ab\Level1FileTypes	REG_SZ	ade,adp,app,asx,bas,bat,cmd,com,cpl,crt,csh,exe,fxp,hlp,hta,inf,ins,...
ab\Level1MIMETypes	REG_SZ	application/hta,x-internet-signup,application/javascript,application/x-javasc...
ab\Level2FileTypes	REG_SZ	ade,adp,asx,bas,bat,cmd,com,cpl,crt,dir,dcr,exe,hlp,hta,htm,html,ht...
ab\Level2MIMETypes	REG_SZ	text/xml,application/xml,application/hta,text/html,application/octet-stream,...
ab\UseRegionalCharset	REG_DWORD	0x00000001 (1)

As you can see, OWA 2003 has two levels of file attachment types. Level1 attachments contain file extensions that are not accessible by OWA. Level2 attachments contain file extensions that are accessible but not before they have been saved on the client machine's hard disk. Table 7.1 shows default file extensions in each attachment type.

Table 7.1 Default Level1 and Level2 File Extensions

Default Level	Extension
Level1	ade, adp, app, asx, bas, bat, chm, cmd, com, cpl, crt, csh, exe, ffp, hlp, hta, inf, ins, isp, js, jse, ksh, lnk, mda, mdb, mde, mdt, mdw, mdz, msc, msi, msp, mst, ops, pcd, pif, prf, prg, reg, scf, scr, sct, shb, shs, url, vb, vbe, vbs, wsc, wsf, wsh
Level2	ade, adp, asx, bas, bat, chm, cmd, com, cpl, crt, dir, dcr, exe, hlp, hta, htm, html, htc, inf, ins, isp, js, jse, lnk, mda, mdb, mde, mdz, mht, mhtml, msc, msi, msp, mst, pcd, pif, plg, prf, reg, scf, scr, sct, shb, shs, shtm, shtml, spl, swf, stm, url, vb, vbe, vbs, wsc, wsf, wsh, xml

In addition to the two standard registry keys, you have the choice of adding an extra REG_DWORD value named *DisableAttachments*. This value gives you the option of allowing or blocking all kinds of attachments. Even craftier, it makes it possible to allow all attachments when OWA accesses the Exchange server on the internal network and to block them if the OWA session is established through a front-end server (see Table 7.2).

Table 7.2 Possible Values for the DisableAttachments REG_DWORD Subkey

Value	Result
0	Allows all types of attachments
1	Blocks all types of attachments
2	Blocks all attachments when the OWA session has been established through a front-end server but permit all attachments if the OWA session is done from the internal network

In conjunction with the last option, we can even go as long as to specify specific front-end servers that should permit all types of attachments. You can do this by creating a REG_SZ value named *AcceptedAttachmentFrontEnds*, with a list of the relevant front-end servers specified in the **Data** field.

For more information, see MS KB: 823486, *Administrative and Registry Key Settings for Exchange Server 2003 Outlook Web Access*, at <http://support.microsoft.com/?id=823486>.



REALITY CHECK...

As part of its “secure by default” initiative, Microsoft has enabled enhanced attachment blocking by default in OWA 2003. With the number of e-mail worms containing malicious code that are spreading around the Internet these days, you have no valid reason to disable the enhanced attachment-blocking feature. However, depending on your specific Exchange environment, you might want to adjust the settings for this tool.

Forms-Based Authentication

We finish this chapter by taking an in-depth look at the new and exciting forms-based authentication feature introduced in Exchange 2003. Forms-based authentication is especially useful in kiosk environments, but it can benefit ordinary organizations in several ways, as you’ll see in this section. To take advantage of forms-based authentication, you must already have implemented SSL on your OWA virtual directories.



BY THE BOOK...

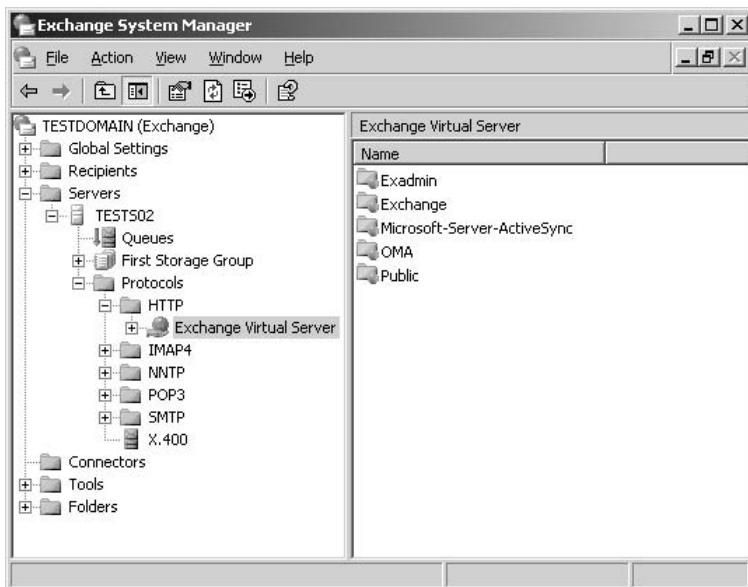
The new OWA 2003 forms-based authentication (also known as *cookie-based authentication*) feature provides your organization with a much more secure OWA infrastructure than was the case with Exchange 2000. When an OWA 2003 user opens a session to the Exchange 2003 server, a special session cookie is created and cached in the browser during the entire OWA session. When the OWA user logs off, the cookie is deleted, which means that we finally have a more secure logoff. Another nifty thing about forms-based authentication is that if an OWA session has been left in an inactive state for a certain amount of time, the session is automatically disconnected.

When forms-based authentication is enabled, users will log on to OWA using a new OWA logon screen. With the new logon screen, a user’s credentials are stored in a browser cookie, or, to be more specific, the user credentials are stored in a *hash*, which then is stored in the cookie.

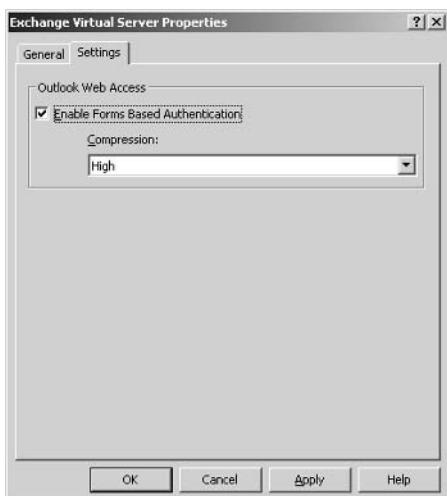
Let's start by enabling forms-based authentication. This is done on the Exchange 2003 server, so to continue we need to perform the following steps:

1. Log on to the **Exchange 2003 server**.
2. Open the **Exchange System Manager**.
3. Navigate to **Servers | Server | Protocols | HTTP | Exchange Virtual Server** (see Figure 7.13).

Figure 7.13 HTTP Exchange Virtual Server



4. Right-click the **Exchange Virtual Server** and click **Properties**.
5. Select the **Settings** tab.
6. Put a check mark in the box next to **Enable Forms Based Authentication**. See Figure 7.14.

Figure 7.14 The Settings Tab for Forms-Based Authentication

As you can see in Figure 7.14, there's a Compression drop-down box, in which you can choose among **None**, **Low**, and **High**. You might wonder what compression has to do with forms-based authentication; the answer is relatively short—nothing. The reason that the compression option is located under the Settings tab is that to work, it requires that forms-based authentication is enabled. The compression feature can provide OWA performance improvements of nearly 50 percent for most actions on slow network connections, so it's definitely worth enabling it if you are struggling with a slow network. (Note that the compression feature uses Gzip encoding and therefore works only with Internet Explorer 6.0 or later and Netscape Navigator 6.0 or later.)

7. Click **OK** and close the **System Manager**, then log off the **Exchange 2003 server**.

We have now enabled forms-based authentication and are ready to take a closer look at this exciting feature.

8. Launch **Internet Explorer**.
9. Type the URL to OWA, which would normally be something like **www.yourdomain.com/exchange** or **https://mail.yourdomain.com**. You are presented with the new forms-based authentication logon screen, shown in Figure 7.15.

Figure 7.15 The Forms-Based Authentication Logon Page



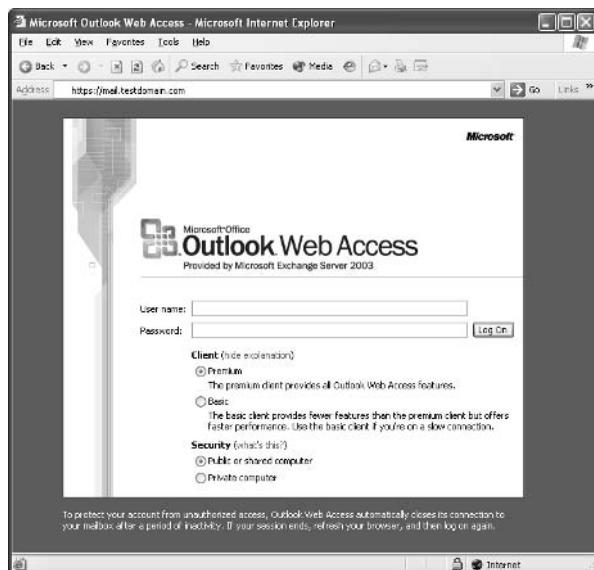
Now let's take a look at each function included on the new logon screen.

Username and Password

The fields Username and Password shouldn't need any explanation, but it's worth noting that when forms-based authentication is enabled, the **Default Domain** setting on the Exchange virtual directory is set to \, which makes it possible for your users to log on to OWA using their *user principal names (UPNs)*.

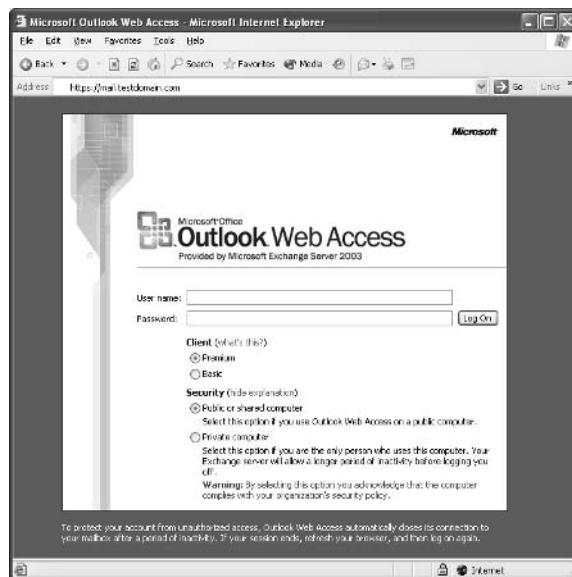
Clients: Premium and Basic

In Exchange 2003 we have two types of OWA clients: a Premium client and a Basic client. In earlier versions of Exchange, these were known as the *rich client* and the *reach client*. The concept is still the same, though; the Premium client provides a more feature-rich user interface (it looks and acts very similar to the full Outlook 2003 client) than the Basic client. To be able to use the Premium client version, the client must at least have Internet Explorer (IE) 5.01 installed. The Basic client can be used with almost any other browser, such as Netscape Navigator, Mozilla, Opera, and Internet Explorer 4.0 and so on (see Figure 7.16).

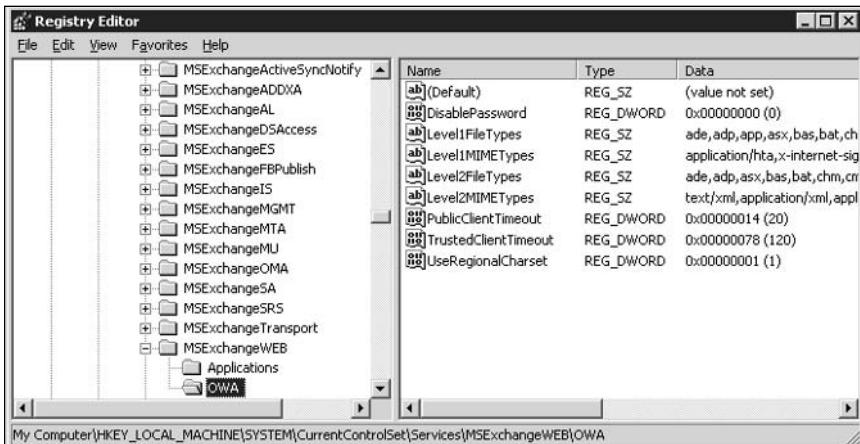
Figure 7.16 Forms-Based Authentication Logon Page Client Options

Security: Public or Shared Computer and Private Computer

From a security point of view, we've now reached the most interesting part of the new forms-based authentication logon screen (see Figure 7.17)—that is, security, whereby we can choose between **Public or Shared Computer** (Internet café and other public computers) and **Private Computer** (home computer, office computer and so on). The difference between the two types of options is the inactivity period before the OWA session with the Exchange server times out. For public or shared computers, the default timeout is 15 minutes; for private computers, it's 24 hours.

Figure 7.17 Forms-Based Authentication Logon Page Security

If you for some reason should have any special need for changing the default values, this can be done by adding two registry *REG_DWORD* values on the Exchange 2003 server, as shown in Figure 7.18.

Figure 7.18 Public or Shared Computer and Private Computer Timeout Values in the Registry Editor

The public or shared computer is at: HKLM\System\CurrentControlSet\Services\MSEExchangeWEB\OWA\PublicClientTimeout.

The private computer is located at: HKLM\System\CurrentControlSet\Services\MSExchangeWEB\OWA\TrustedClientTimeout.

The data values are in minutes. The minimum value is 1 (minute) and the max value is 4320 (30 days). To read more about OWA cookie session timeouts, see MS KB: 823486, *Administrative and Registry Key Settings for Exchange Server 2003 Outlook Web Access* at <http://support.microsoft.com/?id=823486>.

It's worth noting the Forms-based Authentication timeout values aren't as precise as you might expect. The timeout will always occur between the specified value and $1.5 \times <\text{setting}>$. This means that if you set the timeout to occur after 60 minutes, for example, it will actually happen somewhere between 60 and 90 minutes. As mentioned previously, this is also the case for the default Basic and Premium timeout values set to 15 minutes and 24 hours, respectively. So, in the real world, the timeout for the Basic client will happen between 15–25 minutes and the timeout for the premium client between 24–36 hours.

REALITY CHECK...

Even though Microsoft developed the forms-based authentication feature specifically with Internet kiosks in mind, private organizations may very well benefit from implementing the feature. But keep in mind Microsoft suggests that you upgrade all front-end and back-end servers to Exchange 2003 before using this feature.

Notes from the Underground...

Why It Might Not Always Be a Good Idea to Enable Forms-Based Authentication

If your organization uses front-end server(s) placed directly in a perimeter network (also known as a *demilitarized zone*, or DMZ), it might not always be a good idea to deploy the forms-based authentication feature. Forms-based authentication uses the Basic authentication method, which means that any front-end server(s) in a perimeter network must have access to send Remote Procedure Calls (RPCs) to the Active Directory on the private network. Of course, you could use IPSec or other protocols, but you should nevertheless definitely examine your front-end

Continued

topology, before enabling forms-based authentication, since it could cause a potential security hole.

Your A** Is Covered If You ...

- Give yourself time to understand each of the new security features included in OWA 2003.
- Surveys your requirements, identifying the OWA security features your Exchange environment needs.
- Carefully test a given security feature in a test lab before messing with it in your production environment.
- Make sure that you are fully aware of the difference between a public or shared computer and a private computer in regard to forms-based authentication.

Chapter 8

Exchange Protocol/ Client Encryption

In this Chapter

Now that we have secured most of the components of your Exchange 2003 Messaging environment, this chapter will explore securing the communication between your servers and clients by using encryption. Not every organization's security policy demands that all communication is encrypted, but you should get acquainted with its implementation. We will also take a closer look at the new Remote Procedure Calls over Hyper Text Transfer Protocol (RPC over HTTP) feature introduced in Exchange 2003.

In this chapter, we explore the following topics:

- Encrypting SMTP traffic
- Encrypting POP3 and IMAP4 traffic
- Securing clients using S/MIME
- Configuring and securing RPC over HTTP(S)

By the time you reach the end of this chapter you will know how to secure SMTP and POP3/IMAP4 traffic by enabling encryption. In addition, you will be shown where you configure the S/MIME settings in an Outlook 2003 client. To finish the chapter, we give step-by-step instructions on how to use the new, exciting Remote Procedure Calls over Hypertext Transfer Protocol (RPC over HTTP) Exchange 2003 feature.

Encrypting SMTP Traffic

If you're really serious about protecting e-mail traffic in your Exchange messaging environment, you might want to enable Transport Layer Security/Secure Socket Layer (TLS/SSL) on your Exchange 2003 SMTP virtual server(s) in your organization. This feature can encrypt the SMTP traffic between the clients and the server. If you are concerned about SMTP traffic being intercepted on the network, we recommend using IPSec between Exchange servers. IPSec can be used to encrypt not only the SMTP traffic but also LDAP queries to domain controllers and global catalog servers.



BY THE BOOK...

All message systems are vulnerable to information being intercepted on the network through the use of a sniffer-type device, and Exchange 2003 is no exception. The degree of difficulty that an intruder encounters when analyzing e-mail traffic depends on the type of client being used. Outlook clients using MAPI over RPC can transmit data in an encoded format, but (by default) the data is not encrypted. When encoding MAPI over RPC data, the recipient's and sender's names may be in clear text, but the message body and attachments are encoded. Only the more elite intruders would be able to use this encoded information. However, SMTP Internet is astoundingly easy to intercept, and it is also easy to view the data. Even though the message is Multipurpose Internet Mail Extension (MIME) encoded, the message text is easily decoded using a Base64 encoding/decoding program.

Configuring SMTP with TLS/SSL

To configure TLS/SSL on our SMTP virtual servers, we need to create an SSL certificate. This process is very similar to creating an SSL certificate for an HTTP virtual server (OWA). In Chapter 5, we showed you how you get an SSL certificate from a CA. So if you haven't already installed a CA, you should do so now by following the step-by-step instructions in Chapter 5.

To obtain and install an SSL certificate from the CA for use on our Exchange 2003's SMTP virtual server, do the following:

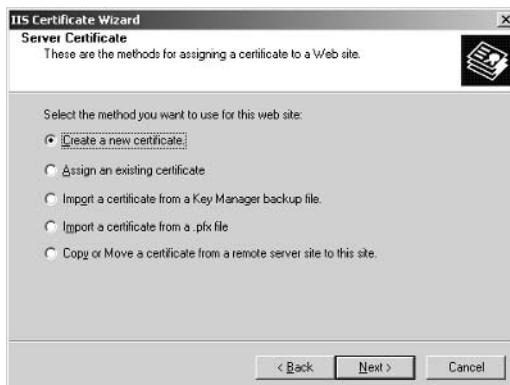
1. On the Exchange server, open the **Exchange System Manager**.
2. Drill down to **Servers | Server | Protocols | SMTP**.
3. Right-click **Default SMTP Virtual Server**, then select **Properties**.
4. Select the **Access** tab (see Figure 8.1), then click the **Certificate** button.

Figure 8.1 Properties of the Default SMTP Virtual Server



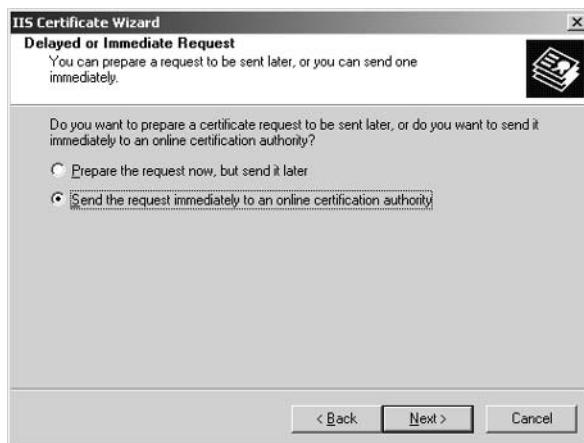
5. In the Web Server Certificate Wizard, click **Next**.
6. Because we are creating a new certificate, select **Create a new certificate** (see Figure 8.2), then click **Next**.

Figure 8.2 Selecting to Create a New Certificate



7. Because we have an internal online CA available, select **Send the request immediately to an online certification authority** (see Figure 8.3), then click **Next**.

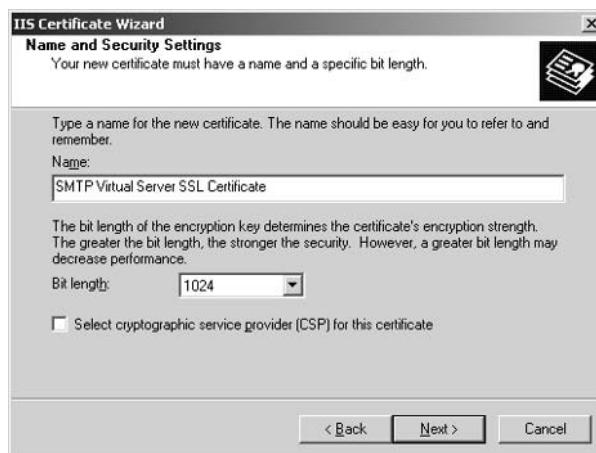
Figure 8.3 Delayed or Immediate Request



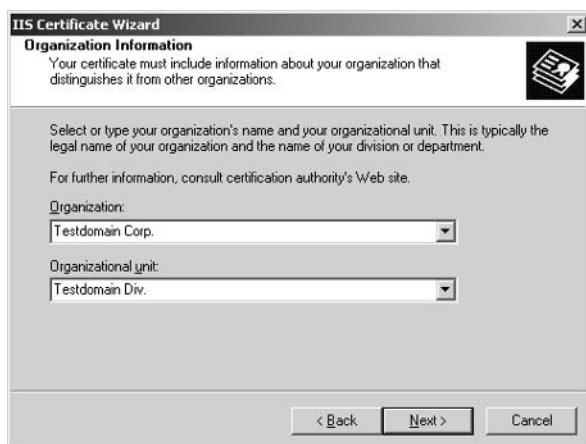
8. Give the certificate a name (see Figure 8.4), then click **Next**.

Note: It's also possible to specify a bit length, but because the default (1024) should be sufficient in most situations, leave the default as it is.

Figure 8.4 Name and Security Settings



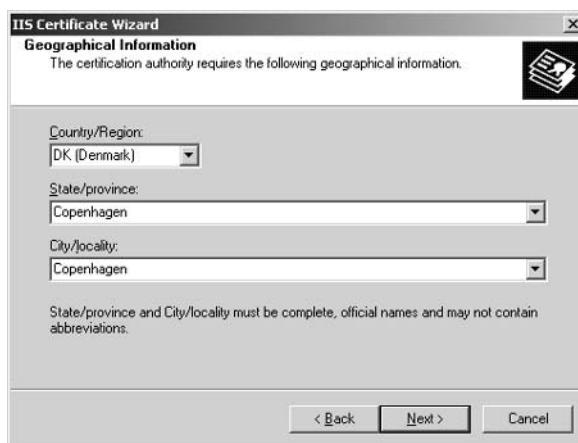
9. Specify your organization and organizational unit (see Figure 8.5), then click **Next**.

Figure 8.5 Organization Information

10. It's time to specify the common name of the SSL certificate (see Figure 8.6). This name should be the external FQDN of the server. By *external* we mean as it appears on the Internet. This server internal FQDN is, for example, tests02.testdomain.com, but its external FQDN is mail.testdomain.com. When you have specified a name, click **Next**.

Figure 8.6 Your Site's Common Name

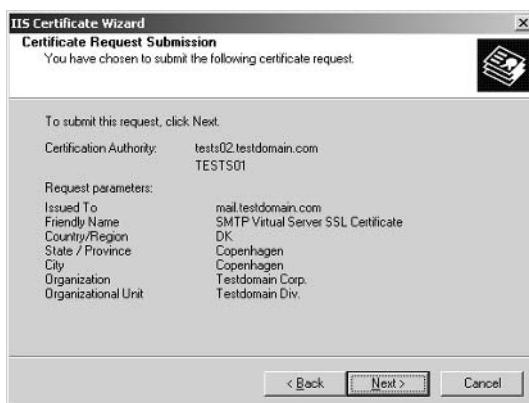
11. Specify country/region, state/province, and city/locality as you want them to appear on the certificate (see Figure 8.7), then click **Next**.

Figure 8.7 Geographical Information

12. We need to select the online CA we want to use (see Figure 8.8). This step shouldn't be very hard because we only have one, so just click **Next**.

Figure 8.8 Choose a Certificate Authority

13. We now see a summary of the information specified through the wizard (see Figure 8.9). This is your final chance to jump back, if you need to make any corrections. Otherwise, click **Next**, then click **Finish**.

Figure 8.9 Certificate Request Submission

Notes from the Underground...

Using a Third-Party Certificate

Note that if you use a third-party certificate such as VeriSign (www.verisign.com), Thawte (www.thawte.com), or InstantSSL (www.instantssl.com), the process of issuing the SMTP SSL certificate is slightly different, but normally the third-party providers have good, detailed documentation available on their Web sites.

Now that you've created the SMTP SSL certificate, we can move on. Let's now discuss the three methods of using the TLS/SSL. We can secure our SMTP traffic on inbound mail, on outbound mail, or for specific domains or one or more in conjunction.

Enabling TLS/SSL for Inbound Mail

Still under the **Access** tab of the Default SMTP Virtual Server's **Properties**, you can see that the **Communication** button has been activated. (In Figure 8.1 you can see it was grayed out before we created the SSL/TLS certificate.). This is where we can enable TLS/SSL for all inbound SMTP mail received by this SMTP virtual server, so do the following:

Warning: Before you enable this setting, you should be sure that any servers communicating with this one support TLS. If they don't, they won't be able to negotiate and therefore can't deliver any e-mail messages to this server. So be very careful with this setting.

1. Click the **Communications** button.
2. We get the screen shown in Figure 8.10. Enable both **Require secure channel** and **Require 128-bit encryption**, then click **OK**.

Figure 8.10 Enabling TLS



Notes from the Underground...

Performance Load When Enabling TLS/SSL

Enabling TLS/SSL on an SMTP Virtual Server can increase performance load on the server, so, depending on how overloaded your Exchange 2003 server is, you might want to reconsider enabling this feature. Do you want a slow Exchange server with tight security or a less secure Exchange server that performs well? The decision is yours.

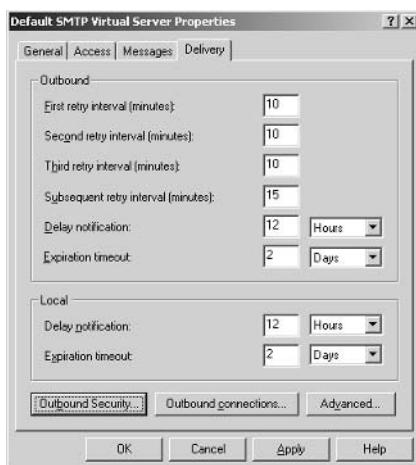
Enabling TLS/SSL for Outbound Mail

If you want all outbound SMTP mail encrypted, you can set that option under the **Delivery** tab of the **SMTP Virtual Server**. So, with the **Properties** of your Default SMTP Virtual Server still open, do the following:

Warning: Enabling the TLS encryption under Outbound Security means that the SMTP Virtual Server only will or can communicate with other SMTP servers supporting TLS. Therefore, remember to do thorough testing before enabling this setting.

1. Click the **Delivery** tab, then click the **Outbound Security** button (see Figure 8.11).

Figure 8.11 The SMTP Virtual Server Delivery Tab



2. On the **Outbound Security** screen (see Figure 8.12), simply put a check mark next to **TLS encryption**, then click **OK**.

Figure 8.12 Enabling TLS Encryption on the Outbound Security Page



Enabling TLS/SSL for One or More Domains

The last option is to use TLS/SSL encryption only for SMTP communication with one or more other SMTP domains, which might be a better idea than enabling it on an SMTP Virtual Server, because chances are not all SMTP servers with which your server communicates support TLS/SSL. This can't be accomplished under an SMTP Virtual Server, but instead by creating an SMTP connector, then enabling the TLS/SSL option on the Outbound Security page of this connector. For details on how you create an SMTP connector, refer to Chapter 4.

Enabling IPSec Between SMTP Servers

One method of securing your SMTP traffic network on the internal network is to use IPSec between your Exchange servers. IPSec is used not only to secure SMTP traffic; it can also secure traffic between other kinds of Windows 200x servers. Although IPSec is a great way to protect the traffic between your SMTP servers, you should be aware that the method tends to create quite a lot of overhead. Details on how to implement IPSec in your network are beyond the scope of this book; instead, we suggest you read the Microsoft white paper, “Using Microsoft Windows IPSec to Help Secure an Internal Corporate Network Server,” at www.microsoft.com/downloads/details.aspx?FamilyID=a774012a-ac25-4a1d-8851-b7a09e3f1dc9&displaylang=en.

Encrypting MAPI Information on the Network

Many administrators are unaware that they can encrypt Messaging Application Programming Interface over Remote Procedure Calls (MAPI over RPC) information on the network and that doing so will benefit them in several ways. Although MAPI information on the network is difficult to decode, it is not impossible. Outlook MAPI clients use Remote Procedure Calls (RPCs) to communicate with the Exchange information store and the Active Directory (or Exchange System Attendant). RPCs include the ability to provide encryption of the RPC data stream using RSA RC-2 streaming encryption (either 40-bit encryption for Windows 95/98/Me or 128-bit encryption for Windows NT/2000/XP clients with the appropriate service packs).

Enabling MAPI over RPC client encryption is simple, but it must be configured at the messaging profile rather than at the server. Display the properties of the user's messaging profile and click **Properties** for the **Microsoft Exchange Server** service, then choose the **Advanced** property page, or the **Security** property page in Outlook 2003 (see Figure 8.13). For earlier clients, click the **When using the network** and / or **When using dial-up networking** check boxes to encrypt MAPI over RPC data crossing the network. For Outlook 2003, click the **Encrypt data between Microsoft Office Outlook and Microsoft Exchange Server** check box.

Figure 8.13 Encrypting Data Transferred from MAPI Clients to



Encrypting POP3 and IMAP4 Traffic

If you have any POP3 or IMAP4 clients in your messaging environment and these users are external (remote) users of some sort, it's very important to secure this type of traffic as well.



BY THE BOOK...

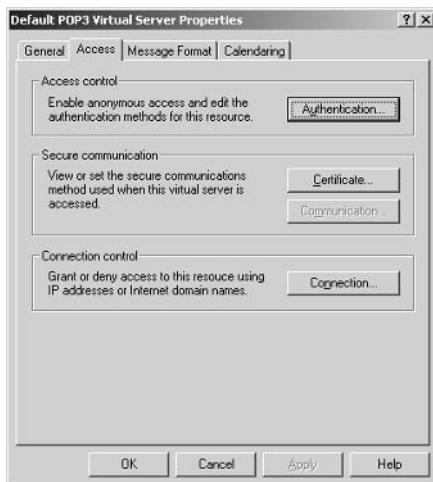
Exchange 2003 fully supports POP3 and IMAP4, two different methods for accessing a mailbox. POP3 allows a client to retrieve a specific user's mail from the server. It's worth noting that this protocol can't access public or private folders. In addition, it's not intended to provide full manipulation of mail on the server. Although the option of leaving mail on the server is available, mail is typically downloaded and then deleted. POP3 is used only to retrieve mail and is therefore used in conjunction with SMTP, which is used to send mail. Opposite POP3, IMAP4 allows a client to access messages in private and public folders on a server. It also allows users to access mail in their mailboxes without downloading the messages to a specific computer. Like POP3, IMAP4 cannot send mail, so this protocol is also used in conjunction with SMTP. In regard to features, IMAP4 is far superior to POP3.

Encrypting POP3 and IMAP4 traffic is very similar to encrypting traffic on SMTP Virtual Servers. To enable TLS/SSL on a POP3 or IMAP4 virtual server, do the following:

Note: Enabling this feature is an identical process whether it's done on a POP3 or an IMAP4 Virtual Server. In our example, we show how it's done on a POP3 Virtual Server.

1. On the Exchange server, open the **Exchange System Manager**.
2. Drill down to **Servers | Server | Protocols | POP3**.
3. Right-click the default POP3 Virtual Server, then select **Properties**.
4. Click the **Access** tab (see Figure 8.14).

Figure 8.14 Properties of a Default POP3 Virtual Server Access Tab



We can create a certificate by executing the Security Certificate Wizard and thereafter enable **Require secure channel** and **Require 128-bit encryption**, but since this procedure is identical to how it's done when dealing with the SMTP Virtual Servers (as described at the beginning of this chapter), we won't cover it again. We'll skip the certificate part and jump directly into enabling the TLS/SSL feature.

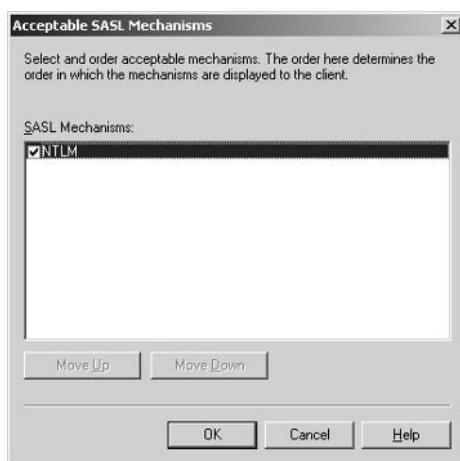
5. Click the **Authentication** button, then put a check mark in front of **Requires SSL/TLS encryption** (see Figure 8.15).

Figure 8.15 Enabling Requires SSL/TLS Encryption



Before you clicking OK, we thought it would be a good idea to provide you with a little information regarding the Simple Authentication and Security Layer (SASL) feature, which is enabled by default. When you use the SASL authentication method, usernames and passwords are encrypted using the Microsoft Windows Lan Manager (NTLM) security package. However, it's worth noting that message data isn't encrypted. The SAL authentication method only supports NTLM (see Figure 8.16) as of this writing, but this could change in future service packs or Exchange versions.

Figure 8.16 SASL Authentication Method



6. Click **OK**.

Securing Clients Using S/MIME

For some organizations, it might not be enough to secure the traffic itself. They might also want to implement Secure/Multipurpose Internet Mail Extensions (S/MIME) on their mail clients. S/MIME defines extensions to the MIME standard that allow a user to send encrypted and/or digitally signed messages between any two messaging clients as long as both clients support S/MIME. When an S/MIME solution is used, the message body and attachments are encrypted at the sender's computer prior to being sent to the sender's home server. The message remains encrypted while it is transmitted and while it is stored in the recipient's home message store. It is decrypted only when the intended recipient opens the message.



BY THE BOOK...

With Exchange 2003, Microsoft introduces some pretty important changes in regard to support for message security. With Exchange 2003, we can secure messages with the help of both digital signatures and message encryption. This is done through Exchange 2003's support for S/MIME version 3. Exchange 2003 fully supports S/MIME version 3 e-mail, allowing users to take advantage of message security services when sending and receiving e-mail messages to and from users of other S/MIME version 3 e-mail systems. You might remember that Exchange 2000 used the Key Management server, but this has changed with Exchange 2003, which instead provides the S/MIME functionality through Certificate Authority Services in Windows 2003 Server.

Using S/MIME

Before your users can use S/MIME, you basically need a security certificate; this can either be issued to your clients using your own internal CA or be obtained from a third-party certificate provider such as VeriSign, Thawte, or InstantSSL. Bear in mind, setting up your own CA typically depends on the size of your organization. Setting up your own doesn't really make sense if your organization consists of only a few people.

Because Microsoft has done a superior job in regards to documenting Message Security and S/MIME in general, we won't go into detail on how you set up and configure message security and S/MIME in your mail clients. We instead recommend that you read two Microsoft technical articles containing all that information on message security and S/MIME you will ever want to know. The first, "Quick Start Guide for S/MIME in Exchange Server 2003" (44 pages), is kind of an introductory article; the second, "Exchange Server 2003 Message Security Guide" (144 pages), is a more comprehensive guide. Both are available from the Security section of the Exchange 2003 Technical Documentation Library, which can be found at www.microsoft.com/technet/prodtechnol/exchange/2003/library.

Enabling S/MIME and Outlook

Although this book doesn't focus on the details of the clients in regard to S/MIME, we thought we at least would show you where the S/MIME settings are configured in an Outlook 2003 client. Therefore, do the following:

1. In Outlook, click **Tools | Options** in the menu.
2. Select the **Security** tab. You will be presented with the screen shown in Figure 8.17.

Figure 8.17 Security Options in Outlook 2003



3. As you can see, we have the options of encrypting e-mail, adding digital signature to outgoing messages, even requesting an S/MIME receipt from all S/MIME signed messages, and much more. If you click the **Settings** button under Default Setting, which brings us the screen shown in Figure 8.18, you can specify certificates and the type of algorithms that should be used.

Figure 8.18 Default Encrypted E-Mail Settings

Notes from the Underground...

Free Digital Signature Certificate

If you are an individual person (rather than an organization) interested in a digitally signed certificate but prefer not to pay for it, InstantSSL offers one for personal use. Read more on how to get this free certificate at www.instantssl.com/ssl-certificate-products/free-email-certificate.html.

Configuring RPC over HTTP(S)

Remote Procedure Calls over Hypertext Transfer Protocol (RPC over HTTP) is a new and exciting Exchange 2003 feature with which it is possible to connect Outlook MAPI clients to the Exchange 2003 Server directly over the Internet securely and without losing any form of functionality compared to ordinary Outlook RPC over TCP/IP clients. As you might know, this can also be accomplished using VPN connections, but unfortunately Outlook MAPI clients over a VPN connection have never worked very well. Using RPC over HTTP(S) instead of a tradi-

tional VPN connection also increase security because the remote users get access to only their specific mailboxes instead of the entire network.



BY THE BOOK...

The technology behind the RPC over HTTP(S) functionality is quite interesting. Most Exchange admins are aware that the Outlook client normally communicates with the Exchange server with the help of MAPI calls, which are sent via RPCs. This is still true with RPC over HTTP, but the RPC over HTTP(S) functionality puts an HTTP wrapper around the traffic. This makes it possible for the Outlook clients to communicate with the Exchange 2003 server, even though they aren't connected to the local network. The nice thing about the RPC over HTTP(S) functionality, besides that users get full Outlook access, is that you have to open only one port in the firewall, typically port 443 (SSL), just as with OWA.

The RPC over HTTP(S) feature is not enabled by default in Exchange 2003, so you need to do some configuration on the server side before you actually start configuring an Outlook client. But first you need to be aware of the requirements to use RPC over HTTP(S).

Requirements

It's very important that you understand the requirements in order for RPC over HTTP(S) to work. Read the following requirements carefully.

- **Client side** The client(s) must at least be running Windows XP (both Home and Pro are supported) with Service Pack 1. In addition, you will need to install the patch mentioned in Microsoft KB article 331320, “Outlook 2003 Performs Slowly or Stops Responding When Connected to Exchange Server 2003 Through HTTP,” at www.support.microsoft.com/?id=331320. This patch will be included in Windows XP Service Pack 2, which is just around the corner. The client needs to run Outlook 2003, as previous Outlook versions aren't supported.
- **Server side** All Exchange 2003 servers and any other servers (more specifically, domain controllers and Global Catalog servers) with which the RPC over HTTP(S) clients will communicate must be running Windows 2003 Server. It's not a requirement that you run Exchange 2003 in a front-end/back-

end topology in order for RPC over HTTP(S) to work; it's fully supported using RPC over HTTP(S) in a single-server scenario. But that said, it's recommended that you use a front-end/back-end scenario, if possible placed behind an ISA server.

In addition, you need an SSL certificate on the Exchange server (typically on your front-end server). You have the option of issuing this using your own Microsoft CA or getting the SSL certificate from a third-party certificate provider such as VeriSign, Thawte, or InstantSSL.

Note: To see how you install your own Certificate Authority Service and enable SSL on the default Web site in the IIS Manager, refer back to Chapter 5, which included a step-by-step guide.



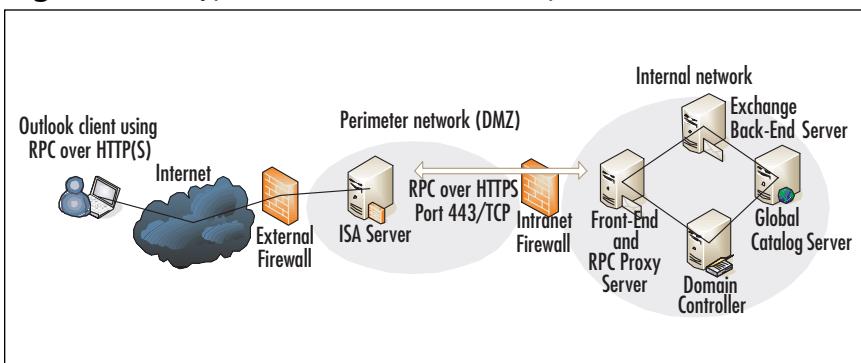
REALITY CHECK...

When using an SSL certificate from a third-party certificate provider, the certificate is automatically trusted, but if you use your own CA service, you must make sure that your client computers trust the certification authority, since Web browsers in this scenario by default won't trust your root certification authority.

For more information on how to have your clients trust a root CA, read Microsoft KB article 297681, "Error Message: This Security Certificate Was Issued by a Company That You Have Not Chosen to Trust," at www.support.microsoft.com/?id=297681.

In Figure 8.19, you see the recommended RPC over HTTP(S) setup when dealing with Exchange multiserver scenarios.

Figure 8.19 Typical RPC Over HTTP(S) Setup in a Multiserver



The nice thing about the scenario shown in Figure 8.19 is that we only have to open one port in our intranet firewall in order for external Outlook client connection using the RPC over HTTP(S) feature.

Notes from the Underground...

Using an ISA Server to Publish MAPI RPCs

If you have (or plan to have) an Internet Security and Acceleration (ISA) server located in your perimeter network (DMZ), you have the option of publishing the various Exchange protocols, including MAPI RPCs (port 135/TCP), which also make it possible to connect Outlook MAPI clients to the Exchange server directly over the Internet. So if you have an ISA server already deployed in your network, you might wonder, "Is it necessary to configure RPC over HTTP(S)?" The answer is: "It depends on your ISP." Many ISPs allowed RPC traffic (port 135/TCP) in the past. But after all the aggressive e-mail-borne virus attacks we have seen in the last couple of years, many of them have begun to block port 135/RPC. So if your ISP has blocked port 135/TCP and you need to offer full Outlook MAPI client support to your remote users, you are more or less forced to use the RPC over HTTP(S) feature.

For details on how to configure an ISA server to publish the various Exchange protocols, we suggest you check out some of the articles written by the ISA server guru himself, Dr. Thomas Shinder, which can be found at www.msexchange.org or www.isaserver.org. If you're really interested in the details, you should consider reading his book *ISA Server and Beyond* (Syngress Publishing, ISBN 1931836663).

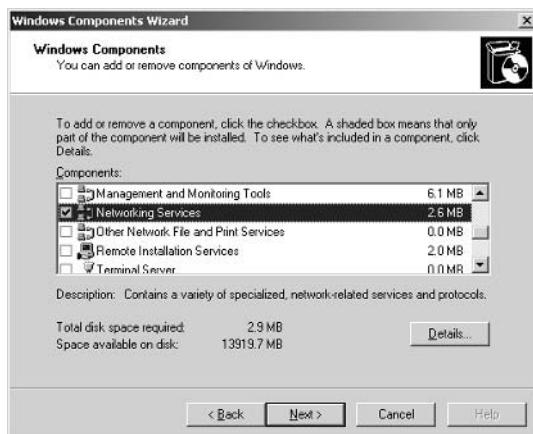
Configure RPC Over HTTP on a Front-End Server

In order for your remote Outlook clients to connect to their mailboxes using RPC over HTTP(S), you need to install the RPC over HTTP proxy component on the server you dedicate as the RPC proxy server. The RPC proxy server is the server processing the Outlook 2003 RPC requests that arrive from the Internet.

To install the RPC proxy component, do the following:

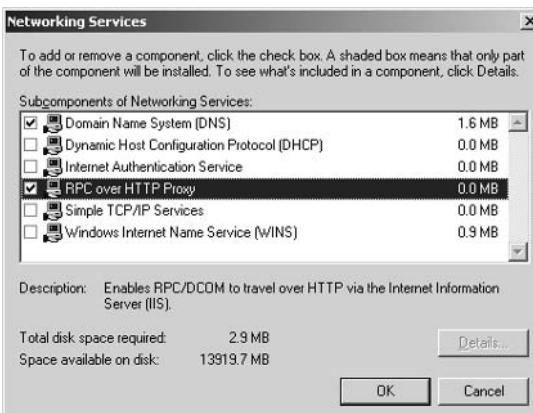
1. Log on to the server that is going to be the RPC proxy server. This can be any Windows 2003 server, but in this example we use the front end shown in Figure 8.1.
2. Click **Start | Settings | Control Panel | Add or Remove Programs**.
3. Click **Add/Remove Windows Components**, then double-click **Networking Services**. You will be presented with the screen shown in Figure 8.20.

Figure 8.20 Add/Remove Windows Components Networking Services



4. Put a check mark in **RPC over HTTP Proxy** (see Figure 8.21), then click **OK**.

Figure 8.21 Selecting RPC Over HTTP Proxy

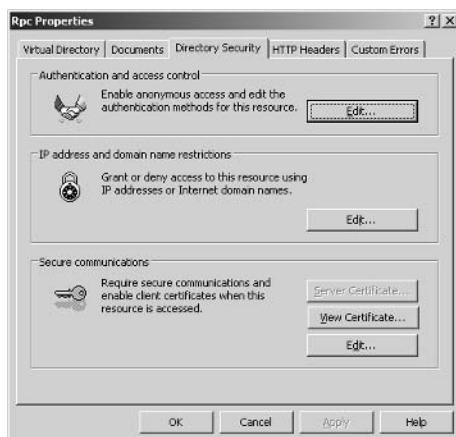


5. Click **Next**. Windows will now start copying the necessary files. When this process is completed, click **Finish** and exit **Add or Remove Programs**.

We now need to configure the RPC virtual directory in the IIS Manager. To do this, follow these steps:

- 1 Click **Start | Administrative Tools**, then open the **Internet Information Services (IIS) Manager**.
2. Expand **Local Computer | Web Sites | Default Web Site**.
3. Right-click the RPC virtual directory, then select **Properties**.
4. Click the **Directory Security** tab (see Figure 8.22), then click **Edit** under **Authentication and access control**.

Figure 8.22 Properties of RPC Virtual Directory



5. Remove the check mark in **Enable anonymous access**, then instead enable **Basic authentication** (see Figure 8.23).

Figure 8.23 Enabling Basic Authentication

6. Read the security warning message shown in Figure 8.24 and then click **Yes** to agree to continue.

Figure 8.24 Security Warning Message

7. Click **OK**.

You have now configured the RPC virtual directory to use basic authentication. If you haven't already done so, now is the time to enable SSL on this directory as well. Even if you think you have enabled SSL on the default Web site, you should double-check just in case. So do the following:

1. Still under the **Directory Security** tab of the RPC virtual directory, click **Edit** under **Secure Communications**.
2. If there are check marks in the **Require secure channel (SSL)** and **Require 128-bit encryption** boxes (see Figure 8.25), click **OK**. If not, enable both options, then click **OK**.

Figure 8.25 Checking if SSL is enabled on the RPC Virtual Directory

Note: For security reasons it's recommended that you use 128-bit encryption, but it's not required for RPC over HTTP(S) to function properly.

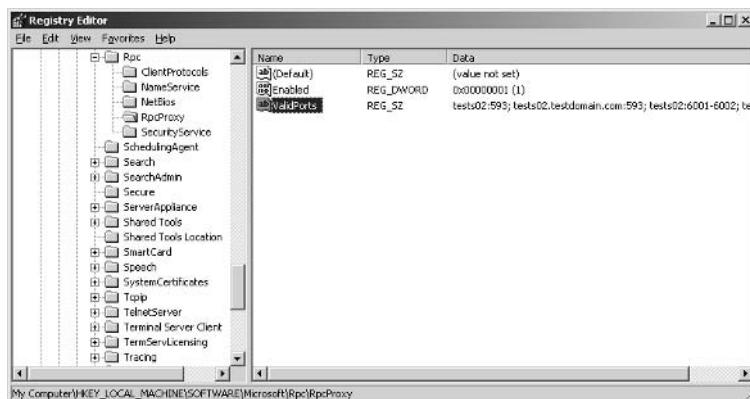
Specifying the RPC Proxy Ports

If you have a multiserver Exchange environment and you have installed the RPC over HTTP proxy server component on a front-end server located in your perimeter network (DMZ), you should configure the RPC proxy server to use specific ports to communicate with the rest of the servers on the internal network. Table 8.1 lists the ports that Exchange uses by default.

Table 8.1 Default RPC Proxy Server Ports

Port	Description
593/TCP	RPC traffic to the end-point mapper service
6001/TCP	RPC traffic to Information Store
6002/TCP	RPC traffic to Directory service
6004/TCP	RPC traffic to DS Proxy service

If the RPC proxy server is located in the perimeter network (DMZ), you must open the port numbers shown in Table 8.1 on your intranet firewall in order for the RPC proxy server to reach the internal Exchange back-end server(s), domain controller(s), and Global Catalog server(s). In addition, you need to list the servers the Outlook clients need to reach; this is done through the registry key located under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RPC\RpcProxy (see Figure 8.26).

Figure 8.26 RPCProxy *ValidPorts* Registry Key

Here you need to change the value of the *ValidPorts* key. The values should be entered in the following format:

```
ExchangeServer:593; ExchangeServerFQDN:593; ExchangeServer:6001-6002; ExchangeServerFQDN:6001-6002; ExchangeServer:6004;
ExchangeServerFQDN:6004; GlobalCatalogServer:593;
GlobalCatalogServerFQDN:593; GlobalCatalogServer:6004;
GlobalCatalogServerFQDN:6004
```

This means that if your Exchange back-end server is named Exchange01 and your Global Catalog server is called GlobalCatalog01 and both are members of the AD domain testdomain.com located on your internal network, you would need to enter the following strings in the Data field of the *ValidPorts* registry key:

```
Exchange01:593; Exchange01.testdomain.com:593; Exchange01:6001-6002; Exchange01.testdomain.com:6001-6002; Exchange01:6004;
Exchange01.testdomain.com:6004; GlobalCatalog01:593;
GlobalCatalog01.testdomain.com:593; GlobalCatalog01:6004;
GlobalCatalog01.testdomain.com:6004
```

Note: If you have more than one Exchange back end, domain controller, or Global Catalog server, you have to add these to this string as well.

When you have specified the RPC proxy port numbers on the RPC proxy server, you will also need to configure your Global Catalog servers. This is done the following way:

1. Log on to the **Global Catalog Server**.
2. Open the Registry Editor and navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.

3. Click **Edit | New**, then select **Multi-String Value**.
4. Name it **NSPI interface protocol sequences**.
5. Right-click the **NSPI interface protocol sequences** multi-string value, then click **Modify**.
6. Type **ncacn_http:6004** in the value box.

By configuring this setting, we force the Global Catalog server to listen for RPC over HTTP traffic on port 6004, which is also the port we have specified on the RPC over HTTP proxy server. You now need to reboot the Global Catalog server for the changes to take effect.

Disabling DCOM Support in RPC over HTTP

Distributed Component Object Model (DCOM) is a protocol that client/server applications can use on top of the RPC protocol. When you install the RPC over HTTP proxy component, the RPC proxy server will by default also accept DCOM requests using this protocol. These DCOM requests are then sent to a local port on the server implementing RPC over HTTP (TCP port 593). In dealing with security, it's considered best practice to disable or remove all nonessential components and services, so if you don't use DCOM in your environment, you would typically want to remove DCOM support. To see how to do that, we suggest you read Microsoft KB article 826382, "How to Disable DCOM Support in RPC over HTTP," at www.support.microsoft.com/default.aspx?kbid=826382.



REALITY CHECK...

If your Exchange front-end server on which the RPC over HTTP proxy service has been configured is placed on your internal network together with the rest of your servers, you don't need to specify the RPC proxy ports, since all port numbers normally would be open between the RPC over HTTP proxy server and the servers with which it needs to communicate.

Configuring the Client

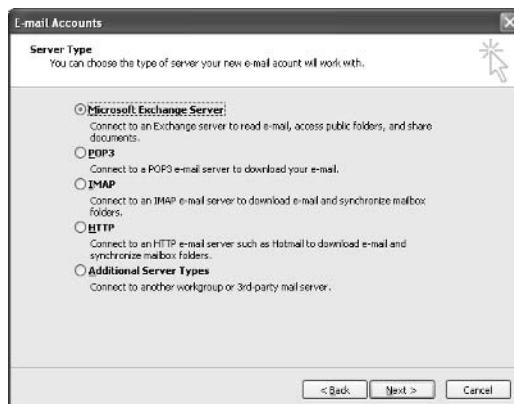
Now that the server-side part of RPC over HTTP(S) has been configured, it's time to configure our Outlook client(s). To do this, log on to your favorite Windows XP client machine and do the following:

1. Click **Start | Settings | Control Panel** then double-click the **Mail** icon. (If that icon isn't visible, switch to classic view.)
2. Because we want to configure a new profile, select **Show Profiles**, then click **Add** (see Figure 8.27).

Figure 8.27 Creating a New RPC Over HTTP(S) Outlook Profile

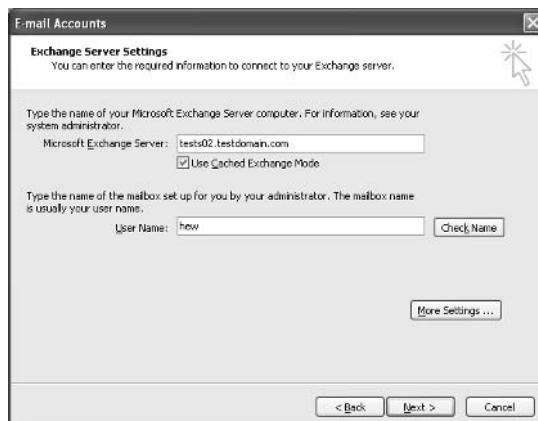


3. Give the profile a descriptive name such as **users_name (RPC over HTTPS)**.
4. Make sure that **Add a new e-mail account** is selected, then click **Next**.
5. Under Server types, select **Microsoft Exchange Server** (see Figure 8.28), then click **Next**.

Figure 8.28 Selecting Server Type: Microsoft Exchange Server

The time has come to specify the FQDN of your Exchange server, but don't let this fool you—it's actually the internal FQDN you need to specify (not the external!).

6. Enter the Exchange server's FQDN, which in this example is **tests02.testdomain.com**, then make sure cached mode isn't enabled (not yet at least). Then enter your username in the **User Name** field, but don't click Check Name yet! Instead, click **More Settings** (see Figure 8.29).

Figure 8.29 Specifying Internal FQDN and Username

7. After a few seconds, you will probably be asked to validate to the Exchange server. Enter a valid username and password, then click **OK** (see Figure 8.30).

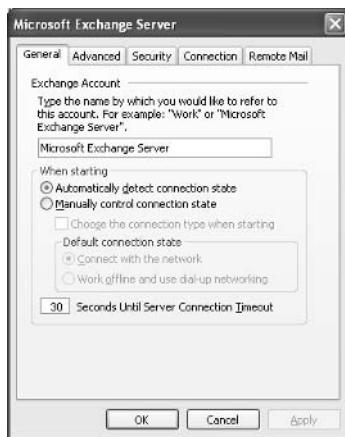
Note: If you instead get a warning message indicating the Exchange server is unavailable, simply click OK twice.

Figure 8.30 Validation Box



No matter if you were validated or got the warning message, you should end up with the screen shown in Figure 8.31.

Figure 8.31 General Tab Under the Properties of the Outlook 2003 Mail Profile



8. Click the **Connection** tab (see Figure 8.32).



REALITY CHECK...

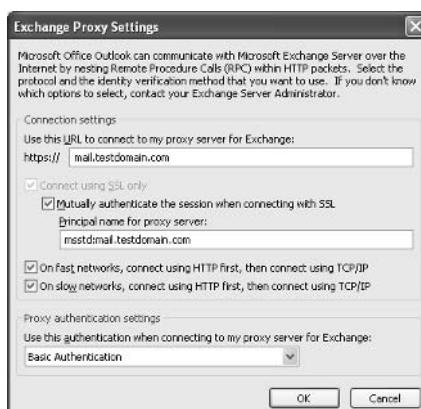
Several Exchange forums, newsgroups, and other communities have had a great deal of discussion as to whether it is necessary to allow port 135 directly from the Internet, if the Outlook client is configured from a remote site. This is not necessary, since all necessary communication is done via port 443/SSL.

Figure 8.32 Connection Tab



- Select the **Connect using Internet Explorer's or a 3rd party dialer**, then put a check mark in **Connect to my Exchange mailbox using HTTP**, then click the **Exchange Proxy Settings** button. The screen shown in Figure 8.33 will appear.

Figure 8.33 Exchange Proxy Settings Configuration



10. This screen needs some extra attention because it's quite important how you configure the Exchange Proxy Settings. If you don't specify the correct URL(s), you will never be able to make a connection via RPC over HTTP(S). First we need to specify the URL to the RPC proxy server, and because this, in this example, is our front-end server, we enter **mail.testdomain.com**. This URL should be your external FQDN, which can be reached from the Internet. In typical situations, this FQDN is the same as the one you specified in the Common Name field of your Web site's SSL certificate.

Then we have the option of enabling **Mutually authenticate the session when connecting with SSL** and then specify the **Principal name for proxy server**, which in this example also is the external FQDN of the Exchange front-end server. As you can see in Figure 8.15, you must specify the URL as **msstd:mail.testdomain.com**; msstd is a Microsoft-standard form that needs to be used for specifying the principal name.



REALITY CHECK...

It's not required that you enable the **Mutually authenticate the session when connecting with SSL** feature, but using the feature provides the most optimal security.

11. The next two features—**On fast networks, connect using HTTP first, then connect using TCP/IP** and **On slow networks, connect using HTTP first, then connect using TCP/IP**—don't have anything to do with security, but it's generally a good idea to enable them. The last feature, though, is quite important—this is where you specify the proxy authentication settings. Here you should select **Basic authentication** in the drop-down text box. When you have specified the Exchange Proxy Settings and everything else has been configured properly, you should be able to click the **Check Name** button to resolve the internal FQDN of the Exchange server and the specified username. When you have done so, click **OK** and exit any open window.

12. Now, execute Outlook. You will be prompted for a username and password. When those are validated, Outlook should open and you should have full Outlook 2003 functionality directly over the Internet using RPC over HTTP(S).

Notes from the Underground...

That Damned RPC Over HTTP(S) Thing Won't Work!

As much joy as you will have when you have managed to get RPC over HTTP(S) to work properly, you can experience as much frustration when it just doesn't want to do what you want it to do. There have been many questions on the Exchange forums, newsgroups, and other communities relating to RPC over HTTP(S). Obviously, many Exchange admins can have a difficult time getting this feature to work. We therefore thought we would provide you with a few tips to help you in your troubleshooting as well as links to the best RPC over HTTP(S) documentation on the Web as of this writing.

The first thing to try if RPC over HTTP(S) doesn't work is to start Outlook 2003 with the /RPCDIAG switch. Simply click **Start | Run** and type **Outlook.exe /RPCDIAG**. This way you can see if Outlook connects to the proper services and if it does so over RPC over HTTP(S). Note that if HTTPS appears in the Conn column in the Exchange Connection Status dialog box, a service is connected using RPC over HTTP(S).

Another thing to try is to access the RPC virtual directory through your Web browser. Simply start your browser and point to <https://mail.testdomain.com/rpc>. You should get an error message 403.2 if you do the certificate and permission on the directory has been set up correctly.

You can also use the RPCPING tool located on the Exchange 2003 CD or directly from Microsoft Exchange Product Support Services' FTP site for troubleshooting: <ftp.microsoft.com/PSS/Tools/Exchange%20Support%20Tools>. The following MS KB article has instructions on how to use RPCPING: 831051, "How to Use the RPC Ping Utility to Troubleshoot Connectivity Issues with the Exchange Over the Internet Feature in Outlook 2003," at www.support.microsoft.com/default.aspx?id=831051.

Here are some other useful RPC over HTTP(S) links:

- Microsoft KB article 833401, "How to Configure RPC Over HTTP in Exchange Server 2003": www.support.microsoft.com/?id=833401
- Exchange Server 2003 RPC over HTTP Deployment Scenarios: www.microsoft.com/technet/prodtechnol/exchange/2003/library/ex2k3rpc.mspx
- Configuring Outlook 2003 for RPC over HTTP: www.microsoft.com/office/ork/2003/three/ch8/outc07.htm#sub_1
- Microsoft KB article 826486, "You Cannot Use RPC Over HTTP with a Proxy Automatic Configuration Script": support.microsoft.com/default.aspx?id=826486
- Microsoft KB article 822594, "Remote Procedure Call Over HTTP Is Not Successful or Reverts to TCP": support.microsoft.com/default.aspx?id=822594
- Remote Procedure Calls Using RPC over HTTP: msdn.microsoft.com/library/en-us/rpc/rpc/remote_procedure_calls_using_rpc_over_http.asp?frame=true
- RPC over HTTP Deployment Recommendations: msdn.microsoft.com/library/en-us/rpc/rpc/rpc_over_http_deployment_recommendations.asp?frame=true
- Microsoft KB article 829134, "Support WebCast: Using Microsoft Exchange Over the Internet (RPC/HTTP) with Microsoft Office Outlook 2003": www.support.microsoft.com/default.aspx?id=829134
- Microsoft KB article 831050, "Configuration Options for the Exchange Over the Internet Feature in Outlook 2003": www.support.microsoft.com/default.aspx?id=831050
- Microsoft KB article 820281, "You Must Provide Windows Account Credentials When You Connect to Exchange Server 2003 With Outlook Over HTTP": www.support.microsoft.com/default.aspx?id=820281
- Exchange Server 2003 Deployment Guide (Chapter 8): www.microsoft.com/technet/prodtechnol/exchange/2003/library/depguide.mspx

Your A** Is Covered If You...

- Are aware of the options available in regard to encrypting SMTP traffic between your servers/clients.
- Read the two Microsoft technical articles covering S/MIME and message security mentioned in this chapter.
- Know how to secure your clients using S/MIME.
- Know how to configure, use, and troubleshoot the RPC over HTTP(S) feature.

Chapter 9

Combating Spam

In this Chapter

By now our Exchange messaging environment should be in a state that we can call fairly secure, but to have an ideal setup, we still have a few important tasks to complete. One of these tasks is to set up a properly configured antispam system to protect our messaging environment against spam and other unsolicited e-mail messages.

Spam is an ever-growing problem that causes companies around the world to lose enormous amounts of money each year. Microsoft has included some new features in Outlook 2003 and Exchange 2003 that will help us to combat spam.

The topics covered in this chapter are:

- Client-Side Filtering
- Server-Side Filtering
- Intelligent Message Filter (IMF)

By the end of this chapter, you will have a thorough understanding of the built-in antispam features of Outlook 2003 and Exchange 2003. You will also gain insight into Microsoft upcoming Exchange 2003 antispam IMF add-on.

Client-Side Filtering

As part of its trustworthy computing initiative, Microsoft promises to reduce spam. Outlook 2003 includes new and improved functionality that specifically addresses spam. The most notable of the new antispam features included in Outlook 2003 is definitely the new junk e-mail filter based on the Microsoft SmartScreen technology, which is also used with MSN and Hotmail. The new SmartScreen-based junk e-mail filter helps prevent spam and other unsolicited messages from reaching users, improving on earlier versions of Outlook. It also provides enhanced flexibility and control.



By THE BOOK...

Because the new Outlook junk e-mail filter uses Microsoft's SmartScreen-based technology, it provides proactive prevention against spam, which means that unlike most other spam filters, it doesn't rely on previous knowledge of a specific spam e-mail message to protect against it.

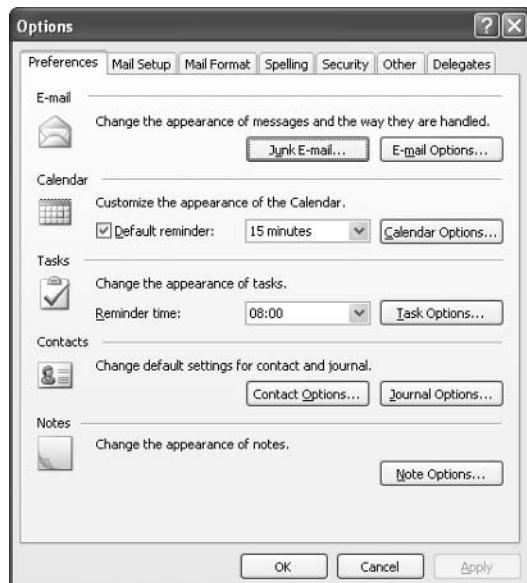
The junk e-mail filter uses a comprehensive approach to help protect against spam by combining list-based approaches with machine learning technology. As time has passed, more and more e-mail messages have been collected from Microsoft's community of spam fighters, and the Outlook 2003 junk e-mail filter is learning a larger "vocabulary" that continually increases its knowledge of the latest definitions and indicators of spam. Microsoft is committed to sharing this intelligence with updates to the junk e-mail filter at the Office Update Web site, and the company has already provided one update since the product release. Outlook 2003 also includes the Web Beacon Blocking feature, the Safe Senders/Safe Recipients/Blocked Senders lists, and the enhanced Attachment Blocking feature, which we also touched in Chapter 7.

To read more about the improvements in the Outlook 2003 junk e-mail Filter, we suggest you take a look at the Microsoft white paper, *Microsoft Office Outlook 2003 Junk E-Mail Filter With Microsoft SmartScreen Technology*, which can be downloaded from www.microsoft.com/office/outlook/prodinfo/filter.mspx.

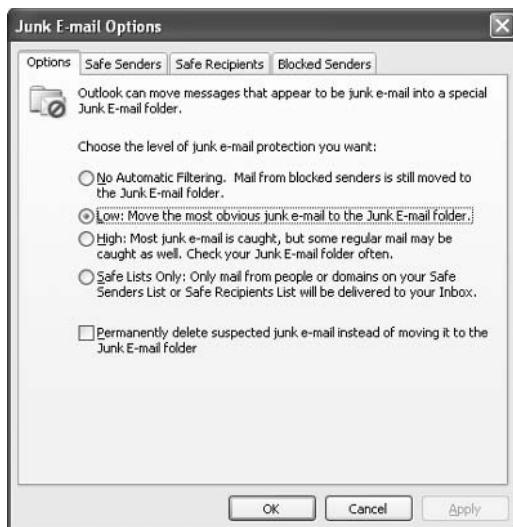
Let's go through each of the configuration option screens related to the Outlook 2003 junk e-mail filter. To get started, we need to do the following:

1. Launch **Outlook 2003**.
2. In the menu, click **Tools | Options**.
3. On the Preferences tab, click the **Junk E-mail** button (see Figure 9.1).

Figure 9.1 Outlook 2003 Options Screen



Now you might be prompted with the dialog box shown in Figure 9.2. This is a warning explaining that to use the junk e-mail filter, you must configure your Outlook Profile to use cached mode; otherwise the filter won't work. The reason that you must run Outlook in cached mode is that the full content of each e-mail message must be downloaded before it can be filtered. If you're already running in cached mode, you will be presented with the screen shown in Figure 9.3.

Figure 9.2 Junk E-Mail Filter Warning**Figure 9.3** Junk E-Mail Options

Under the Options tab shown in Figure 9.3, we can specify how aggressively we want the level of junk e-mail protection to be. There are four settings to choose from:

- **No Automatic Filtering** With the No Automatic Filtering setting, Outlook will only block e-mail addresses or domains already contained on the Blocked Senders list. So, although the automatic junk e-mail filter has been turned off, all e-mail addresses and/or domains present on the Blocked Senders list will be moved to the Outlook Junk E-mail folder.

- **Low (Default setting)** The Low setting moves the most obvious junk e-mail to the Outlook Junk E-mail folder. If you don't receive many junk e-mail messages and want to see all but the most obvious ones, you should select this option.
- **High** With the High setting, Outlook catches most junk e-mail. If you receive a large volume of junk e-mail messages, select this option. But make it a habit to periodically review the messages moved to your Junk E-mail folder, because some wanted messages could be moved there as well.
- **Safe List Only** When the Safe List Only setting is selected, only mail from people or domains on your Safe Senders List or Safe Recipients lists will be delivered to your inbox. Any e-mail messages sent from someone not on your Safe Senders list or sent to a mailing list not on the Safe Recipients list will be treated as junk e-mail.

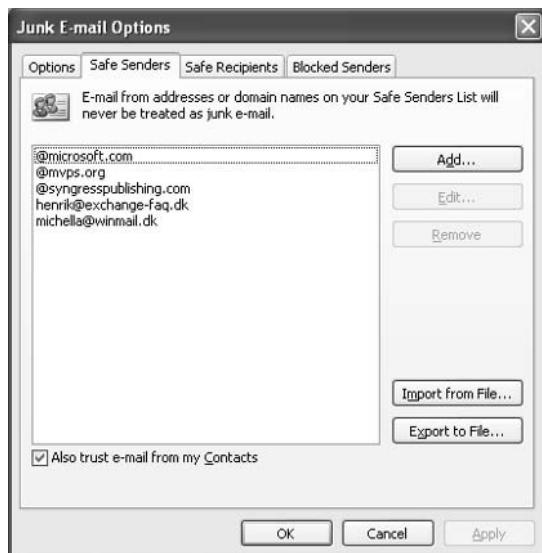
In the very bottom of the Options tab in Figure 9.3, you also have the possibility of putting a check mark in the box next to **Permanently delete suspected junk e-mail instead of moving it to the Junk E-mail folder**, but you should be very careful with this option, because it will permanently delete suspected junk e-mail messages, which means that the messages are immediately deleted and not moved into the Deleted Items folder.

Let's move on by clicking the **Safe Senders** tab.

Safe Senders

Safe Senders are people and/or domains from whom you want to receive e-mail messages. E-mail addresses and domains on the Safe Senders list will never be treated as junk e-mail.

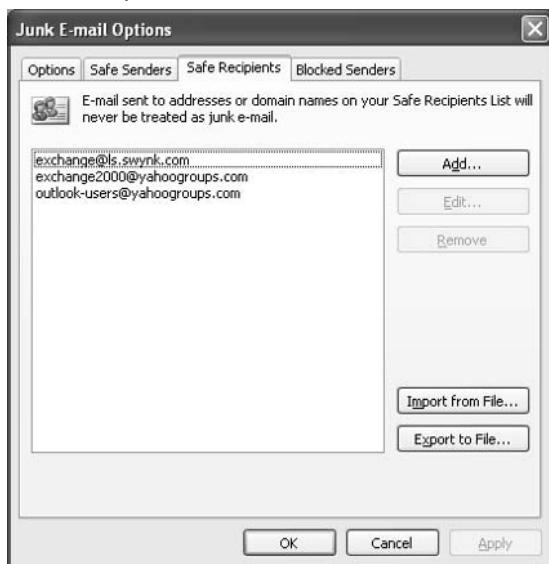
The Safe Senders List (see Figure 9.4) should look familiar, since it's almost identical to the OWA 2003 version, which we covered in Chapter 7. But if you look closer, you can see that we have a few more options available when accessing the list through Outlook 2003. As shown in Figure 9.4, it's possible to import and export the Safe Senders list to and from a file (the file must be in a text or tab-separated value file format). This is a nice feature if as an Exchange Admin, for example, you have created a list you want to share with your users.

Figure 9.4 Safe Senders List

Also notice the option **Also trust e-mail from my Contacts**. As you might already have guessed, checking this option will make Outlook trust all addresses contained in your Contacts folder. Now click the **Safe Recipients** tab.

Safe Recipients

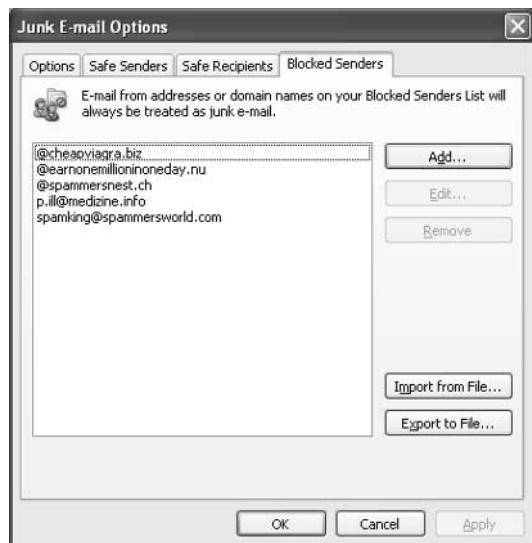
Safe Recipients are distribution or mailing lists of which you are a member and from which you want to receive e-mail messages (see Figure 9.5). You can also add individual e-mail addresses to your Safe Recipients list. For example, you might want to allow messages that are sent to not only you but also to a particular person.

Figure 9.5 Safe Recipients List

As was the case on the Safe Senders list, we can import or export from a .txt file to the Safe Recipients list. Now click the **Blocked Senders** tab.

Blocked Senders

Blocked senders are people and domains from which you don't want to receive e-mail messages (see Figure 9.6). Messages received from any e-mail address or domain on your Blocked Senders list are sent directly to your Junk E-mail folder.

Figure 9.6 Blocked Senders List

When any incoming messages are checked, each junk e-mail filter list gives e-mail address precedence over domains. Let's take an example. Suppose that the domain `syngresspublishing.com` is on your Blocked Senders list (of course, this would never be the case in real life), and the address `editor@syngresspublishing.com` was on your Safe Senders List. The address `editor@syngresspublishing.com` would then be allowed into your inbox, but all other e-mail addresses with the `syngresspublishing.com` domain would be sent to your Junk E-mail folder.

As was the case on the Safe Senders and Safe Recipients lists, we can import or export from a .txt file to the Blocked Senders list.

Note: The Safe Senders, Safe Recipients, and Blocked Senders lists were featured because they are so common to the Outlook Web Access variants, also covered in Chapter 7.

We've been through all four tabs of the Junk E-mail Options, and it's time to move on to the External Content Settings, so click **OK** to exit the Options, and click the **Security** tab (see Figure 9.7).

Figure 9.7 The Security Options Tab

Click **Change Automatic Download Settings** under Download Pictures. You'll see the screen presented in Figure 9.8.

Figure 9.8 Automatic Picture Download Settings

Under Automatic Picture Download Settings, we can specify whether pictures or other content in HTML e-mail should be automatically downloaded. We can even specify whether downloads in e-mail messages from the Safe Senders and Safe Recipients lists used by the Junk E-mail folder should be permitted or not. We can also specify

whether downloads from Web sites in the Trusted Zone of the Outlook Security Zone should be permitted. Last but not least, it's possible to enable **Warn me before downloading content when editing, forwarding, or replying to e-mail**, which, when enabled, displays a warning message for each edited, forwarded, or replied message containing external content.



REALITY CHECK...

If for some reason you haven't upgraded your clients to Outlook 2003 yet, you could instead use a third-party product such as Sunbelt's iHateSpam, Cloudmark's SpamNet, and many others. For a good list containing client-based antispam software, check out the following link at Slipstick: www.slipstick.com/addins/content_control.htm.

Almost all of them support Outlook 2000–2002 and typically cost between \$20 and \$30 per seat, depending on discount. But be aware that this could end up as a rather expensive solution if you have several thousand seats.

Server-Side Filtering

When Microsoft developed Exchange 2003, the company knew it had to improve the server's ability to combat spam, Exchange 2003 therefore introduces several new antispam features such as connection filtering, recipient filters, and sender filters. This is much more than its predecessor Exchange 2000 offered, but we still miss some important features such as Bayesian filtering and heuristics-based analysis. Some of these missing features will be introduced with the new SmartScreen-based Exchange 2003 add-on, Intelligent Message Filter (IMF), which Microsoft will release later this year, but unfortunately IMF will only be available to SA customers. (We will talk more about IMF later in this chapter.)



BY THE BOOK...

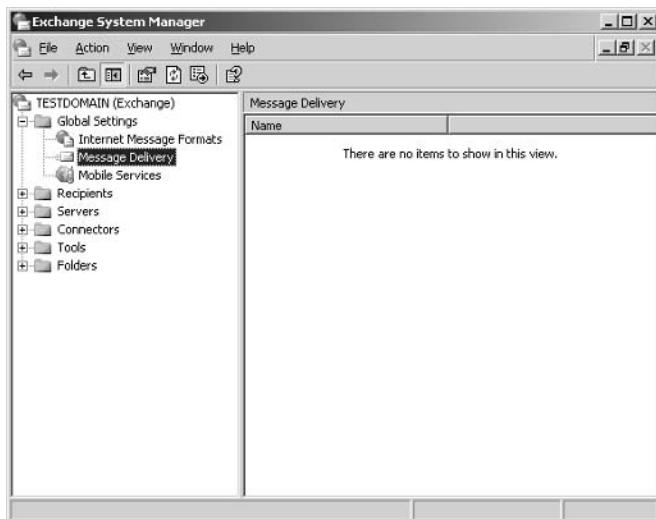
One of the most interesting new antispam features of Exchange 2003 is the connection filtering feature, which, among other things, includes support for real-time blacklists (RBLs), which means that Exchange 2003 uses external services that list known sources of spam and other unsolicited e-mail sources, dialup user

accounts, and servers with open relays. The RBL feature allows you to check a given incoming IP address against a RBL provider's list for the specific categories you would like to filter. With the recipient filtering feature, you can block mail that is send to invalid recipients. You can also block mail to any recipients who are specified in a recipient filter list, whether they are valid or not. The recipient filter feature blocks mail to invalid recipients by filtering inbound mail based on Active Directory lookups. The sender filtering feature is used to block messages that were sent by particular users.

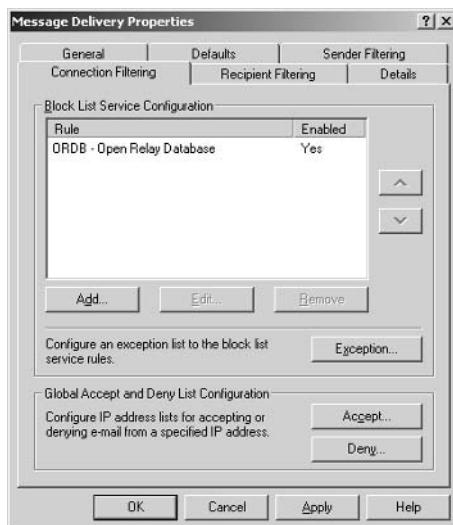
Let's take a step-by-step look at how to configure each of the new Exchange 2003 antispam features. We start with configuring the Connection Filtering feature. To get to the Connection Filtering tab, we need to perform the following steps:

1. Logon to the Exchange 2003 server.
2. Start the **Exchange System Manager**.
3. Expand **Global Settings** (see Figure 9.9).

Figure 9.9 The Exchange System Manager



4. Right-click **Message Delivery** and select **Properties**.
5. Click the **Connection Filtering** tab (see Figure 9.10).

Figure 9.10 The Connection Filtering Tab

Connection Filtering

A new feature in Exchange 2003 is the possibility of specifying one or more block list service providers (also known as real-time blacklists, or RBLs). The two terms will be used interchangeably throughout the chapter). For readers who don't know what blacklists are all about, here comes an explanation. A *blacklist* is a list containing entries of known spammers and servers that acts as open relays, which spammers can hijack when they want to use innocent servers to sent spam messages. By checking all inbound messages against one or more blacklists, you can get rid of a rather big percentage of the spam your organization receives. Note that you always should test a blacklist before introducing it to your production environment, because some blacklists might be too effective, meaning that they will filter e-mails your users actually want to receive. Also keep in mind that connection-filtering rules apply only to anonymous connections and not users and computers.

Let's take a closer look at the different options available, when specifying a new list to block. Click the **Add** button shown in Figure 9.10. You'll see a screen like the one shown in Figure 9.11.

Figure 9.11 Connection Filtering Rule



As you can see in Figure 9.11, we now need to enter the necessary block list information.

Display Name

In the Display Name field, you should type the connection-filtering rule name that you want displayed on the list on the Connection Filtering tab. This name could be anything, but a good rule of thumb is to use the name of the Black List provider.

DNS Suffix of Provider

In the DNS Suffix of Provider field, you should enter the DNS suffix of the blacklist provider.

In Table 9.1 we have created a list of some of the well known and effective blacklist providers. You can add multiple blacklists to your Exchange server. If you look back at Figure 9.10, you can see that you can use the arrow buttons to the right to put the lists in the order you want them queried. It's not recommended that you add more than four to five blacklists to your server, especially not on servers with a lot of traffic. The reason is that each inbound mail message, whether it's spam or not, needs to be queried against each blacklist, which, as you might guess, puts a performance burden on a possibly already overloaded Exchange server.

Table 9.1 Good Real-Time Blacklist Providers

Provider Name	DNS Suffix	Blacklist Web Site	Description
Open Relay Database	relays.ordb.org	www.ordb.org	Lists verified open relays. One of the (ORDB) largest databases, used widely for open relay filtering.
SPAMCOP	bl.spamcop.net	www.spamcop.net	Lists spam carriers, sources, or open relays. Has complex rules to decide whether a host is a spam carrier or not.
Blacklists China and Korea	cn-kr.blackholes.us	www.blackholes.us	This zone lists China and Korea network Korea US (BLCKUS-CNKR) ranges. China: DNS result 127.0.0.2. Korea: DNS result 127.0.0.3. 127.0.0.2 and 127.0.0.3 tests are supported.
Domain Name System Real-Time Black Lists (DNSRBL-SPAM)	spam.dnsrbl.net	www.dnsrbl.com	List of confirmed “honey pot” spammers. These are addresses created for the sole purpose of placing them in “harvesting” contexts. Anyone sending mail to one of these addresses is a spammer.
Domain Name System Real-Time Blacklists Dialup Networking (DNSRBL-DUN)	dun.dnsrbl.net	www.dnsrbl.com	Lists dialup networking pools that are never a legitimate source to directly contact a remote mail server.
DEVNULL	dev.null.dk	dev.null.dk	Lists open relays.

Custom Error Message to Return

When adding a block list, we also have the option of creating a custom error message that will be returned to the sender. Usually you should leave this field blank to use the default error message. The default message is:

```
<IP address> has been blocked by <Connection Filter Rule Name>
```

If you create your own custom error message, you can use the variables shown in Table 9.2.

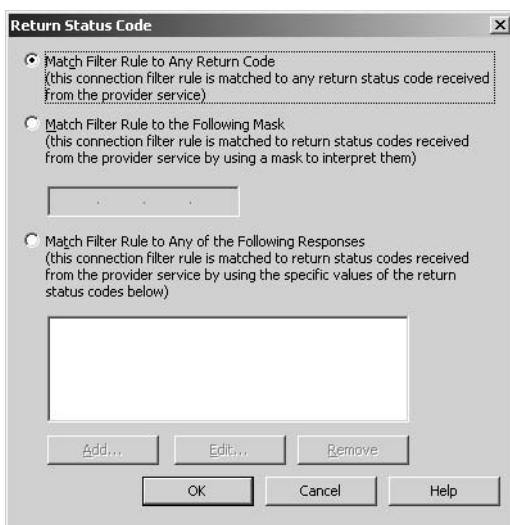
Table 9.2 Available Custom Error Message Variables

Variables	Description
%0	Connecting IP address
%1	Name of connection filter rule.
%2	The block list provider.

Return Status Code

This option is used to configure the return status code against which you want to filter. Let's click the **Return Status Code** button so we can see the three Return Status Codes options it's possible to choose between (see Figure 9.12).

Figure 9.12 Return Status Code



Here are the options presented on the Return Status Code screen:

- **Match Filter Rule to Any Return Code** This is the default setting. You should select this option to match all return codes with the filter rule. If an IP address is found on any list, the blacklist provider service sends a positive return code, and the filter rule will block the IP address.
- **Match Filter Rule to the Following Mask** Enter the mask that you want to use to interpret the return status codes from the blacklist provider service. Contact your blacklist provider service to determine the conventions used in the provider's masks.
- **Match Filter Rule to Any of the Following Responses** If you want the filter rule to match one of multiple return status codes, then enter the return status codes you want the rule to match. For example, you can use this option if you want to check the status codes returned when an IP address is on the list of known sources of unsolicited commercial e-mail or on the dialup user list.

Disable This Rule

The last option under Connection Filtering rules (refer back to Figure 9.11) is quite easy to explain. This check box is simply used to disable a created rule.

Notes from the Underground...

Information About Block List Service Providers and Status Codes

When we specify a Block List (aka Real-time Black List) provider, each time an e-mail message arrives at the Exchange server, the server performs a lookup of the source IP address of sending mail server in the specified blacklist. If the IP address isn't present on the blacklist, the list returns a "Host not found" error message. If the IP address is present, the blacklist service returns a status code, with an indication of the reason that the IP address is listed. The following is a list of the most common RLB status codes.

Continued

- 127.0.0.2 Verified open relay
- 127.0.0.3 Dialup spam source
- 127.0.0.4 Confirmed spam source
- 127.0.0.5 Smart host
- 127.0.0.6 A spamware software developer or spamvertized site (spamsites.org)
- 127.0.0.7 List server that automatically opts users in without confirmation
- 127.0.0.8 Insecure formmail.cgi script
- 127.0.0.9 Open proxy servers

Exception Lists

Now that you've seen the steps necessary for adding a blacklist, we can move on to have a look at the Exception list. Click the **Exception** button shown in Figure 9.10. We are now presented with the screen shown in Figure 9.13. As you can see, it's possible to add SMTP addresses to an exception list. All SMTP addresses on this list will not be filtered by the blacklist rules. The purpose of the Exception list is to give us an option of specifying important SMTP addresses (such as company partners and the like) so that mail messages from these senders don't get filtered by one of our configured block lists.

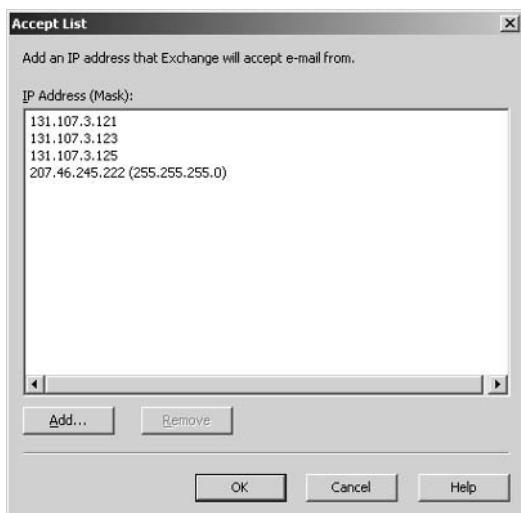
Please note that you're not limited to adding individual SMTP addresses to this list. You can also use wildcard addresses (for example, `*@testdomain.com`), as shown in Figure 9.13.

Figure 9.13 An SMTP Address Exception List

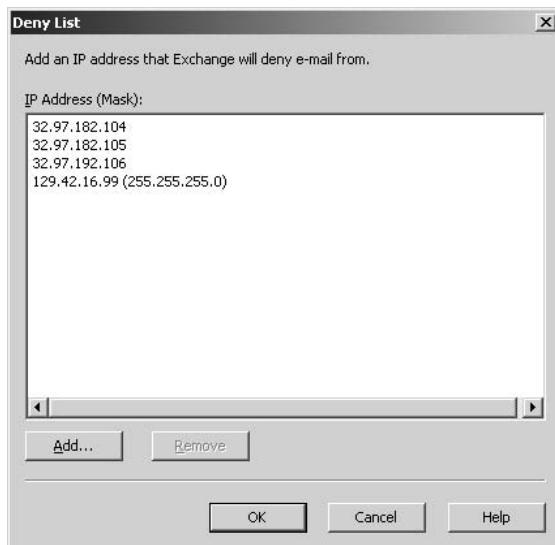
Global Accept and Deny List

We have now reached the last feature available under the Connection Filtering tab. Actually, it's two features: the global Accept and Deny lists (refer back to Figure 9.10).

- **Accept list** The Accept list (see Figure 9.14) is used to add a single IP address or a group of IP addresses from which you want to accept messages on a global level. Exchange checks the global Accept and Deny lists before checking the connection filter rules. If an IP address is found on the global Accept list, the Exchange server automatically accepts the message without checking the connection filter rules.

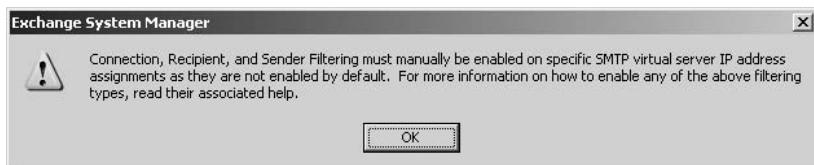
Figure 9.14 The Global Accept List

- **Deny list** The Deny list (see Figure 9.15) is also used to add a single IP address or a group of IP addresses, but opposite the Accept list, these addresses are denied access, before checking the connection filter rules. Exchange simply drops the SMTP connection right after the mail (*MAIL FROM*) command is issued.

Figure 9.15 The Global Deny List

Let's finish the Connection Filtering tab with an important note that also relates to the Recipient and Sender filtering tabs. When creating a Connection, Recipient, and Sender filtering rule and then clicking **Apply**, we receive the warning box shown in Figure 9.16.

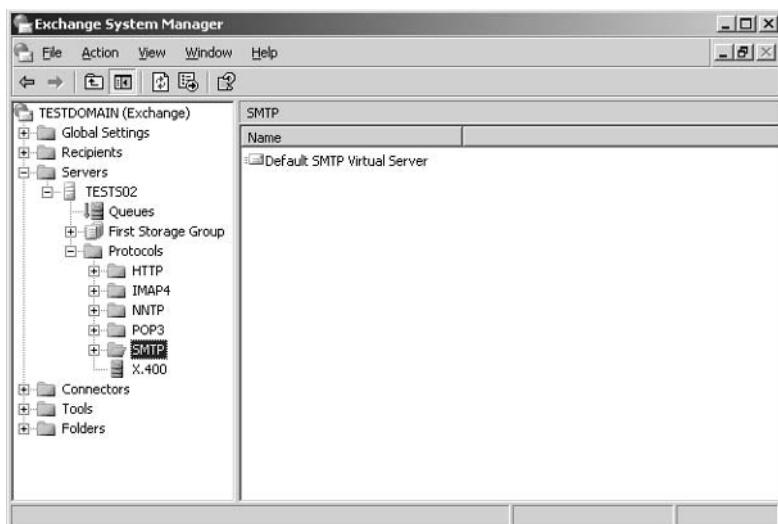
Figure 9.16 Filtering Rule Warning



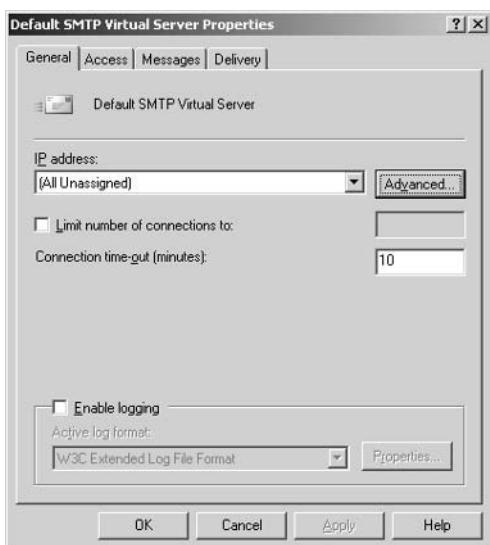
To apply the filtering rule to a SMTP virtual server, we need to do the following:

1. In the Exchange System Manager, drill down to **Servers** | **Server** | **Protocols** | **SMTP** (see Figure 9.17).

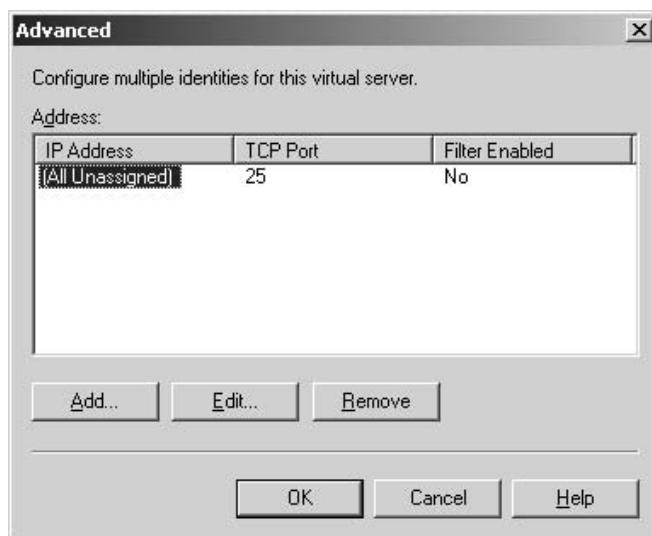
Figure 9.17 Default SMTP Virtual Server in System Manager



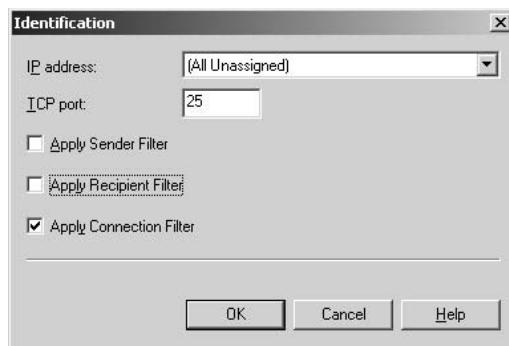
2. Right-click **Default SMTP Virtual Server** in the right pane, then select **Properties** (see Figure 9.18).

Figure 9.18 Properties of Default SMTP Virtual Server

3. Under **General**, click the **Advanced** button. You'll see the screen shown in Figure 9.19.

Figure 9.19 Advanced Properties

4. Now click **Edit**, and you'll see the Identification screen shown in Figure 9.20.

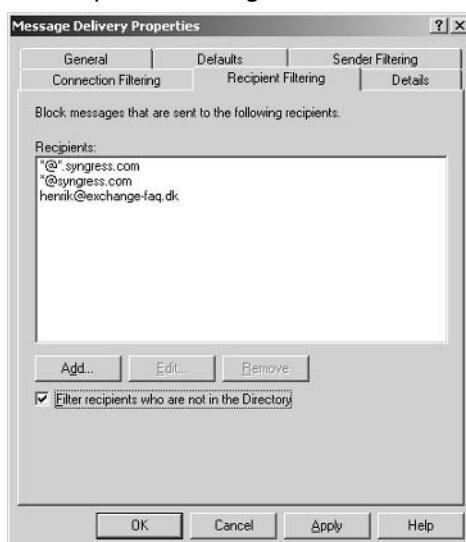
Figure 9.20 Identification

As you can see in Figure 9.20, this is where we apply the Connection, Recipient, and Sender filtering rules to our default SMTP virtual server.

We can now move on to the Recipient Filtering tab.

Recipient Filtering

The Recipient Filtering feature allows us to block incoming e-mail messages that are addressed to specific recipients. We can filter recipients using several formats. We can specify individual e-mail addresses, or we can filter a complete group of e-mail addresses using wildcards such as `*@syngress.com` (or even subdomains such as `*@*.syngress.com`), as shown in Figure 9.21.

Figure 9.21 The Recipient Filtering Tab

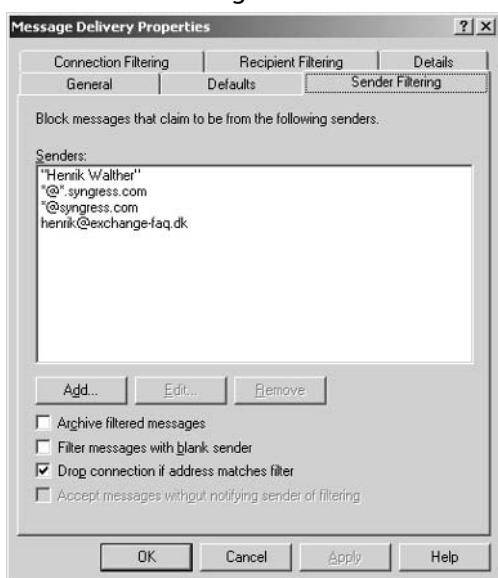
Filtering Recipients Not in the Directory

When the **Filter recipients who are not in the Directory** option is enabled, the system will filter all incoming e-mail messages sent to e-mail addresses not present in Active Directory. Spammers often use automatically generated e-mail addresses in an attempt to send messages to as many users as possible, so in many cases it might be a good idea to enable the Directory lookup feature. Another benefit of enabling this feature is that all e-mail sent to former employees (and that has been deleted and therefore no longer carries an e-mail address) will be filtered automatically. But the feature also has its drawbacks: Enabling it could potentially allow spammers to discover valid e-mail addresses in your organization because during the SMTP session, the SMTP virtual server sends different responses for valid and invalid recipients. As is the case with connection filtering, this feature doesn't apply to authenticated users and computers.

There's really not that many nitty-gritty parts under the Recipient Filtering tab, so let's move right on to the Sender Filtering tab.

Sender Filtering

There will always be some e-mail addresses or e-mail domains from which you don't want to receive messages. This is what the Sender Filtering tab is for; it's used to filter e-mail messages that claim to be sent by particular users. We can filter senders using several formats: We can specify individual e-mail addresses, we can filter a complete group of e-mail addresses using wildcards such as `*@syngress.com` (or even subdomains such as `*@*.syngress.com`), and we can use display names enclosed by quotes, such as "Henrik Walther" (see Figure 9.22).

Figure 9.22 The Sender Filtering Tab

Through this tab, we can control the following options:

- **Archive filtered messages** When this box is checked, all filtered e-mail messages are archived. Depending on the amount of filtered e-mail, the archive can become very large. For that reason, you should be sure to check the archive files on a regular basis. Note that the filtered message archive is created in the C:\Program Files\Exchsrvr\Mailroot\vsi folder.
- **Filter messages with blank sender** Spammers often use e-mail scripts to send spam messages, which often results in e-mail messages with blank From lines. If you enable this check box, all received e-mail messages with a blank From line will be filtered.
- **Drop connection if address matches filter** If this check box is enabled, an SMTP session to a sender's address that matches an address on the filter will be terminated immediately. This is quite a nice feature because, to deliver even more spam, the spammer needs to reconnect to your SMTP server.
- **Accept messages without notifying sender of filtering** Enabling this check box will prevent any nondelivery report (NDR) from being returned to the sender of filtered e-mail messages. Use this option if you don't want potential spammers

to know that their junk mail didn't reach its destination. If your organization receives a large amount of filtered e-mail, enabling this check box can drastically improve server and network performance.



REALITY CHECK...

The frequency with which users receive spam has increased significantly over the past couple of years. The best way to defend against spam nowadays is to use a so-called *defense-in-depth system* to block as much spam as possible, before it finally reaches the recipients' mailboxes. This basically means you have a multiple defense layer system, which includes firewalls, content-filtering servers, SMTP relay servers (also known as SMTP gateways), and the like. Unfortunately, such systems are only suitable for big organizations; most small and midsize organizations have neither the budget nor the IT staff to support them.

The Intelligent Message Filter

The built-in antispam features of Outlook and Exchange 2003 may be enough for some organizations, but many would say they are too basic for their Exchange environment. But before you rush out and invest money in an expensive third-party antispam solution, it's a good idea to consider some details about Microsoft's upcoming Exchange 2003 anti-spam add-on, which goes by the name Intelligent Message Filter (IMF) and should be released in the first half of 2004.

The IMF is based on the SmartScreen technology developed by Microsoft Research. The SmartScreen technology makes it possible for IMF to distinguish between legitimate e-mail and unsolicited e-mail or other junk e-mail. The SmartScreen technology's first appearance was with Microsoft's MSN Hotmail clients. SmartScreen tracks over 500,000 e-mail characteristics based on data from hundreds of thousands MSN Hotmail subscribers, who volunteered to classify millions of e-mail messages as legitimate or spam. Because of all the MSN Hotmail tracked e-mail characteristics, IMF can help determine whether each incoming e-mail message is likely to be spam.

Each incoming e-mail on an Exchange 2003 server with IMF installed is assigned a rating based on the probability that the message is

unsolicited commercial e-mail or junk e-mail. The rating is then stored in a database together with the message and contains a message property called a *spam confidence level*. This rating persists with the message when it's sent to other servers running Exchange and even other users' inboxes.

It's up to the Exchange admin to determine how IMF should handle e-mail messages. This is done by setting either a gateway threshold or a mailbox store threshold, both of which are based on the spam confidence level ratings. If the message has a higher rating than the gateway threshold allows, IMF will take the action specified at the Exchange gateway server level. If the message has a lower rating, it's sent to the recipient's Exchange mailbox store. If the message has a higher rating than the threshold of the mailbox store, it will be delivered to the user's mailbox, where it then will be moved to the Junk E-mail folder.

Things Worth Noting About the IMF

Keep the following points in mind when you're considering using the IMF:

- The spam confidence level rating only can be used by Outlook 2003 and Exchange 2003 or later.
- IMF can only be installed on a server running either Exchange 2003 Standard or Enterprise, not on Exchange 2000 and/or SMTP relay servers, as most third-party antispam solutions can.
- IMF will only be available to software assurance (SA) customers.
- IMF will be released in the first half of 2004.
- IMF is heuristics-based and will therefore improve over time.
- IMF will integrate with both Outlook 2003 and Outlook Web Access (OWA) 2003 trust and junk filter lists.
- Spam confidence levels (SCLs) can be set by the Administrator.

For more information about Microsoft's IMF, visit www.microsoft.com/exchange/techinfo/security/imfOverview.asp.

Microsoft also has plans to extend and enhance the Exchange messaging environments with the release of a newly developed Simple Mail Transfer Protocol (SMTP) implementation that acts as a perimeter or edge guard. The Exchange Edge services will enable you to better protect your e-mail system from junk e-mail and viruses as well as improve the efficiency of handling and routing Internet e-mail traffic. If every-

thing goes as planned, the Exchange Edge services should be released in 2005. For more information about Exchange Edge services, visit www.microsoft.com/exchange/techinfo/security/edgeservices.asp.



REALITY CHECK...

As mentioned earlier, the IMF add-on will be available exclusively to customers enrolled in Software Assurance, so many organizations won't be able to take advantage of it. Instead, they will have to invest in one of the third-party antispam products on the market.

Your A** Is Covered If You...

- Educate your users to use the Outlook 2003 junk e-mail filter.
- Take your time to understand each of the built-in spam-filtering possibilities of Exchange 2003.
- Thoroughly test any antispam functionality before implementing it in your production environment.
- Research what blacklists are and how they can help you combat spam and other unsolicited junk e-mail.
- Know about the antispam technologies Microsoft has on the horizon.

Chapter 10

Protecting

Against Viruses

In this Chapter

An essential part of protecting your Exchange environment is planning and deploying an appropriate virus defense system. The system should be able to protect against viruses at several levels throughout your organization's messaging system. Gone are the days when it was sufficient to install a single-layer system. Depending on the size of your Exchange environment, you should strive to scan for viruses in the perimeter network (the DMZ), typically by using SMTP gateways, at each Exchange server level, as well as the client level. Another important task is to educate your users so that they have a proper understanding of suspicious e-mail messages and therefore know how to deal with incoming e-mail, especially those including attachments.

In this chapter we'll discuss:

- E-mail viruses
- Server-side protection
- Client-side protection
- Educating your users
- Cleaning up after a virus outbreak

By the time you reach the end of this chapter, you will have a proper understanding of the types of virus that exist and why it's a good idea to use a multilayered defense system to combat viruses. Later you will learn some tips on how to educate your users to protect themselves against viruses. To finish the chapter, you'll see how to clean up after a virus outbreak using ExMerge.

E-Mail Viruses

Several years ago, most viruses spread primarily via infected diskettes, but with the introduction of the Internet, new methods of distribution mechanisms such as e-mail arose. Today e-mail is a vital form of communication between businesses, and for this reason, viruses are spreading much faster than ever before. In minutes an e-mail–borne virus can infect an entire organization. Depending on its effect, this can cost the organization millions of dollars in productivity loss and cleanup expenses.



BY THE BOOK...

Because the fight against viruses won't be over in the near future, it's absolutely mandatory to have a well functioning, solid virus defense system in your organization, preferably using a multilayered approach. It's only a question of one single user executing a malicious program attached to an innocent looking e-mail message cause havoc, which more specifically means that the virus could spread itself at the great and take down the Exchange messaging system in a matter of minutes.

Notes from the Underground...

Viruses, Trojans, and Worms

A *computer virus* is a program—more specifically, a piece of executable code—that has the ability to replicate itself over a network. Today computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to all types of files. The impact of viruses can range from making your computer crash during certain operations to deleting important files, possibly rendering your computer inoperable.

A *Trojan horse* is a malicious program that pretends to be an application. A Trojan is usually intended to do something the user does not expect, such as running some form of destructive code when a user executes a safe program such as Microsoft Word. Don't confuse a Trojan with a virus; a Trojan is a malicious program often distributed through e-mail–borne viruses such as worms.

A *worm* is a virus that resides in a computer's active memory and duplicates itself over and over. Worms often send copies of themselves to other computers, often through e-mail. Worms are

Continued

not attached to other programs or files. They really don't have to be, since they can replicate from computer to computer simply by residing in memory.

The first spectacular e-mail virus appeared in 1999 and was named Melissa. The Melissa virus hid in an attached Microsoft Word document (.doc file) and was let loose by an anonymous person, who originally posted it to a newsgroup as a Word document. Being unaware the Word document contained a malicious macro virus, a large number of the newsgroup readers started to download and open the document, thereby triggering the virus. Melissa was created in such a way that when triggered, it sent itself to the first 50 people in the respective user's personal address book. The e-mails that were sent to these people contained a friendly note that included the person's name, which caused the recipient to think it was from a friendly source and harmless and therefore to open it. Once the user opened the attachment, Melissa again created 50 e-mail messages and sent itself to the first 50 recipients of the user's personal address book. This resulted in Melissa being the fastest-spreading e-mail virus ever, causing e-mail users, especially midsize to large organizations, to shut down their messaging systems.

A little more than a year later, the I Love You virus was unleashed. I Love You was even simpler than the Melissa variant; it was nothing more than a script attached to an e-mail message. When users double-clicked it, the code was executed and sent itself to all recipients in the users' address books and started to corrupt files on the victim's machine.

Because the antivirus vendors were several hours behind the outbreaks in coming up with updated signatures, Melissa and the I Love You viruses created a big mess at organizations all around the world. Believe it or not, these two e-mail–borne viruses were actually the primary reason that messaging security from 2000 on got a lot more focused and effective than had been the case.

Since then we have been overwhelmed with many new kinds of viruses. The newest ones at the time of this writing are variants of Bagle, Nachi, and Netsky. The latest variant of Bagle (Bagle.K) is so mean that it hides itself in a password-protected .zip file. The password for the .zip file is contained in the body of the message, and the user is directed to use it when opening the file. Because the Bagle.K virus travels in a password-protected .zip file, antivirus software on the central mail gateway cannot scan it. The new .zip file variants have therefore caused many Exchange admins around the world to start blocking .zip files.

Unfortunately, viruses won't disappear in the near future. So far, many thousands of variants have been identified, and according to researchers, more than 200 new ones are created each month. With

numbers like those, it's quite safe to say that most organizations will deal regularly with virus outbreaks. No person using a computer is immune from viruses.

Server-Side Protection

You can use several approaches to protect your organization against viruses. The most efficient way is to put up a multilayered defense system, which scans for viruses at several levels in the organization. In this section we look at the options available for the server side. Many organizations, depending on size, configure one or more antivirus SMTP gateways in their perimeter network (the DMZ), which is one of the most efficient ways to block viruses. This way the viruses almost never enter the internal network and therefore can't do any harm to your internal servers or client machines. If this system is configured properly, you can catch between 95 and 99 percent of all e-mail–borne viruses. In conjunction with using antivirus SMTP gateways, most organizations also run Exchange-aware antivirus software on the Exchange servers themselves, preferably from another antivirus vendor than the software installed on the SMTP gateway server(s).



BY THE BOOK...

It would be naïve to think that it's enough to install an antivirus software on your organization's desktop clients. You must at the very least install antivirus software on the Exchange server itself, but if your organization's IT budget allows it, you should really strive for implementing an SMTP gateway with some effective antivirus software (preferably including multiple scanning engines) in your perimeter network (the DMZ), so that e-mail messages containing malicious code can be filtered before arriving at your internal network.

When dealing with the server side, we have three methods of protecting our Exchange messaging system against e-mail–borne viruses: We can install antivirus software on a dedicated SMTP gateway, install it directly on the Exchange server, or use a combination of the two. Using a combination is, of course, the most efficient and secure solution.

Exchange Server

Many organizations, especially small ones, only install Exchange-aware virus scanners directly on the Exchange server(s). The primary reason is they don't have the budgets to buy extra hardware dedicated as SMTP gateways. An Exchange-aware virus scanner typically needs to be installed on each Exchange server in the organization, since each Exchange server has its own set of mailbox and public folder stores. You can use one of three approaches to scan the content of the Information store. Even though we recommend you use antivirus software supporting the new Virus Scanning API (VSAPI) 2.5 in Exchange 2003, we thought it a good idea to summarize the methods each of the standards use to clean out the information store from potential malicious e-mail messages:

- **Messaging Application Programming Interface (MAPI)**

Traditionally, antivirus vendors have approached protecting Exchange servers by using MAPI to scan mailboxes and public folders. All MAPI-based antivirus products use an asynchronous hook to log on to each mailbox and public folder after having received a so-called MAPI alert indicating a new message or file has been stored in a mailbox or public folder. The rather old MAPI-based method (introduced in Exchange 5.5) has some severe limitations and disadvantages. MAPI-based scanners need to log on to any given mailbox in order to scan its content; for this reason, there could be situations in which the user gets to a virus infected e-mail message first. Another disadvantage is that MAPI-based scanners don't really understand single-instance storage (placing copy of an attachment in the Information Store that provides links to each recipient for whom the message is intended), meaning that if, for example, you send an e-mail message to 500 people, that message has to be scanned the same number of times, which would have a significant impact on the Exchange server's performance. In addition to scanning attachments multiple times, MAPI-based scanners also run the risk of letting unscanned messages through, especially in heavy load scenarios such as during a virus outbreak. MAPI-based scanners also have the limitation of not being able to scan IMAP, POP3, and OWA traffic. Furthermore, they cannot scan outgoing e-mail messages. As you can see, the list of drawbacks in using a MAPI-based scanner is lengthy, so you should avoid installing MAPI-based antivirus software on your Exchange 2003 server(s).

- **Extensible Storage Engine (ESE)** Due to all the drawbacks of using a MAPI-based scanner, a few antivirus vendors developed their own solutions. They built their products to take advantage of the Extensible Storage Engine (ESE) API, which makes it possible to scan e-mail messages before they are committed to the Information Store. This method is much more efficient than the MAPI-based method, which requires system-generated logons into every mailbox. The antivirus vendors accomplished this improvement by momentarily swapping out the ESE.DLL file while it loads its own code, thereby providing an active entry point into the ESE system, then reinserting the Exchange SES.DLL so that the Information Store initialization could continue. Among the vendors using this approach are Trend Micro and Sybari. Although the ESE-based scanners have several benefits over the MAPI-based versions, you should still strive to install a VSAPI 2.5-based scanner on your Exchange 2003 server.
- **Antivirus API (AVAPI) 1.0 and Virus Scanning API (VSAPI) 2.0** It wasn't only the antivirus vendors who were unsatisfied with the MAPI-based scanning method. Microsoft also knew it had to do something about it, so it developed and released AVAPI. AVAPI made it possible for antivirus vendors to integrate their AV code directly into the Information Store, but even though AVAPI took care of all the problems we faced with the MAPI-based version, several new problems arose. For that reason, Microsoft developed and introduced VSAPI 2.0, which was included in Exchange 2000 Service Pack 1. VSAPI 2.0 fixed most of the problems in AVAPI 1.0.
- **VSAPI 2.5** Exchange 2003 presents us with VSAPI 2.5, which has been improved even further. Among the improvements are virus-scanning APIs that allow antivirus vendor products to run on Exchange 2003 servers that do not have resident Exchange mailboxes (for example, gateway servers or bridge-head servers). In addition, VSAPI 2.5 allows antivirus vendor products to delete messages and send messages to the sender, and additional virus status messages allow clients to better indicate the infection status of a particular message. VSAPI 2.5 also makes it easier for vendors to write SMTP event sink scans.

To see a complete list of vendors supporting VSAPI, visit the Microsoft site: www.microsoft.com/exchange/partners/antivirus.asp.

Notes from the Underground...

Should I Run a File-Level Virus Scanner on My Exchange 2003 Server?

You might wonder if you should run a file-level virus-scanner on your Exchange server. The answer is, it depends. You should be aware that file-level scanners scan a file when the file is used or at a scheduled interval, and these scanners may lock or quarantine an Exchange log or a database file while Exchange 2003 tries to use the file. This behavior may cause a severe failure in Exchange 2003 and may also generate -1018 errors. You should also note that file-level scanners don't provide protection against e-mail viruses, since they aren't capable of scanning the Information Store. If you decide to install a file-level virus scanner on your Exchange server(s), please be aware that you must exclude certain folders. Failing to do so will most likely result in corrupt databases (.edb and .stm files) and log files at some point. The folders you should exclude from both on-demand file-level scanners and memory-resident file-level scanners are as follows:

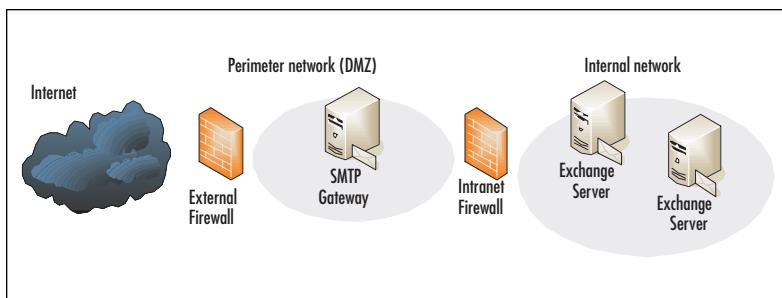
- Exchange databases and log files across storage groups and MTA files, which by default are located in C:\Program Files\Exchsrvr\Mdbdata.
- Other log files such as those in C:\Program Files\Exchsrvr\server_name.log directory.
- The Mailroot virtual server folder, located in C:\Program Files\Exchsrvr.
- The working folder that is used to store streaming .tmp files used for message conversion, by default C:\Program Files\Exchsrvr\Mdbdata.
- Site Replication Service (SRS) files, by default located in C:\Program Files\Exchsrvr\Srsdata.
- Microsoft Internet Information Services (IIS) system files, located in C:\Windows\System32\Inetsrv.
- Checkpoint (.chk) files, default located under C:\Program Files\Exchsrvr\Mdbdata.
- The temporary folder used for offline maintenance with utilities such as Eseutil.exe; by default this is the folder from which the .exe file is run.

For more specific details, see Microsoft KB article 823166, "Overview of Exchange Server 2003 and Antivirus Software," at www.support.microsoft.com/?id=823166.

SMTP Gateway

A popular approach to dealing with viruses today is to set up one or more SMTP gateways, typically placed in the perimeter network (the DMZ). The purpose of these SMTP gateways is to scan all incoming e-mail messages for viruses before they reach your Exchange server(s) on the internal network (see Figure 10.1). The primary benefit of using SMTP gateways is that e-mail–borne viruses are detected and removed before they reach the mission-critical Exchange server(s).

Figure 10.1 Antivirus SMTP Relay Setup



Even though you run virus scanners on your gateway, it is recommended that you have some sort of Exchange-aware virus scanner installed on your internal Exchange servers as well. The reason is that antivirus SMTP gateways only protect you from viruses received from external mail servers, which means that they won't detect any internal e-mail–borne virus in your network.

Today you can get many Exchange-aware antivirus products and products specifically designed to be installed on a SMTP gateway. Table 10.1 lists some of the more popular vendors and their products.

Table 10.1 Antivirus Exchange and SMTP Gateway Vendors and Products

Vendor	Product	Link
GFI	MailSecurity for Exchange/SMTP	www.gfi.com
Symantec	Symantec Mail Security for Microsoft Exchange	www.symantec.com
Trend Micro	ScanMail Suite for Microsoft Exchange	www.trend.com

Continued

Table 10.1 Antivirus Exchange and SMTP Gateway Vendors and Products

Vendor	Product	Link
ClearSwift	MailSweeper Business Suite	www.mimesweeper.com
Panda Software	Panda BusinessSecure Antivirus with Exchange	www.pandasoftware.com
F-Secure	F-Secure Antivirus for Microsoft Exchange	www.f-secure.com
Red Earth Software	Policy Patrol Enterprise	www.policypatrol.com
CMS	Praetor for Microsoft Exchange Server	www.cmsconnect.com
RAV	RAV AntiVirus for Mail Servers	www.ravantivirus.com
Sybari	Sybari's Antigen for Microsoft Exchange	www.sybari.com

Notes from the Underground...

Considerations in Choosing Your Antivirus Software

In selecting antivirus software, we are faced with several decisions as to which software package suits our organization best. Some of the most interesting decisions are based on vendor support, support for multiple antivirus engines, and performance. Because antivirus software has become one of the most critical components in protecting our network from security threats, you must carefully plan, test, and then implement the antivirus solution you have chosen.

Client-Side Protection

Even though you have virus scanners running both on your SMTP gateways and the Exchange servers themselves, you should also run antivirus software on your desktop client machines. Don't forget that your client machines can be infected through sources other than e-mail, such as diskettes (yes, they are still used) or CDs or through a Web site con-

taining embedded malicious code opened with Internet Explorer. In addition, you could be lucky and have some of those “smart users” who think it a clever idea to retrieve their private e-mail from some kind of POP3 account.



BY THE BOOK...

The client side of Outlook 2003 has improved a great deal over previous versions. This new version includes several new security enhancements that limit the possibilities that a client machine will be affected by a malicious virus. In particular, the Outlook 2003 attachment-blocking features enhance security on the client side. But because Outlook or Windows doesn’t include an antivirus product natively, it’s still mandatory that you install a client-based antivirus product on each client machine in your organization.



REALITY CHECK...

In today’s world, it’s not enough to run antivirus software on your organization’s client desktop machines, with the proliferation of spyware, malware, and adware plaguing the Internet. To fight these types of threats, you should consider installing a software-based firewall (such as Zone Alarm) and a powerful security and personal privacy tool such as PestPatrol or Adaware that detects and eliminates destructive pests such as Trojans, spyware, adware, and hacker tools.

Educate Your Users

One of the best weapons against e-mail–borne viruses is educating your users. Your users should know how to react when dealing with e-mail messages, especially those including attachments. They should be aware that just because they know the sender of a given e-mail message, that doesn’t necessarily mean it’s harmless and therefore can be opened. You should make it a habit to inform your users of any high-risk viruses making the rounds of the Internet, but don’t overreact! If you send too many virus warnings to your users, they tend to take them less seriously. It’s up to you how you find the golden middle way.

In your security policy, include information about what your users are allowed to do and how they should react when dealing with e-mail and attachments, such as what type of attachment they may open. It would also be wise to tell them why it's a bad idea to send virus warnings received from anyone besides the IT Department to other users on the network.



REALITY CHECK...

If you're going to keep up to date with new viruses, it's generally a good idea to check the different antivirus product vendors' sites because they are updated almost on the fly. But did you know that Microsoft also has an antivirus-related site? Check it out at www.microsoft.com/security/antivirus. Not only is this site updated with new antivirus information, it also announces new initiatives such as the Antivirus Reward Program.

Default Outlook 2003 Attachment Blocking

It might come to no surprise that no matter how much you educate your users, there will always be some who don't think twice before opening an attachment containing malicious code. Therefore, it's a good idea to block as many extensions as possible, before they arrive at the user's mail client. This process can be done by your antivirus product, depending on your antivirus vendor. If your vendor's product doesn't handle this task, fear not—Outlook will do it for you. Table 10.2 lists the types of extensions Outlook 2003 blocks by default.

Table 10.2 Extensions Blocked by Outlook 2003

Extension	Description
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.app	Microsoft Visual FoxPro application
.asx	Windows Media Audio or Video shortcut
.bas	Visual Basic class module
.bat	Batch file
.cer	Certificate file

Continued

Table 10.2 Extensions Blocked by Outlook 2003

Extension	Description
.chm	Compiled HTML Help file
.cmd	Windows NT Command script
.com	MS-DOS program
.cpl	Control Panel extension
.crt	Security certificate
.csh	KornShell script file
.exe	Program
.fxp	Microsoft Visual FoxPro compiled program
.hlp	Help file
.hta	HTML program
.inf	Setup information
.ins	Internet Naming Service
.isp	Internet Communication settings
.isp	JScript Script file
.js	JScript Script file
.jse	Jscript Encoded Script file
.ksh	KornShell script file
.lnk	Shortcut
.mda	Microsoft Access add-in program
.mdb	Microsoft Access program
.mdt	Microsoft Access workgroup information
.mdw	Microsoft Access workgroup information
.mde	Microsoft Access MDE database
.mdz	Microsoft Access wizard program
.msc	Microsoft Common Console document
.msi	Windows Installer package
.msp	Windows Installer patch
.mst	Visual Test source files
.ops	Office XP settings
.pcd	Photo CD image
.pif	Shortcut to MS-DOS program
.prf	Microsoft Outlook profile settings
.prg	Microsoft Visual FoxPro program

Continued

Table 10.2 Extensions Blocked by Outlook 2003

Extension	Description
.pst	Microsoft Outlook Personal Folders file
.reg	Registration entries
.scf	Windows Explorer command
.scr	Screen saver
.sct	Windows Script Component
.shb	Shell Scrap Object
.shs	Shell Scrap Object
.url	Internet shortcut
.vb	VBScript file
.vbe	VBScript encoded script file
.vbs	Visual Basic Script file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file

We also suggest you consider whether your users should be allowed to receive .doc, .xls, or .zip files. To see how to configure Outlook 2003 to block additional attachment types, read MS KB article 837388, “How to configure Outlook to block additional attachment file name extensions,” at www.support.microsoft.com/?id=837388.



REALITY CHECK...

If you’re one of the Exchange admins who prefer doing everything through a GUI, you’re in luck: Several third-party utilities can add or remove file types from the attachment block list in Outlook 2003. For a thorough list, visit the Slipstick Systems site: www.slipstick.com/addins/antivirus.htm.

Cleaning Up After a Virus Outbreak

You might wonder what to do if you should learn one day that your antivirus product's signature isn't up to date, and your users' mailboxes are suddenly bombarded by some kind of malicious e-mail virus. Well, if you're lucky, the vendor will quickly provide a signature update, and you might have the opportunity to scan all mailboxes on your Exchange server and have the virus scanner remove any infected messages from the mailboxes. But what do you do if that isn't an option? ExMerge comes to the rescue. You probably know ExMerge as a utility to export and import mailboxes to or from .pst files during Exchange server migrations, but ExMerge can be used for a lot more, including being used as a virus cleanup utility.



BY THE BOOK...

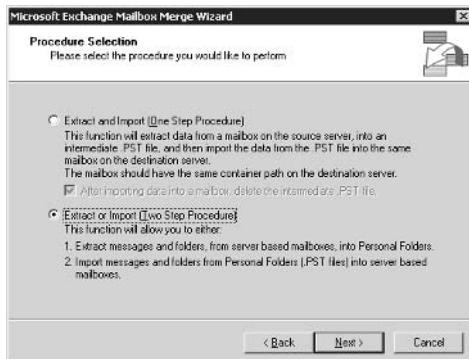
Administrators frequently use the ExMerge.exe tool to back up mailbox data or migrate it from one mailbox to another. ExMerge is designed to copy mailbox data into a personal folder file (.pst) that can then be imported to another mailbox. However, you can also use ExMerge to extract specific messages from mailbox stores to .pst files and then delete the .pst files instead of importing them into new mailbox stores.

In this section you'll see step by step how it's possible to strip a specific e-mail–borne virus from your user's mailboxes using the ExMerge utility. Let's begin:

1. Start by grabbing the most recent version of ExMerge 2003 from www.microsoft.com/exchange/downloads/2003.asp.
2. Place a copy of ExMerge in the C:\Program Files\Exchsrvr\Bin folder.
3. Make sure you have the proper permissions to access your users' mailboxes. (Read more in MS KB 262054, "XADM: How to Get Service Account Access to All Mailboxes in Exchange 2000," at support.microsoft.com/?id=262054.)
4. Execute **Exmerge.exe**, then click **Next**.

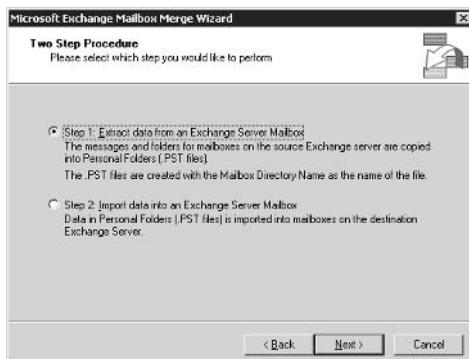
5. Select **Extract or Import (Two Step Procedure)**, and click **Next** (see Figure 10.2).

Figure 10.2 ExMerge Extract or Import (Two Step Procedure)

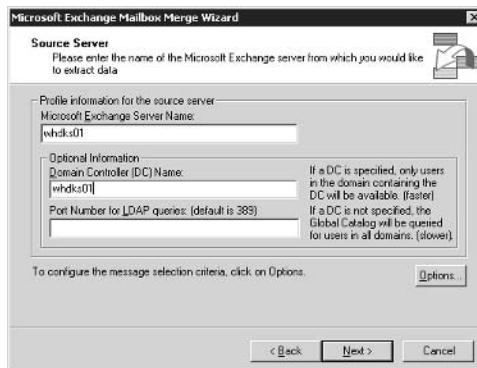


6. Choose **Step 1: Extract data from an Exchange Server Mailbox**, and click **Next** (see Figure 10.3).

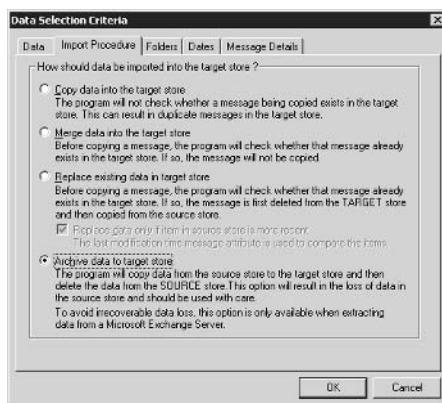
Figure 10.3 Choose to Extract Data from an Exchange Server Mailbox



7. Specify the names of your Exchange server and domain controller (see Figure 10.4).

Figure 10.4 Specify Exchange Server and Domain Controller

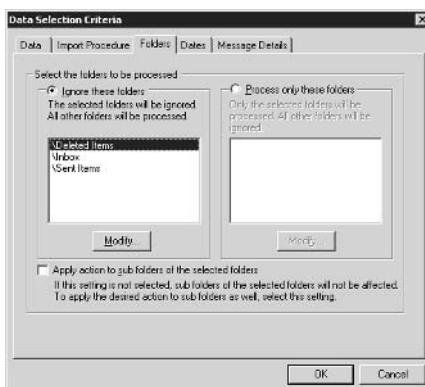
- Click **Options**, then choose the **Import Procedure** tab (see Figure 10.5) and select **Archive data to target store**. Be sure to read this option carefully before continuing.

Figure 10.5 The Import Procedure Tab

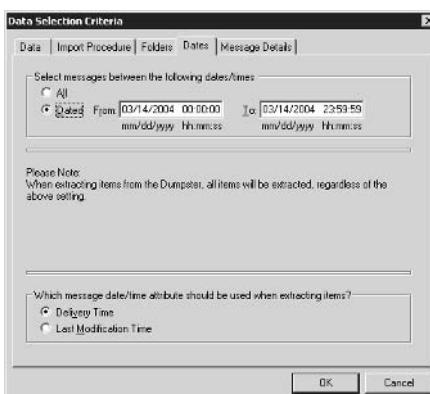
- Now it's time to tell ExMerge what messages need to be ExMerged from the mailboxes. Select the **Folders** tab. You will be prompted with the warning box shown in Figure 10.6.

Figure 10.6 ExMerge Warning Box

10. Click **Yes** in the warning box. You will see the Folders tab (see Figure 10.7).

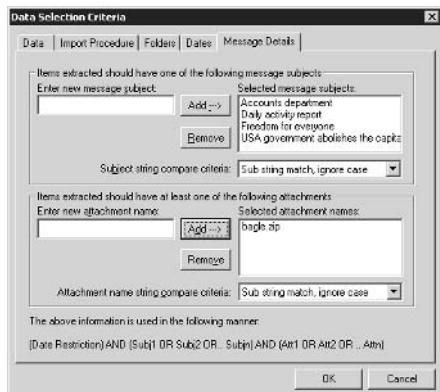
Figure 10.7 The Folders Tab

11. In the Folders tab, you have the option of specifying which folders in each mailbox should be processed. When you have made your selection, you can continue. Click the **Dates** tab (see Figure 10.8).

Figure 10.8 The Dates Tab

12. In the Dates tab, you can select a date range, if you know the specific date your Exchange mailboxes started to be infected. Now click the **Message Details** tab (see Figure 10.9).

Figure 10.9 The Message Details Tab

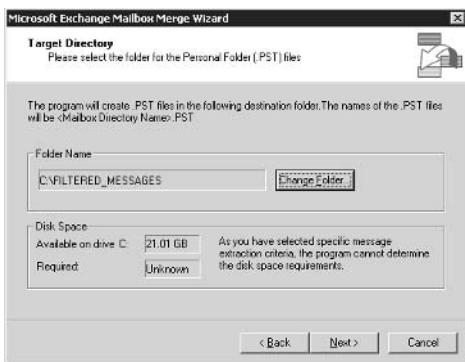


13. The Message Details tab is probably the most important one, since this is where you enter the message subject and attachments to look for. This example specifies a few of the message subject lines relating to the Bagle.E worm. Click **OK**, then click **Next**. You'll be presented with the Microsoft Exchange Mailbox Merge Wizard. Make your mailbox selections and click **Next** (see Figure 10.10).

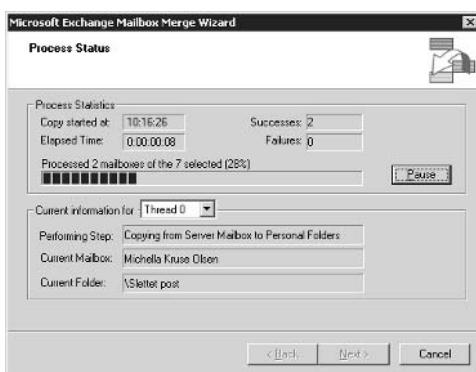
Figure 10.10 ExMerge Mailbox Selections



14. Choose **Default Locale** of the mailboxes, then click **Next**.
15. Now specify the destination folder of the stripped messages' .pst files (see Figure 10.11). Click **Next**, then click **Next** again.

Figure 10.11 ExMerge Specify Target Folder

16. ExMerge now starts to ExMerge any messages matching the criteria we defined earlier (see Figure 10.12).

Figure 10.12 ExMerging Data Matching Criteria

17. When the operation has completed successfully, click **Finish**.

ExMerge has now filtered any messages matching the criteria we specified earlier. These messages can be found in the folder we specified in Figure 10.11. One thing that's important to remember is that using this method will only filter any matching messages from your users' mailboxes, so if any of your users use local .pst files, they will not be checked.

Your A** Is Covered If You...

- Know how to differentiate the existing types of viruses and other malicious programs from each other.
- Use a multilayered defense system to protect against e-mail–borne viruses.
- Use a multiple virus scanning engine product.
- Educate your users about the potential risks of e-mail use.
- Implement a strict attachment-blocking policy.
- Take time to understand how you can clean up after a virus outbreak.

Chapter 11

Auditing Exchange

In this Chapter

Auditing Exchange usage is essential. If you are not currently auditing your Exchange system, you might not even realize you are having security problems. Still worse, you could discover that you have a security problem but not be able to track it down. Auditing will help you in these tasks. The auditing process breaks down into a couple of categories: Windows 2000/2003 event auditing and Exchange 2000/2003 diagnostics logging.

In this chapter we examine the following topics:

- Windows 2000/2003 auditing
- Auditing Changes to the Exchange Configuration
- Exchange Diagnostics Logging
- Microsoft Operations Manager and Exchange 2003

By the time you reach the end of this chapter, you will be aware of some of the options you have in regard to auditing your Windows 2000/2003 and Exchange 2000/2003 systems.

Windows 2000/2003 Auditing

The Event Log Service takes care of all Windows 2000/2003 auditing. You probably know the Event Log Service pretty well, so we won't go into any details here describing it or show you how it works. Instead, let's look at a few tips on what you should audit in regard to Exchange 2000/2003.



BY THE BOOK...

The Event Log Service records all types of events on the system (server). The service consists of several different logs: the Application log, the Security log, the System log, the Directory Service log, the DNS Server log, and the File Replication log.

Dealing with Exchange 2000/2003 auditing, the interesting log is the Security log, which audits everything specified in the Audit Policy in the Local or Domain Policies.

One of the essential security auditing tools that you need to take advantage of is the built-in Windows 2000/2003 event auditing that you can turn on through the Local Security Policy or collectively for an entire organizational unit (OU) of computers through an Active Directory Group Policy Object. Figure 11.1 shows the typical audit policy events that it's a good idea to configure.

Figure 11.1 Audit Policy Events for Exchange Servers

The screenshot shows the Windows Local Security Settings dialog box. The left pane displays a tree view of security settings, with the 'Audit Policy' node expanded. The right pane lists audit policy events with their corresponding security settings:

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	Failure
Audit system events	Success, Failure

The events that we typically choose to audit notify us when someone accesses the server, when someone makes security or account-related changes to the server, and when someone restarts the server. Table 11.1 shows the events that we typically tend to log, along with an explanation of each.

Table 11.1 Recommended Audit Policy Events

Policy	Explanation
Audit account logon events	Audits logons using domain accounts.
Audit account management	Audits changes to accounts, such as reset passwords or group membership changes. This audit event does not always generate the detail we'd like, such as whether an account is enabled or disabled—just that the account is changed.
Audit logon events	Audits logons using accounts that are local to the member server.
Audit policy changes	Audits policy changes such as changing the audit policy.
Audit system events	Audits events such as system shutdown or restart.

Although we prefer not to configure an audit policy that logs every single activity that occurs on a server, we also shy away from minimal auditing or auditing that examines only failures. Each additional audit policy you place on the server increases the load on the server by some amount, and it increases the size of the security log files. If you are truly concerned about logging events that could affect the security of your system, you will log not only events in which someone has tried and failed to accomplish something; you will also look at events in which someone has tried and succeeded. This has been our philosophy for some time and it has served us well, though some people think we are a bit paranoid.

For more information on Windows event auditing, we recommend you check the following Microsoft KB articles:

- 299475, “Windows 2000 Security Event Descriptions (Part 1 of 2),” www.support.microsoft.com/?id=299475
- 301677, “Windows 2000 Security Event Descriptions (Part 2 of 2),” www.support.microsoft.com/?id=301677
- 314955, “How to Audit Active Directory Objects in Windows 2000,” www.support.microsoft.com/?id=314955

- 252412, “How to Enable Local Auditing Policies on Windows 2000,” www.support.microsoft.com/?id=252412



REALITY CHECK...

Windows event logs can grow to quite a significant size very quickly. The default size for these logs in Windows 2000 is 512KB, and they overwrite only data that is older than seven days. In Windows 2003, they are set to 16,384KB (16MB) by default. Administrators frequently ignore the warning that an audit log is full and then later wonder why they don’t have complete information in their audit logs. If you’re running Exchange 2003 on Windows 2000-based server, we recommend that you increase the size of your audit logs to a useful and reasonable size, such as 16,384KB (16MB), which is the default in Windows 2003 Server.

Depending on your messaging environment, you might also want to consider investing in reporting software, such as Microsoft Operations Manager (MOM), for which there are several messaging environment management packages (from both third parties and Microsoft). You can download a free management package specifically developed for Exchange 2003 servers. Read more about MOM and the Exchange 2003 management package at the following links:

- Microsoft Operations Manager homepage:
www.microsoft.com/mom
 - Download details, Exchange 2003: Management Pack:
www.microsoft.com/downloads/details.aspx?FamilyId=56D036BF-8DD3-4993-BF07-07F99F1D5CC4&displaylang=en
-

Auditing Changes to the Exchange Configuration

It’s important that you know where you control auditing so that you can track Exchange organization changes. Let’s look at this concept now.



BY THE BOOK...

No single auditing category will allow you to track every possible change that someone makes to an Exchange 2000 or Exchange

2003 server. To understand where to enable auditing to follow Exchange organization changes, you must understand where the configuration data is actually stored and where it is modified.

Almost all the configuration information in Exchange 2000/2003 is stored in the Active Directory's configuration partition. The configuration partition is replicated between all domain controllers in the entire organization. The configuration can be changed on any domain controller in the forest.

Auditing changes to the Exchange organization requires enabling auditing through a Group Policy Object (preferably the Default Domain Controller Policy) that affects domain controllers in each domain. You must enable the Audit Policy setting Audit Directory Service Access for the domain controllers, not the Exchange servers. Enabling successes will show any successful changes to anything in the configuration partition, including the Exchange configuration. If you are using Windows 2000 Active Directory or an Active Directory that has been upgraded from Windows 2000, you also need to enable auditing on the Microsoft Exchange container in the Configuration container using ADSIEDit.

Once auditing is enabled for the Exchange configuration and Directory Service Access auditing is enabled on the domain controllers, you will find events in the domain controller's event logs indicating the type of activity. The domain controller on which this information is found is the one on which the change was made; the audit event can be found on the domain controller that was being used by Exchange System Manager when the change was made. The level of detail is surprisingly good, even when changing a single attribute.

Notes from the Underground...

When You Can't Find Information on That Specific EventID Error

We have all tried it—looking up information on a specific EventID error from one of our servers' Event logs. Often it's an EventID error we haven't seen before and do not know how to correct. To handle such situations, we recommend you visit www.eventid.net. At this site you can look up information on specific EventID errors. You can also provide information about an EventID that might not be listed there. If you're a serious Exchange or other type of server admin, you might already

Continued

know this site, since it has existed for several years, but for those readers who aren't aware of it, we suggest you give it a visit right away.

Exchange Diagnostics Logging

There are also a few categories that you should enable for Exchange diagnostics logging. In Exchange 5.5, you could find the Diagnostics Logging property page in a couple of different locations, but in Exchange 2000 and Exchange 2003, these events are all centrally located on a single property page on the properties of each server.

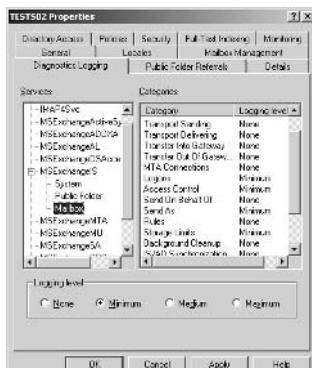


BY THE BOOK...

Diagnostics logging levels determine which Exchange 2000/2003 events are written to the Windows 2000/2003 application event log. You normally log only critical events; however, when problems occur, diagnostics logging enables you to change the logging levels to capture greater detail. Events can range from significant events such as application failures to moderately important events such as the receipt of messages across a gateway or events relevant only to debugging. There are a few security-related diagnostic logging options as well, which we discuss throughout this section.

To enable any type of diagnostics logging for Exchange, you must configure the Diagnostics Logging property page for each server individually. Figure 11.2 shows the Diagnostics Logging property page for an Exchange 2003 server.

Figure 11.2 Diagnostics Logging for an Exchange 2003 Server



To accurately track usage of the Exchange mailboxes, you should enable a number of Exchange diagnostic logging categories. Table 11.2 lists these categories and the locations in which you will find them.

Table 11.2 Diagnostics Logging Categories for Exchange 2000/2003 Servers

Category	Explanation
MSEExchangeIS Mailbox Logons	Tracks access to mailboxes
MSEExchangeIS Mailbox Access Control	Logs events when users attempt to access a mailbox to which they have no or insufficient permissions
MSEExchangeIS Mailbox Send As	Logs events when a user uses the Send As permission
MSEExchangeIS Public Folder Logons	Tracks access to the public folder store
MSEExchangeIS Public Folder Access Control	Logs events when users attempt to access a public folder to which they have no or insufficient permissions
MSEExchangeIS System Virus Scanning	Logs events related to virus-scanning programs that are AVAPI 2.0 compliant
IMAP4 Connections	Logs information about IMAP4 client connections such as IP address
IMAP4 Authentication	Logs information about IMAP4 client authentication
POP3Svc Connections	Logs information about IMAP4 client connections such as IP address
POP3Svc Authentication	Logs information about POP3 client authentication

Although these are not the only categories of events you can log with Exchange 2003, we consider them the bare essential events from a security perspective. Many organizations have requirements for logging additional information such as replication, X.400 MTA connections, and transport-related events. The categories in Table 11.2 should be set to at least minimum.

When you are scanning your event logs, looking for possible intrusions or things that just don't look right, the event IDs in Table 11.3

could be helpful. These are by no means the only events you should be looking at, but they will help you narrow down the events that indicate when a user is accessing the store.

Table 11.3 Exchange 2000/2003 Security-Related Events Found in the Application Log

Source	ID	Explanation
MSEExchangeIS Mailbox	1009	Mailbox access
MSEExchangeIS Mailbox	1016	Mailbox access by someone other than the mailbox owner
MSEExchangeIS Mailbox	1029	Attempted access to mailbox by unauthorized user or user with insufficient rights
MSEExchangeIS Mailbox	1032	Successful use of Send As right
MSEExchangeIS Public	1235	Attempted access to public folder by unauthorized user or user with insufficient rights
IMAP4SVC	1000	IMAP4 client connection established
IMAP4SVC	1010	IMAP4 client successfully logged on
IMAP4Svc	1011	IMAP4 client authentication failed
IMAP4Svc	1043	Maximum number of invalid commands from IMAP4 client has been reached; connection dropped
POP3SVC	1000	POP3 client connection established
POP3SVC	1010	POP3 client successfully logged on
POP3SVC	1011	POP3 authentication failed
POP3SVC	1043	Maximum number of invalid commands from POP3 client has been reached. Connection dropped



REALITY CHECK...

Be careful when you specify type of logging level, because medium and especially maximum logging can put quite a performance load on your Exchange servers. For most environments, minimum logging should be sufficient.

Microsoft Operations Manager and Exchange 2003

Microsoft Operations Manager (MOM) with the Exchange 2003 Management Pack is a very interesting product (for relatively large organizations, though). With MOM and the Exchange 2003

Management Pack, you can be proactive by monitoring the performance, availability, and security features of Exchange 2003, alerting you to events that have a direct impact on server availability while filtering out events that require no action. By detecting, alerting on, and automatically responding to critical events, the management pack helps identify, correct, and prevent possible Exchange service outages.

This management pack is designed to detect indications of a potential service interruption and to immediately send an alert to your Exchange administrator if a service interruption occurs. It can proactively monitor over 1,600 events, performance counters, services, and Internet protocols, such as:

- Directory Service Access (DSAccess)
- Microsoft Exchange Information Store service
- Extensible Storage Engine (ESE)
- Message transfer agent (MTA)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP3)
- Internet Message Access Protocol (IMAP4)

MOM includes many Exchange-specific reports to help you quickly identify and correct Exchange issues. With these reports, it's possible to analyze and graph performance data to understand usage trends, perform accurate load balancing, and manage system capacity.

The following reports are available in the Exchange 2003 Management pack:

- **Health monitoring and operations report** Get a summary of Exchange 2003 health and usage, server availability, and configuration of Exchange 2003 servers, databases, and mailboxes.
- **Server availability report** Find out the percentage of server availability for computers running Exchange 2003 during the specified time period. The percentage of availability and unavailability is listed along with the reasons that the servers were unavailable.

- **Usage and health report** Get information about server usage and the health of computers running Exchange 2003 based on key Exchange and SMTP performance counters. The report presents daily totals and averages for the specified time period. The highest average for each counter in a 30-minute period is also included, with the time of occurrence for the highest average.

Additional Exchange 2003 Management Pack reports include:

- Mailbox and folder sizes
- Disk usage
- Mailboxes per server
- Traffic analysis

A nice thing about MOM is that several third-party vendors such as Hewlett-Packard, Quest, and Veritas are developing their own packages that can integrate directly into MOM. We suggest you read more about this trend at the Microsoft Operations Manager site at www.microsoft.com/mom.

Your A** Is Covered If You...

- Know what options you have available in regard to Windows 2000/2003 and Exchange 2000/2003 auditing.
- Set up a reasonable Windows 2000/2003 audit policy based on the recommendations in this chapter.
- Test the different Exchange Diagnostics Logging settings and consider implementing the ones we suggested in this chapter.

Appendix

Planning Server Roles

and Server Security

In this Appendix:

Planning an effective security strategy for Windows Server 2003 requires an understanding of the roles that different servers play on the network and the security needs of different types of servers based on the security requirements of your organization. Securing the servers is an important part of any network administrator's job.

- Understanding Server Roles
- Planning a Server Security Strategy
- Planning Baseline Security
- Customizing Server Security

In this appendix, we will first review server roles and ensure that you have an understanding of the many roles Windows Server 2003 can play on the network. Then we will delve into how to plan a server security strategy. We will examine how to choose the right operating system according to security needs, how to identify minimum security requirements for your organization, and how to identify the correct configurations to satisfy those security requirements.

Understanding Server Roles

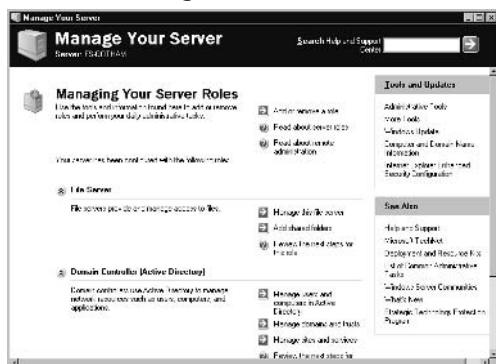
When Windows Server 2003 is installed on a computer, it provides a wide variety of tools and functionality. However, additional features may still need to be installed on the server to bring clients the services they need. The server may need to supply file and print services, authenticate users, or support a local intranet Web site. Until Windows Server 2003 is configured to supply these services, clients will be unable to use the server in a manner that is required by the organization.

Server roles are profiles that are used to configure Windows Server 2003 to provide specific functionality to the network. When you set up a server to use a specific role, various services and tools are enabled or installed, and the server is configured to provide additional services and resources to network clients. Roles are applied to machines using the Configure Your Server Wizard and managed using the Manage Your Server tool.

As shown in Figure A.1, Manage Your Server provides information about the roles that are currently configured for a server, and it provides the ability to add and remove roles from a server. Depending on your server's settings, this tool will start automatically upon logon. If you've checked the **Don't display this page at logon** check box at the bottom of this window, Manage Your Server will not start automatically. You can start it manually by selecting **Start | Administrative Tools | Manage Your Server**.

As shown in Figure A.1, there are a variety of items in Manage Your Server's main window. The left side of the window lists the roles currently configured for the server. Beside each entry, there are buttons that relate to the corresponding role. These buttons differ from role to role, and they are used to invoke other tools for managing the role or to view information on additional steps that can be taken to configure, administer, and maintain the role.

Figure A.1 The Main Manage Your Server Window



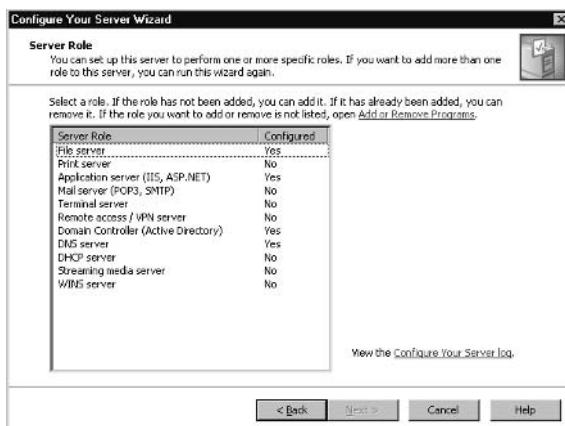
Near the top of the Manage Your Server window are three buttons. Two of these are used to obtain additional information about roles and remote administration. The other button, labeled **Add or remove a role**, is used to invoke the Configure Your Server Wizard. You can also start the Wizard by selecting **Start | Administrative Tools | Configure Your Server**.

When the Configure Your Server Wizard starts, it informs you of possible preliminary steps that need to be taken before a new role is added. As shown in Figure A.2, these steps include ensuring that network and Internet connections are set up and active for the server, peripherals are turned on, and your Windows Server 2003 installation CD is available. When you finish reading this information, click the **Next** button to have the Wizard test network connections and continue to the next step.

Figure A.2 Preliminary Steps of the Configure Your Server Wizard



In the next window, shown in Figure A.3, roles that are available to add and remove through the Wizard are listed in the **Server Role** column; the **Configured** column indicates whether the role has been previously installed. If you want to install a role that isn't listed here, click the **Add or Remove Programs** link to open the Add or Remove Programs applet (in the Windows Control Panel), where you can configure additional services.

Figure A.3 Configuring Server Roles

In Figure A.3, you can see that there are 11 different roles that can be applied to Windows Server 2003 through the Configure Your Server Wizard. These roles are as follows:

- **Domain controller** This role is used for authentication and installs Active Directory on the server.
- **File server** This role is used to provide access to files stored on the server.
- **Print server** This role is used to provide network printing functionality.
- **DHCP server** This role allocates IP addresses and provides configuration information to clients.
- **DNS server** This role resolves IP addresses to domain names (and vice versa).
- **WINS server** This role resolves IP addresses to NetBIOS names (and vice versa).
- **Mail server** This role provides e-mail services.
- **Application server** This role makes distributed applications and Web applications available to clients.
- **Terminal server** This role provides Terminal Services for clients to access applications running on the server.
- **Remote access/VPN server** This role provides remote access to machines through dial-up connections and virtual private networks (VPNs).

- **Streaming media server** This role provides Windows Media Services so that clients can access streaming audio and video.

After you select the role to add to the server, click **Next** to step through the process of setting up that role. Each set of configuration windows is different for each server role. Also, although multiple roles can be installed on Windows Server 2003, only one role at a time can be configured using the Configure Your Server Wizard. To install additional roles, you need to run the Wizard again.

Before setting up a server role, it is important to understand each of the roles that can be applied to Windows Server 2003 so you select the roles most appropriate for the server's use and for your organization. In the sections that follow, we will discuss these roles in greater detail and examine how they are installed with the Configure Your Server Wizard and other tools.

Domain Controllers (Authentication Servers)

Domain controllers are a fundamental part of a Microsoft network because they are used to manage domains. An important function of a domain controller is user authentication and access control. By combining authentication and access control, a domain controller can permit or deny access to network services and resources on a user by user basis.

Active Directory

To perform these functions, the domain controller must have information about users and other objects in a domain. In Windows 2000 and Windows Server 2003, this data is stored in *Active Directory* (AD), which is a directory service that runs on domain controllers.

When AD is installed, the server becomes a domain controller. Until this time, it is a member server that cannot be used for domain authentication and management of domain users or other domain-based objects. This does not mean, however, that AD can be installed on every version of Windows Server 2003. It can be installed on Standard Edition, Enterprise Edition, and Datacenter Edition, but servers running the Web Edition of Windows Server 2003 cannot be domain controllers. Web Edition servers can be only stand-alone or member servers that provide resources and services to the network.

A Windows Server 2003 computer can be changed into a domain controller by using the Configure Your Server Wizard or by using the Active Directory Installation Wizard (DCPROMO). DCPROMO is a

tool that promotes a member server to domain controller status. During the installation, a writable copy of the AD database is placed on the server's hard disk. The file used to store directory information is called NTDS.dit and, by default, is located in %systemroot%\NTDS. When changes are made to the directory, they are saved to this file.

Operations Master Roles

In Windows Server 2003, all domain controllers are relatively equal by default. However, there are still some operations that need to be performed by a single domain controller in the domain or forest. To address these, Microsoft created the concept of *operations masters*. Operations masters serve many purposes. Some control where components of AD can be modified; others store specific information that is key to the healthy function of AD at the domain level. Because only one domain controller in a domain or forest fulfills a given role, these roles are also referred to as *Flexible Single Master of Operations* (FSMO) roles. Some FSMO roles are unique to each domain; others are unique to the forest.

There are five different types of master roles, each serving a specific purpose. Two of these master roles are applied at the forest level (forest-wide roles), and the others are applied at the domain level (domain-wide roles). The following are the forest-wide operations master roles:

- **Schema master** A domain controller that is in charge of all changes to the AD schema. The schema determines which object classes and attributes are used within the forest. If additional object classes or attributes need to be added, the schema master is used to write to the directory's schema, which is then replicated to other domain controllers in the forest. Updates to the schema can be performed only on the domain controller acting in this role.
- **Domain naming master** A domain controller that is in charge of adding new domains and removing unneeded ones from the forest. It is responsible for any changes to the domain namespace. This role prevents naming conflicts, because such changes can be performed only if the domain naming master is online.

In addition to the two forest-wide master roles, there are three domain-wide master roles: relative ID (RID) master, primary domain controller (PDC) emulator, and infrastructure master. These roles are described in the following sections.

Relative ID Master

The *relative ID master* is responsible for allocating sequences of numbers (called relative IDs, or RIDs) that are used in creating new security principles in the domain. Security principles are user, group, and computer accounts. These numbers are issued to all domain controllers in the domain. When an object is created, a number that uniquely identifies the object is assigned to it. This number consists of two parts: a domain security ID (or computer SID if a local user or group account is being created) and an RID. Together, the domain SID and RID combine to form the object's unique SID. The domain security ID is the same for all objects in that domain. The RID is unique to each object. Instead of using the name of a user, computer, or group, Windows uses the SID to identify and reference security principles. To avoid potential conflicts of domain controllers issuing the same number to an object, only one RID master exists in a domain. This controls the allocation of RID numbers to each domain controller. The domain controller can then assign the RIDs to objects when they are created.

PDC Emulator

The *primary domain controller (PDC) emulator* is designed to act like a Windows NT PDC when the domain is in Windows 2000 mixed mode. This is necessary if Windows NT backup domain controllers (BDCs) still exist on the network. Clients earlier than Windows 2000 also use the PDC emulator for processing password changes, though installation of the AD client software on these systems enables them to change their password on any domain controller in the domain to which they authenticate. The PDC emulator also synchronizes the time on all domain controllers the domain. For replication accuracy, it is critical for all domain controllers to have synchronized time.

Even if you do not have any servers running as BDCs on the network, the PDC emulator still serves a critical purpose in each domain. The PDC emulator receives preferred replication of all password changes performed on other domain controllers within the domain. When a password is changed on a domain controller, it is sent to the PDC emulator. If a user changes his or her password on one domain controller, and then attempts to log on to another, the second domain controller may still have old password information. Because this domain controller considers it a bad password, it forwards the authentication request to the PDC emulator to determine whether the password is actually valid. In addition, the PDC emulator initiates urgent replication so that the password change can propagate as soon as possible. Urgent replication is also used for other security-sensitive replication traffic, such as account lockouts.

This operations master is by far the most critical at the domain level. Because of this, you should ensure that it is carefully placed on your network and housed on a high-availability, high-capacity server.

Infrastructure Master

The *infrastructure master* is in charge of updating changes that are made to group memberships. When a user moves to a different domain and his or her group membership changes, it may take time for these changes to be reflected in the group. To remedy this, the infrastructure master is used to update such changes in its domain. The domain controller in the infrastructure master role compares its data to the Global Catalog, which is a subset of directory information for all domains in the forest and contains information on groups. The Global Catalog stores information on universal group memberships, in which users from any domain can be added and allowed access to any domain, and maps the memberships users have to specific groups. When changes occur to group membership, the infrastructure master updates its group-to-user references and replicates these changes to other domain controllers in the domain.

File and Print Servers

Two of the basic functions in a network are saving files in a central location on the network and printing the contents of files to shared printers. When file server or print server roles are configured in Windows Server 2003, additional functions become available that make using and managing the server more effective.

Print Servers

Print servers are used provide access to printers across the network. Print servers allow you to control when print devices can be used by allowing you to schedule the availability of printers, set priority for print jobs, and configure printer properties. Using a browser, an administrator can also view, pause, resume, and/or delete print jobs.

By configuring Windows Server 2003 in the role of a print server, you can manage printers remotely through the GUI and by using Windows Management Instrumentation (WMI). WMI is a management application program interface (API) that allows you to monitor and control printing. Using WMI, an administrator can manage components like print servers and print devices from a command line.

Print servers also provide alternative methods of printing to specific print devices. Users working at machines running Windows XP can print to specific printers by using a Uniform Resource Locator (URL).

File Servers

Administrators benefit from *file servers* by being able to manage disk space, control access, and limit the amount of space that is made available to individual users. If NTFS volumes are used, disk quotas can be set to limit the amount of space available to each user. This prevents users from filling the hard disk with superfluous data or older information that may no longer be needed.

In addition to these features, a file server also provides other functionality that offers security and availability of data. File servers with NTFS volumes have the *Encrypted File System* (EFS) enabled, so that any data can be encrypted using a public key system. To make it easier for users to access shared files, the *Distributed File Service* (DFS) can be used, which allows data that is located on servers throughout the enterprise to be accessible from a single shared folder. When DFS is used, files stored on different volumes, shares, or servers appear as if they reside in the same location.

DHCP, DNS, and WINS Servers

The roles of DHCP, DNS, and WINS servers are used for uniquely identifying computers and finding them on the network. A DHCP server issues a unique IP address to computer on the network. DNS and WINS servers resolve the IP address to and from user-friendly names that are easier for users to deal with. With Windows Server 2003 acting as a DHCP, DNS, and/or WINS server, clients can be automatically issued an IP address and find other machines and devices more easily.

DHCP Servers

DHCP is the *Dynamic Host Configuration Protocol*, and it is used to dynamically issue IP addresses to clients on networks using the Transmission Control Protocol/Internet Protocol (TCP/IP). Many enterprises use static IP addresses only for their servers and network infrastructure equipment (switches, routers, and so on). Dynamic addresses are typically used for all clients.

DNS Servers

The *Domain Name System* (DNS) is a popular method of name resolution used on the Internet and other TCP/IP networks. AD is integrated with DNS, and it uses DNS servers to allow users, computers, applications, and other elements of the network to easily find domain controllers and

other resources on the network. DNS servers are often the targets of attacks. We'll talk about securing a DNS server later in this appendix.

WINS Servers

The *Windows Internet Name Service* (WINS) is another method of name resolution that resolves IP addresses to NetBIOS names, and vice versa. NetBIOS names are used by pre-Windows 2000 servers and clients, and they allow users of those operating systems to log on to Windows Server 2003 domains. They are supported in Windows Server 2003 for backward-compatibility with these older systems. By implementing a WINS server, you allow clients to search for computers and other resources by computer name, rather than by IP address.

Web Servers

Web servers allow organizations to host their own Web sites on the Internet or a local intranet. Implementing a Web server in an organization allows users to benefit by accessing information, downloading files, and using Web-based applications. Web servers are another popular hacker target. We'll discuss steps to secure a web server later in this appendix.

Web Server Protocols

Microsoft's Windows Server 2003 Web server product is *Internet Information Services* (IIS) 6.0, which is included with Windows Server 2003. IIS allows users to access information using a number of protocols that are part of the TCP/IP suite, including:

- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Network News Transfer Protocol (NNTP)
- Simple Mail Transfer Protocol (SMTP)

Web Server Configuration

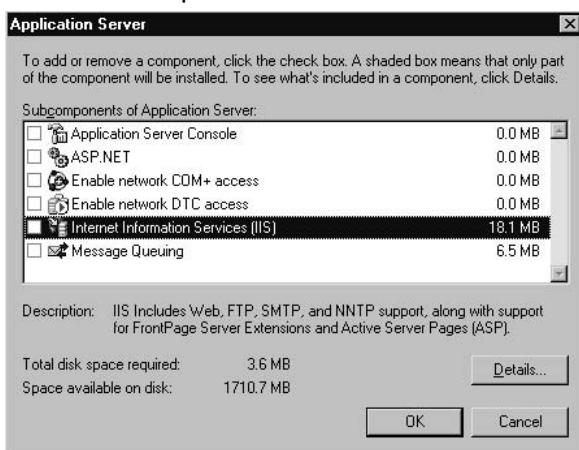
Although a Web server can facilitate a company's ability to disseminate information, it isn't an actual role that is configured using the Configure Your Server Wizard. It is installed as part of the application server role, which we'll discuss later in this appendix. The Configure Your Server Wizard provides an easy, step-by-step method of configuring Web servers through the application server role; however, it isn't the only way to

install IIS. You can also install IIS through the Add or Remove Programs applet in the Windows Control Panel.

Using Add or Remove Programs to install IIS takes a few extra steps, but it allows you to perform the installation without installing other services and features available through the application server role. To use Add or Remove Programs to install IIS, follow these steps:

1. Select **Start | Control Panel | Add or Remove Programs**.
2. Click the **Add/Remove Windows Components** icon to display the **Windows Components Wizard**, which provides a listing of available components to install.
3. In the list, select **Application Server** and click the **Details** button to view the **Application Server** dialog box, shown in Figure A.4.

Figure A.4 Installing IIS through the Application Server Dialog Box in the Windows Components Wizard



4. The **Application Server** dialog box contains a number of subcomponents. To install IIS, select the check box for **Internet Information Services (IIS)**, and either click **OK** to install the default components or click **Details** to view even more subcomponents that can be installed within IIS.
5. When you've made your selections, click **OK** to return to the **Windows Components Wizard**.
6. Click **Next** to have Windows make the configuration changes you requested from your selection.

7. Once the Wizard has finished copying the necessary files and changing system settings, click **Finish** to complete the installation process and exit the Wizard.

Database Servers

Database servers are used to store and manage databases (Microsoft SQL or Oracle, for example) that are stored on the server and to provide data access for authorized users. The Configure Your Server Wizard does not include a configurable role for database servers. Because SQL Server provides additional measures of security that would not otherwise be available (as discussed in the “Securing Database Servers” section later in this appendix) and processing occurs on the server, transactions can occur securely and rapidly.

Mail Servers

Mail servers enable users to send and receive e-mail messages. When a server is configured to be a mail server, two protocols are enabled: SMTP and Post Office Protocol (POP3). SMTP is used by clients and mail servers to send e-mail. POP3 is used by clients when retrieving e-mail from their mail server. Each of these protocols is part of the TCP/IP protocol suite and installed when TCP/IP is installed on a computer. However, even if TCP/IP is installed on Windows Server 2003, the services provided by mail servers still need to be enabled by configuring the machine to take the role of a mail server.

Certificate Authorities

Certificate authorities (CAs) are servers that issue and manage certificates. Certificates are used for a variety of purposes, including encryption, integrity, and verifying the identity of an entity, such as a user, machine, or application and are discussed in chapter 5 in this book.

Application Servers and Terminal Servers

Application servers and terminal servers provide the ability for users to access applications over the network. These roles are two of the most commonly used server roles and are ones you’re likely to implement or manage in your network.

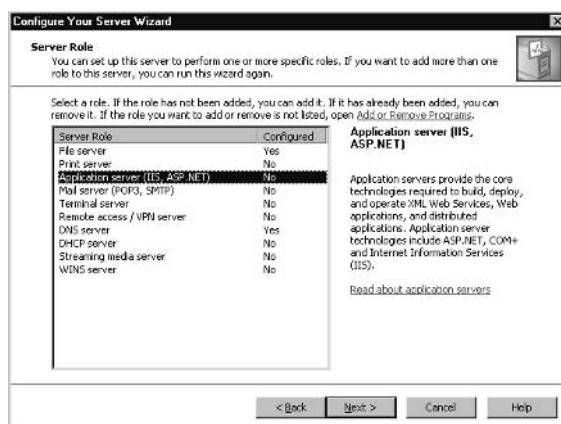
Application Servers

Application servers allow users to run Web applications and distributed programs from the server. Because Web applications require Internet technologies, when Windows Server 2003 is set up as an application server, IIS subcomponents such as ASP can be installed. As explained earlier, IIS is the Web server that comes with Windows Server 2003 and can be used to make Web applications available to users on the network. If IIS has been installed, the application server role will appear as a configured role in the Manage Your Server tool. This is despite the fact that only some components for the application server role have been installed. To modify the installed components, you can either use the Windows Components Wizard or the Configure Your Server Wizard.

Use the following steps to set up an application server in Windows Server 2003.

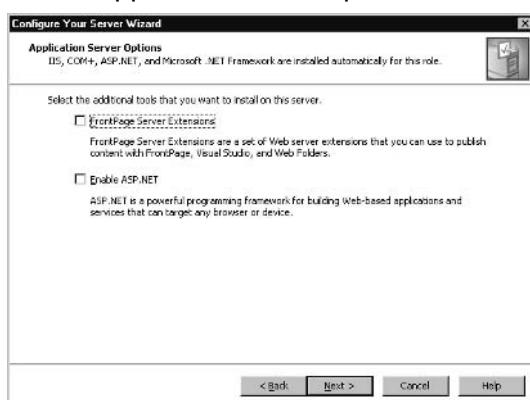
1. Select **Start | Administrative Tools | Manage Your Server**.
2. When Manage Your Server starts, click the Add or remove a role button.
3. When the Configure Your Server Wizard starts, read through the information on the Preliminary Steps window, and then click Next.
4. After the Wizard checks your network settings and operating system version, the Server Role window will appear. From the list, select Application server (IIS, ASP.NET), as shown in Figure A.5. Then click Next to continue.

Figure A.5 Choose the Application Server Role



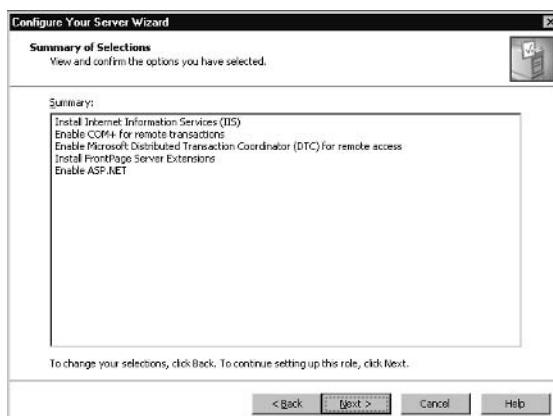
- The Application Server Options window appears, as shown in Figure A.6. Here, you can add components that are used with IIS. Note that IIS will be installed regardless of what you select on this page. Select the FrontPage Server Extensions check box to add Web server extensions that allow content created with FrontPage, Visual Studio, and Web Folders to be published to the IIS Web site. Select Enable ASP.NET to allow Web-based applications created using ASP.NET to be used on the site. After selecting the options you wish to add, click Next to continue.

Figure A.6 Select Application Server Options



- The **Summary of Selections** window, shown in Figure A.7, provides a list of components that will be installed as part of the application server configuration. Review these settings, and then click **Next** to begin installing these components.

Figure A.7 Review the Summary of Selections



7. After copying files, the **Windows Components Wizard** will open and continue the installation. Once it has completed, you will be returned to the **Configure Your Server Wizard**. Click **Finish** to complete the installation.

Terminal Servers

Terminal servers allow remote access to applications using thin-client technology. A benefit of Terminal Services is that users can run programs that they might otherwise be unable to use. For example, a user running an older version of Windows might need to use Office XP, but she doesn't have the minimal requirements install it. Through Terminal Services, she can connect to and be presented with a Windows Server 2003 desktop. If Office XP is installed on the terminal server, the user can open and use the application. Because all processing occurs on the server, the user can run applications that are impossible to install on her local system.

There are a wide variety of clients that can use Terminal Services. Client software is available for Windows 3.11 and later, as well as Macintosh and UNIX. Internet Explorer can also be used to access a terminal server, using the Web client software. Terminal Services can also interact with Citrix clients.

Planning a Server Security Strategy

The only truly secure network is one that is totally inaccessible. Security is always a trade-off between usability and protection. When planning security, you need to find an acceptable balance between the need to secure your network and the need for users to be able to perform their jobs.

In creating a security plan, it is important to realize that the network environment will never be completely secure. The goal is to make it difficult for intruders to obtain unauthorized access, so it isn't worth their time to try or continue attempting to gain access. It is also critical to protect servers from potential disasters and to have methods to restore systems if they become compromised.

A good security plan considers the needs of a company and tries to balance it with their capabilities and current technology. As you'll see in the sections that follow, this means identifying the minimum security requirements for an organization, choosing an operating system, and identifying the configurations necessary to meet these needs. To develop a security plan, you must identify the risks that potentially threaten a network,

determine what countermeasures are available to deal with them, figure out what you can afford financially, and implement the countermeasures that are feasible.

Choosing the Operating System

In planning a strategy for server security, you will need to determine which operating systems will be used in the organization. Different network operating systems provide diverse features that can be used as part of your security strategy, but here we will focus on Windows.

One of the first considerations for the operating system you choose will be the minimum system requirements for installing the operating system. Obviously, if your existing server cannot handle a particular version of Windows, you will not be able to install it. If this is the case, you will need to upgrade the hardware, purchase a new server to support the operating system you want, or choose an operating system that does match the current server's hardware. The minimum system requirements for Windows server operating systems are shown in Table A.1.

Table A.1 Minimum System Requirements for Windows Server Operating Systems

Server	Computer/ Processor	Memory (RAM)	Hard Disk	CPU Support
Windows NT Server 4	486/33 MHz or higher/Pentium, or Pentium Pro processor	16MB; 32MB recommended	Intel and compatible systems: 125MB available hard disk space minimum. RISC-based systems: 160MB available hard disk space	Up to 4 CPUs (retail version); Up to 32 CPUs available from hardware vendors
Windows 2000 Server	133 MHz or higher Pentium-compatible CPU	At least 128MB: 256MB recommended; 4GB maximum	2GB w/ 1GB free space; additional free space required for installing over a network	Up to 4 CPUs
Windows 2000 Advanced Server	133 MHz or higher Pentium-compatible CPU	At least 128MB; 256MB recommended; 8GB max	2GB with 1GB free space; additional free space required for installing over a network	Up to 8 CPUs
Windows 2000 Datacenter	Pentium III Xeon processors or higher	256MB	2GB with 1GB free space; additional free space required for installing over a network	8-way capable or higher server (supports up to 32-way)
Windows Server 2003 Standard Edition	133 MHz	128MB	1.5GB	Up to 4 CPUs
Windows Server 2003 Enterprise Edition	133 MHz for x86-based computers; 733 MHz for Itanium-based computers	128MB	1.5GB for x86-based computers; 2GB for Itanium-based computers	Up to 8 CPUs

Table A.1 Minimum System Requirements for Windows Server Operating Systems

Server	Computer/ Processor	Memory (RAM)	Hard Disk	CPU Support
Windows Server 2003 Datacenter Edition	400 MHz for x86-based computers; 733 MHz for Itanium-based computers	512MB	1.5GB for x86-based computers; 2GB for Itanium-based computers	Minimum 8-way capable machine required; maximum 64
Windows Server 2003 Web Edition	133 MHz	128MB	1.5GB	Up to 2 CPUs

Beyond the minimum requirements, you will need to look at the features available in different versions and editions of Windows, and how they can be used to enhance network security. The progression from one version to another has offered improvements and additions to security, with Windows Server 2003 offering the most security features. By identifying which features are necessary for your organization, you can create a network that provides the necessary functionality and security.

Identifying Minimum Security Requirements for Your Organization

Before you can begin implementing security measures, you need to know what needs protecting. For this reason, the security planning process involves considerable analysis. You need to determine which risks could threaten a company, what impact these threats would have on the company, the assets that the company needs to function, and what can be done to minimize or remove a potential threat.

The following are the main types of threats:

- Environmental threats, such as natural and man-made disasters
- Deliberate threats, where a threat was intentionally caused
- Accidental threats, where a threat was unintentionally caused

Environmental threats can be natural disasters, such as storms, floods, fires, earthquakes, tornadoes, and other acts of nature. When dealing with this type of disaster, it is important to analyze the entire company's risks, considering any branch offices located in different areas that may be prone to different natural disasters.

Human intervention can create problems as devastating as any natural disaster. Man-made disasters can also occur when someone creates an event that has an adverse impact on the company's environment. For example, faulty wiring can cause a fire or power outage. In the same way, a company could be impacted by equipment failures, such as the air conditioning breaking down in the server room, a critical system failing, or any number of other problems.

The deliberate threat type is one that results from malicious persons or programs, and they can include potential risks such as hackers, viruses, Trojan horses, and various other attacks that can damage data and equipment or disrupt services. This type of threat can also include disgruntled employees who have authorized access to such assets and have the ability to harm the company from within.

Many times, internal risks are not malicious in nature, but accidental. Employees can accidentally delete a file, modify information with erroneous data, or make other mistakes that cause some form of loss. Because people are fallible by nature, this type of risk is one of the most common.

Each business must identify the risks it may be in danger of confronting and determine what assets will be affected by a potential problem, including:

- **Hardware** Servers, workstations, hubs, printers, and other equipment.
- **Software** Commercial software (off the shelf) and in-house software.
- **Data** Documents, databases, and other files needed by the business.
- **Personnel** Employees who perform necessary tasks in the company.
- **Sundry equipment** Office supplies, furniture, tools, and other assets needed for the business to function properly.
- **Facilities** The physical building and its components.

When identifying minimum security requirements, it is important to determine the value and importance of assets, so you know which are vital to the company's ability to function. You can then prioritize risk, so that you can protect the most important assets of the company and implement security measures to prevent or minimize potential threats.

Determining the value and importance of assets can be achieved in a number of ways. Keeping an inventory of assets owned by the company will allow you to identify the equipment, software, and other property owned by the company.

To determine the importance of data and other assets, and thereby determine what is vital to secure, you can meet with department heads. Doing so will help you to identify the data and resources that are necessary for people in each department to perform their jobs.

In addition to interviewing different members of an organization, review the corporate policies for specifications of minimum security requirements. For example, a company may have a security policy stating that all data is to be stored in specific folders on the server, and that the IT staff is required to back up this data nightly. Such policies may not only provide insight on what is to be protected, but also what procedures must be followed to provide this protection.

Companies may also be required to protect specific assets by law or to adhere to certain certification standards. For example, hospitals are required to provide a reasonable level of security to protect patient records. If such requirements are not met, an organization can be subject to legal action.

Identifying Configurations to Satisfy Security Requirements

To protect assets from risks that were identified as possible threats to a business, countermeasures must be implemented. Servers will need certain configurations to provide security, and plans must be put into practice. Compare the risks faced by an organization with an operating system's features to find support that will address certain threats.

Configuring the server to use these services or tools can assist in dealing with potential problems. For example, installing AD and using domain controllers on a network can heighten security and provide the ability to control user access and security across the network. In the same way, configuring a file server to use EFS so that data on the server's hard disk is encrypted can augment file security. Using security features in an operating system allows you to minimize many potential threats.

The same technique should be used when determining which roles will be configured on servers. As described earlier, different server roles provide different services to a network. By comparing the functionality of a server role to the needs of a company, you can identify which roles are required. Although it may be tempting to configure a server with every possible role, this can cause problems. When a server is configured to play a certain role in an organization, a number of different services, tools, and technologies may be installed and enabled. Never install more roles than are needed to provide required functionality. Always disable any unneeded services on the server.

Although roles are helpful, running a Wizard to configure servers in a particular role isn't enough to create a secure environment. Additional steps should be followed to protect these servers and the data, applications, and other resources they provide. By customizing servers in this manner, you can ensure that the company will be able to benefit from Windows Server 2003 without compromising security. We'll discuss these steps in the "Customizing Server Security" section later in this appendix.

Planning Baseline Security

Security templates allow you to apply security settings to machines. These templates provide a baseline for analyzing security. Templates are .inf files that can be applied to computers manually or by using Group Policy Objects (GPOs).

Customizing Server Security

Security templates contain predefined configurations, which are a great starting point, but usually, they do not fulfill the needs of many organizations. You may need to make some changes to match the organizational policies of your company. Similarly, configuring roles for servers requires additional steps to make the servers secure from attacks, accidents, and other possible problems. By customizing server security, you can implement security measures that will fulfill the unique needs of your organization.

Securing Servers According to Server Roles

You can use the Configure Your Server Wizard to configure the server for a particular server role. Though this procedure may install and enable a number of different services, tools, and technologies, additional steps usually are required to ensure the server's security. Some tasks are unique to the server's role, but others should be applied to all servers on your network.

Security Issues Related to All Server Roles

Any server used by members of an organization might be at risk of attacks by hackers and malicious programs, as well as accidents or other disasters. You will want to consider taking a number of countermeasures to ensure that any server is well protected.

Physical Security

A large part of physical security involves protecting systems from unauthorized physical access. Even if you've implemented strong security that prevents or limits access across a network, it will do little good if a person can sit at the server and make changes or (even worse) pick up the server and walk away with it.. If people do not have physical access to systems, the chances of unauthorized data access are reduced.

Service Packs and Hotfixes

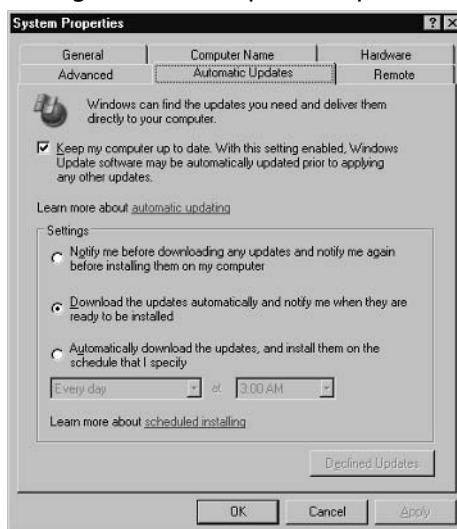
At times, software vendors may release applications or operating systems with known vulnerabilities or bugs, or these problems may be discovered after the software has been released. Service packs contain updates that may improve the reliability, security, and software compatibility of a program or operating system. Patches and bug fixes are used to repair errors in code or security issues. Failing to install these may cause certain features to behave improperly, make improvements or new features unavailable, or leave your system open to attacks from hackers or viruses. In most cases, the service packs, patches, or bug fixes can be acquired from the manufacturer's Web site.

Updates for Windows operating systems are made available on the Windows Update Web site, which can be accessed through an Internet browser by visiting <http://windowsupdate.microsoft.com>. The Windows Update Web site determines what software is recommended to secure your system, and then allows you to download and install it from the site.

Windows Update provides updates for only Windows operating systems, certain other Microsoft software (such as Internet Explorer), and some additional third-party software, such as drivers. To update most third-party programs installed on the computer, you will need to visit the manufacturer's Web site, download the update, and then install it.

Windows 2000, Windows XP, and Windows Server 2003 also provide an automated update and notification tool that allows critical updates to be downloaded and installed without user intervention. When enabled, this tool regularly checks Microsoft's Web site for updates, and if one or more are found, automatically downloads and installs the update. You can also just have it notify you that updates that are available. Because this tool requires connecting to Microsoft over the Internet, it can be used only if the servers or workstations have Internet access.

In some situations, administrators may not want Windows Server 2003 to automatically download and install software without their approval, or they may not want computers to connect to the Microsoft Web site in this manner. In these cases, the Automatic Updates service should be disabled or configured so that it is used for notification only. These settings can be accessed by selecting **Start | Control Panel | System** and clicking the **Automatic Updates** tab in the **System Properties** dialog box (figure A.8).

Figure A.8 Choosing Automatic Updates Options

Antivirus Software

To prevent these malicious programs from causing problems, antivirus software should be installed on servers and workstations throughout the network. Signature files are used to identify viruses and let the software know how to remove them. Because new viruses appear every month, signature files need to be updated regularly by downloading them from the vendor's Web site.

Unnecessary Accounts and Services

Hackers and malicious programs can use insecure elements of a system to acquire greater access and cause more damage. To keep these entities from exploiting elements of your system, you should disable any services that are not needed. If a service has a weakness for which a security patch has not been developed, it could be exploited. By disabling unneeded services, you are cutting off possible avenues of attack. In doing so, you will not affect any functionality used by computers and users, and you can avoid any security issues that may be related to them.

Certain accounts in Windows Server 2003 should also be disabled or deleted. If an account is no longer being used, it should be removed to avoid a person or program using it to obtain unauthorized access. Even if an account will not be used temporarily (for example, during an employee's leave or vacation), the account should be disabled during the user's absence. If an employee has left permanently or a computer has

been removed from the network, these accounts should be deleted. Properly managing users and groups greatly simplifies this task and methods for doing so are discussed in detail in “Working with User, Group and Computer Accounts” later in this book.

There are other accounts that you should consider disabling due to their access level. Windows Server 2003 and previous versions of Windows all have an account named Administrator that has full rights on a server. Because hackers already know the username of this account, they only need to obtain password to achieve this level of access. Although the Administrator account cannot be deleted, it can be disabled and renamed. If you create new user accounts and add them to the Administrators group, and disable the Administrator account, attackers will find it more difficult to determine which account to target.

Another account that is disabled by default, and should remain so, is the Guest account. This account is used to provide anonymous access to users who do not have their own account. Like the Administrator account, the Guest account is created when Windows Server 2003 is installed. Because there is the possibility that this account could accidentally be given improper levels of access and could be exploited to gain even greater access, it is a good idea to leave this account disabled. By giving users their own accounts, you can provide the access they need and audit their actions when necessary.

For any user, group, or computer account, it is important to grant only the minimum level of access needed. You want users to be unable to access anything beyond the scope of their role within the organization. This will assist in keeping other data and systems on the network protected. Determining what level of security a user needs to perform his or her job usually requires some investigation. By understanding the job a user performs, you will be able to determine which resources the user needs to access.

Strong Passwords

Strong passwords are more difficult to crack than simple ones. These types of passwords use a combination of keyboard characters from each of the following categories:

- Lowercase letters (*a–z*)
- Uppercase letters (*A–Z*)
- Numbers (0–9)
- Special characters (^ ~ ! @ # \$ % ^ & ★ () _ + - = { } | [] \ : ; ‘ < > ? , . /)

The length of a password also affects how easy it is to crack. You can use security templates and group policies to control how long a password is valid, the length of a password, and other aspects of password management. Another requirement that is important to having secure passwords is making sure that each time users change their passwords, they use passwords that are different from previous passwords.

To ensure domain controllers are secure, there are a number of password requirements that are enforced by default on Windows 2003 domain controllers:

- The password cannot contain any part of the user's account name.
- It must be a minimum of six characters in length.
- It must contain characters from three of the four categories: lowercase letters, uppercase letters, numbers, and special characters.

NTFS

Windows Server 2003 supports the FAT, FAT32, and NTFS file systems. Of these, NTFS provides the highest level of security. Disk partitions can be formatted with NTFS when a server is initially installed. If a volume is formatted as FAT or FAT32, you can convert it to NTFS. You can convert partitions to NTFS by using the command-line tool *convert.exe*.

Regular Backups

It is also important to perform regular data backups. Windows Server 2003 also provides Automated System Recovery and the Recovery Console for restoring systems that have failed.

Recovery Console is a text-mode command interpreter that can be used without starting Windows Server 2003. It allows you to access the hard disk and use commands to troubleshoot and manage problems that prevent the operating system from starting properly.

Automated System Recovery (ASR) allows you to back up and restore the Registry, boot files, and other system state data, as well as other data used by the operating system. An ASR set consists of files that are needed to restore Windows Server 2003 if the system cannot be started. In addition, ASR creates a floppy disk that contains system settings. Because an ASR set focuses on the files needed to restore the system, data files are not included in the backup. You should create an ASR set each time a major hardware change or a change to the operating system is made on

the computer running Windows Server 2003. ASR should not be used as the first step in recovering an operating system. In fact, Microsoft recommends that it be the last possible option for system recovery and be used only after you've attempted other methods. In many cases, you'll be able to get back into the system using Safe Mode, the Last Known Good Configuration or other options.

To create an ASR set, use the Windows Server 2003 Backup utility. On the **Welcome** tab of the Backup utility, click the **Automated System Recovery Wizard** button. This starts the **Automated System Recovery Preparation Wizard**, which takes you through the steps of backing up the system files needed to recover Windows Server 2003 and creating a floppy disk containing the information needed to restore the system.

Securing Domain Controllers

The methods described in the previous sections can improve the security of a server in any role, but they are particularly important for domain controllers. The effects of an unsecured domain controller can be far-reaching. Information in AD is replicated to other domain controllers, so changes on one domain controller can affect all of them. This means that if an unauthorized entity accessed the directory and made changes, every domain controller would be updated with these changes. This includes disabled or deleted accounts, modifications to groups, and changes to other objects in the directory. Because all Windows 2000 Server domain controllers store a writable copy of AD (unlike Windows Server 2003), additional steps must be taken to secure the directory in a mixed environment.

It is important that group membership is controlled, so that the likelihood of accidental or malicious changes being made to AD is minimized. This especially applies to the Enterprise Admins, Domain Admins, Account Operators, Server Operators, and Administrators groups.

Because anyone who has physical access to the domain controller can make changes to the domain controller and AD, it is important that these servers have heightened security. Consider using smart cards to control authentication at the server console.

Encryption should also be used to protect data and authenticate users. As mentioned, NTFS partitions allow file encryption, and Kerberos provides strong authentication security. In Windows Server 2003, Kerberos is the default authentication protocol for domain members running Windows 2000 or later.

Securing File and Print Servers

File and print servers also need additional security. In addition to setting permissions on files and folders, regularly performing backups, and using antivirus software, organizations may also need to implement greater levels of protection such as encryption. Similarly, print servers need to be protected from improper use and must be configured to prevent unauthorized users from wasting print resources.

File Servers

It is especially important that volumes on a file server are formatted as NTFS and appropriate permissions are set on files and folders. As an added measure of security, these disks should also use EFS.

EFS is used to encrypt data on NTFS volumes. When EFS is used, unauthorized users and malicious programs are prevented from accessing the content of files, regardless of their permissions. EFS file encryption is completely transparent to the user.

Although EFS is an important part of securing a file server, this does not mean that every file on the network is a candidate for being encrypted with EFS. As mentioned, only files on NTFS volumes can be encrypted with EFS. If a volume is formatted as NTFS, files that have the System attribute or are located in `%systemroot%` (for example, C:\Windows) cannot be encrypted. Also, if the file or folder you want to encrypt is compressed, you cannot use encryption. The opposite is also true: if a file or folder is encrypted with EFS, it cannot be compressed.

Another important limitation of EFS is that it encrypts data only on NTFS volumes. When a file is accessed remotely on a file server, Windows Server 2003 decrypts it and sends it across the network in unencrypted form. For data to be encrypted during transmission, other technologies like IPSec must be used.

IPSec ensures that data is sent securely over the network by encrypting packets and authenticating the identity of the sender and receiver. When using IPSec, a policy is applied to both the sender's and receiver's computer, so the systems agree on how data will be encrypted. Other computers that intercept traffic between the machines will be unable to decipher the information contained in the packets.

Print Servers

Files that are being printed may also require protection. IPSec can be implemented to protect the transmission of data being sent to printers. After all, if a document can be captured while being sent to a printer, a

hacker can view its information just as if it were being accessed directly from a server.

Physical security issues can be very important for printers. Anyone with access to a printer can remove printed documents from it. This is especially critical for printers that are routinely used to print sensitive documents or financial instruments like checks. A sensitive document may reside on a highly secure file server, but once it is printed, anyone standing by the printer could simply pick it up and walk away. To prevent this from happening, such printers should be located in secure areas that are not accessible to the public and other unauthorized users.

Just as files can have permissions assigned to them, so can printers. Printer permissions are used to control who can print and manage network printing. They are set on the **Security** tab of a printer's properties. Using printer permissions, you can allow or deny the following permissions for users:

- **Print** Allows users to print documents.
- **Manage Printers** Allows users to perform administrative tasks on a printer, including starting, pausing, and stopping the printer; changing spooler settings; sharing the printer; modifying permissions; and changing property settings.
- **Manage Documents** Allows users to perform administrative tasks relating to documents being printed. It allows users to start, pause, resume, reorder, and cancel documents.

Although different permissions exist for printing, only the Print permission gives the ability to print a document. For example, when only the Manage Documents permission is given, the user has the ability to manage other people's documents but cannot send documents to the printer for printing. Because those who manage printers may need to print test pages to determine if the printer is working properly, the Manage Printers permission can be set only if the Print permission is given.

Because the Print permission is assigned to the Everyone group, all users have access to print to a printer once it is shared on the network. For most printers, it's usually a good idea to remove this permission and add the specific groups within your organization that should have access to the printer.

Securing DHCP, DNS, and WINS Servers

DHCP, DNS, and WINS servers provide the ability to connect to the network and find other computers. DHCP is used to provide IP address

and configuration information to clients. If you do not secure these servers, malicious persons and programs may be able to prohibit users from connecting to the network, redirect traffic to other locations, and impact the ability to use network resources.

DHCP servers do not require authentication when providing a lease. To avoid unauthorized access, it is important you restrict physical and wireless access to your network. In addition, auditing should be enabled on the DHCP server so that you can review requests for leased addresses. By reviewing the logs, you may be able to identify possible problems.

Just as DHCP is an unauthenticated protocol, so is the NetBIOS naming protocol used by WINS. WINS was designed to work with NetBIOS over TCP/IP (NetBT), which does not require any authentication. Because a user does not need to provide credentials to use WINS, it should be regarded as available to unauthorized persons or programs.

Rogue servers can also be a problem on the network. When a client requests a DHCP lease, it does so by broadcast. If an unauthorized person puts a DHCP server on the network, the incorrect IP address and configuration information could be provided to clients. This isn't the case if the rogue DHCP server is running Windows 2000 or Windows Server 2003, because these must be authorized in AD. If the server determines that it is not authorized, the DHCP service will not start. However, pre-Windows 2000 and non-Windows DHCP servers require no authorization and can be effectively used as rogue DHCP servers in a Windows Server 2003 environment. Handing out bogus DHCP leases that do not expire can be a very effective DoS technique. Because of this, it is important to monitor network traffic for DHCP server traffic that does not come from your network's authorized DHCP servers.

Restricting access to DHCP tools and limiting membership in groups that can modify DHCP settings are other important steps in securing a DHCP server. To administer DHCP servers remotely using the DHCP console or Netsh utility, you need to be a member of the Administrators group or the DHCP Administrators group. By restricting membership in these groups, you limit the number of people who can authorize a DHCP server to service client requests.

Securing Web Servers

Because IIS provides a variety of services that allow users to access information from the Web server service, it provides potential avenues of attack for unauthorized users, malicious programs, and other sources. IIS is not installed by default in Windows Server 2003, though in earlier versions of the OS it was installed by default.. If you do not need a Web

server on your network, IIS should remain uninstalled. If it has been installed on servers that do not need it, make sure to uninstall it.

Once IIS is installed on Windows Server 2003, it is locked down to prevent any unneeded services from being exploited. By default, IIS will provide only static content to users. If dynamic content is used on the server, you will need to enable the necessary features. For example, if you your site is going to use ASP, ASP.NET, Common Gateway Interface (CGI), Internet Server Application Programming Interface (ISAPI) or Web Distributed Authoring and Versioning (WebDAV), each of these will need to be enabled before they can be used. As with Windows Server 2003 itself, any components that are not needed should be disabled.

Another default setting of IIS is that it will not compile, execute, or serve files with dynamic extensions. For example, if you have Web pages written as ASPs with the extension .asp, IIS, using default settings, won't provide users with this content. These are not allowed by default because of Microsoft's new security initiatives. Dynamic content can contain malicious code or have weaknesses that can be exploited. If files that provide dynamic content need to be used on the Web server, you must add the file extensions to the Web service extensions list. Any file types that are not needed should not be added.

An important part of protecting Web servers is using firewalls. Rules can be set up on the firewall controlling what kinds of traffic may pass and who can perform certain actions. Recent attacks suggest that firewall software may be a new target for attack, so it's vital to configure your firewall properly and monitor it regularly.

Securing Database Servers

When securing databases, you should take advantage of security features offered by the database software. Microsoft SQL Server, for example, provides two methods of authenticating clients to access data: Windows Authentication Mode and Mixed Mode. When Windows Authentication Mode is used, the SQL Server administrator has the ability to grant logon access to Windows user accounts and groups. If Mixed Mode is used, users can be authenticated through either Windows authentication or separate accounts created within SQL Server.

Regardless of the authentication mode used, like many database applications, SQL Server allows you to control access to data at a granular level. Permissions can be set to determine the operations that a user can perform on the data contained in the database. In many database applications, you can set permissions at the server, database, or table level. While one account might have the ability to create tables and delete data

in all databases, another may only be able to view data in a single database. These permissions are different from those that can be set through AD and NTFS, and they apply only within the database program.

Database servers may also need to be secured through other roles that are used to access the database. For example, IIS is set up through the application role, and Web pages on the server can be used to access data stored in a database. Similarly, applications that are developed and made accessible from a terminal server may be used to view and manipulate database information.

To control access to the database server, you can use settings configured through a *data source name* (DSN). A DSN is commonly used by compiled and Web-based programs to gain access to data that is stored in data management systems and data files. A DSN contains information on the database name, the server it resides on, and the directory in which it's stored (if a data file is used). It also holds the username, password, and driver to use when making the connection. Programs use information in the DSN to connect to the data source, make queries, and manipulate data. To create or modify a DSN, use the Data Sources (ODBC) applet (select **Start | Administrative Tools | Data Sources (ODBC)**).

Because a DSN provides the username and password to use when connecting to the data source, a number of security-related issues arise from its use. Any passwords that are used should follow the recommendations for strong passwords that were discussed earlier in this appendix. In cases where a DSN is being used to connect to a SQL Server database, you also have the option of using Windows authentication or SQL Server authentication. If SQL Server authentication is used, you can enter the username and password of an account created in SQL Server. However, you should avoid entering the name of any accounts with access higher than the user will need. For example, entering the system administrator account (**sa**) would provide a DSN with full access to SQL Server and could maliciously or accidentally cause problems. To avoid possible damage to data or access violations, you should provide the username and password of a SQL Server account that has restricted access.

Securing Mail Servers

When Windows Server 2003 is configured with the mail server role, it should be set up to require secure authentication from e-mail clients. As mentioned earlier, clients retrieve their e-mail from mail servers using the POP3 protocol. Client software and the mail server's POP3 service can be configured to accept only passwords that are encrypted in order to prevent them from being intercepted by unauthorized parties.

In Windows Server 2003, the Microsoft POP3 Service uses Secure Password Authentication (SPA) to ensure that authentication between the mail server and clients is encrypted. SPA is integrated with AD, which is used to authenticate users as they log on to retrieve their e-mail. In cases where domain controllers are not used, SPA can authenticate to local accounts on the mail server. When the POP3 service is configured to accept only authentication using SPA, clients must also be configured to use encrypted authentication. If they are not, clients will attempt to authenticate using cleartext (which is plaintext, or unencrypted data) and will be rejected by the mail server.

To prevent mail servers from filling up with undeleted or unchecked e-mail, disk quotas should also be implemented. Disk quotas can be used only on NTFS partitions. When NTFS is used, permissions can also be set on the directories that store e-mail, preventing unauthorized parties from accessing it on the server.

Index

Numbers

403.2 error message, 210

A

Accept lists (connection filtering), 230
acceptable-use policies, defining, 19
accidental threats, 289, 290
Active Directory (AD), 275
 digest authentication and, 98
 Exchange 2003 dependency on, 14
 mailbox access, granting via, 43–45
Adaware utility, 250
administrative permissions, 26–35
 Exchange Administrator and, 32
 Exchange Full Administrator and, 31
 Exchange View Administrator and, 33
 list of, 35
Administrator account, disabling, 295
administrators, granting access to all
 mailboxes and, 36
ADModify tool, 118
Advanced Queuing Engine (AQE), 16
AH (Authentication Header), 149
anonymous access, 98
 enabling in IISADMPWD virtual
 directory, 123
 SMTP setting for, 57, 59
anonymous connections, 57
Antigen for Microsoft Exchange anti-
 virus software (Sybari), 249
antispam. *See entries at spam*
Antivirus API (AVAPI), 246
AntiVirus for Mail Servers (RAV), 249
Antivirus for Microsoft Exchange (F-
 Secure), 249
antivirus software, 294
 considerations when choosing, 249
 server-side protection and, 244–249
 updating daily, 18
 vendors of (list), 248
application layer filtering, 151
Application log (Event Log Service), 262
application servers, 274, 282–285
AQE (Advanced Queuing Engine), 16
ASR (Automated System Recovery),
 296
attachments
 blocking feature for

 in Outlook 2003, 251–253
 in OWA, 168–170
 viruses and, 242–251
audit policy events, 263
auditing
 Exchange servers, 261–270
 reporting software for, 264, 269
 Windows 2000/2003, 262–264
authentication, 86
 basic, 59, 98
 digest, 98
 dual, 136, 137
 FE/BE deployment scenarios and,
 136–139
 forms-based, 170–176
 enabling, 171
 for OWA, 98–102
 pass-through, 137
 setting via ESM, 94, 99
 SMTP settings for, 57, 59
Authentication Header (AH), 149
authentication servers, 275–278
Automated System Recovery (ASR),
 296
AVAPI (Antivirus API), 246

B

backups, 296
 ensuring physical security for, 21
 performing daily, 18
BADMAIL directory, examining weekly
 or monthly, 19
Bagle e-mail worm, 168, 243
basic authentication, 98
 dual authentication and, 136, 137
 SMTP setting for, 59
Basic clients (OWA), 173
Bayesian filtering, unavailable with
 Exchange 2003, 222
best practices, 9–24
 putting into practice, 18–21
blacklists, 224
 See also real-time blacklists
block list service providers. *See real-time*
 blacklist service providers
blocked messages, custom error message
 for, 227
blocked senders/recipients. *See sender*
 filtering; *recipient filtering*

- buffer overrun attacks, 154
 BusinessSecure Antivirus with Exchange (Panda Software), 249
- C**
- certificate authorities (CAs), 103, 282
 - installing component for, 104–107
 - RPC over HTTP and, 197
 - S/MIME and, 193
 - third-party vendors for, 103, 116
 - TLS/SSL and, 180–185
 - certificate requests
 - creating, 108–116
 - reviewing before submitting, 112
 - Certificate Services Web enrollment site, 107
 - Change Password button, enabling in OWA, 124
 - Change Password feature, 120–127
 - lag time and, 126
 - testing, 125–127
 - ClearSwift's MailSweeper Business Suite antivirus software, 249
 - client-side spam filtering, 214–222
 - client-side virus protection, 249
 - Cloudmark's SpamNet software, 221
 - CMS's Praetor for Microsoft Exchange Server antivirus software, 249
 - collaborative environments, virtual directories for, 94
 - compression, enabling for OWA, 172
 - computer viruses. *See* viruses, protecting against
 - Configure Your Server wizard, 272–275
 - Connection Control feature, 61
 - connection filtering, 222, 223–229
 - filtering rule warning box and, 232
 - connection limits for OWA virtual directories, setting, 101
 - Contacts folder (Outlook 2003), treating addresses in as safe senders, 218
 - content downloads, settings for in Outlook 2003, 221
 - cookie-based authentication. *See* forms-based authentication
 - corporate legal disclaimers
 - configuring for outgoing e-mail, 79
 - software for, 80
 - creating
 - certificate requests, 108–116
 - IISADMPWD virtual directory, 121–124
 - OWA redirect page, 127–131
 - SMTP connectors, 65
- D**
- data source names (DSNs), 302
 - database servers, 282
 - securing, 301
 - DC servers, RPC traffic and, 145–148
 - DCOM (Distributed Component Object Model), disabling support for in RPC over HTTP, 204
 - DCs. *See* domain controllers
 - Default domain setting (SMTP), 60
 - default settings, Exchange 2003 vs. Exchange 2000, 6
 - default timeout, for OWA sessions, 174
 - defense-in-depth systems, 237
 - deliberate threats, 289
 - demilitarized zone (DMZ). *See* perimeter network
 - Denial of Service attacks (DoS attacks), message limits and, 67
 - Deny lists (connection filtering), 230
 - deployment scenarios for servers, 133–156
 - affordability and, 139, 150
 - DFS (Distributed File Service), 279
 - DHCP servers, 274, 279
 - securing, 299
 - diagnostics logging, 266–268
 - Diagnostics Logging property page, 266
 - digest authentication, 98
 - digital signature certificates, for individual use, 195
 - digital signatures, 193
 - S/MIME option for, 160
 - Directory Service Access (DSAccess), 16
 - monitoring software for, 269
 - Directory Service log (Event Log Service), 262

- Directory Service to Metabase
 (DS2MB process), 16, 100
- Disable This Rule option (connection filtering), 228
- disclaimers
 configuring for outgoing e-mail, 79
 software for, 80
- disk space, checking daily, 18
- Display Administrative Groups option, 49
- Display Name field (connection filtering), 225
- Distributed Component Object Model (DCOM), disabling support for in RPC over HTTP, 204
- Distributed File Service (DFS), 279
- distribution lists, 71
- DLL EPOXY, 17
- DMZ. *See* perimeter network
- DNS Server log (Event Log Service), 262
- DNS servers, 274, 279
 securing, 299
- DNS Suffix of Provider field (connection filtering), 225
- Domain Admins group, 27
- domain controllers (DCs), 274, 275–278
 securing, 297
 strong passwords and, 296
- domain name, fully qualified (FQDN), 110
 internal, specifying for Exchange server, 206
- domain naming master, 276
- domain SIDs, 277
- DoS attacks, message limits and, 67
- downloading content, settings for in Outlook 2003, 221
- downloads
 ADModify tool, 118
 Exchange 2003 management package, 264
 ISA Server 2004, beta version of, 155
 MBSA utility, 11
 URLScan utility, 150
 utilities for Exchange 2003, 118
- DS Referral interface, 16
- DS2MB process, 16, 100
- DSAccess process, 16
 monitoring software for, 269
- DSNs (data source names), 302
- DSProxy process, 16
- dual authentication, 136
 using, 137
- E**
- EFS (Encrypted File System), 279, 298
- e-mail address spoofing, 59, 85–89
- e-mail addresses, resolving, 86
- e-mail headers, 89–92
- e-mail messages
 blocked, custom error message for, 227
 footer for, configuring, 79
 junk filters for. *See entries at junk e-mail filter*
 out-of-office responses and, 70
- e-mail viruses, 242–251
- e-mail worms, 168
- enabling
 auditing to track Exchange configuration changes, 265
- Change Password button, in OWA, 124
- diagnostic logging, 266
- forms-based authentication, 171
- junk e-mail filter, 162
- S/MIME, 158–161
- SMTP protocol logging, 72–75
- SSL on OWA, 103–116
- TLS/SSL, 185–188
- Web beacon blocking, 166
- Encapsulating Security Payload (ESP), 149
- Encrypted File System (EFS), 279, 298
- encryption
 EFS for, 279, 298
 for IMAP4 traffic, 190–192
 IPSec and, 148–150, 180, 298
 for POP3 traffic, 190–192
 via S/MIME, 192–195
 options for in OWA, 160
 for SMTP traffic, 179–189
- endless loop problems, 123

- enhanced attachment-blocking feature, 168–170
- E-inspect (log-reporting vendor), 75
- Enterprise Admins group, 27
- environmental threats, 289
- error messages, writing custom for blocked e-mail, 227
- ESE (Extensible Storage Engine), 246
monitoring software for, 269
- ESE98 database engine, 17
- ESM. *See* Exchange System Manager
- ESP (Encapsulating Security Payload), 149
- event auditing, in Windows 2000/2003, 262–264
event logs for, reviewing daily, 18
- Event Log Service, 262
- EventID errors, 265
- Everyone group, 27
- Exadmin virtual directory, 94
- Exception lists (connection filtering), 229
- Exchange 2000 Server
auditing, 261–270
e-mail spoofing and, 87
- Exchange 2003 Management Pack (Microsoft), 269
- Exchange 2003. *See* Exchange Server 2003
- Exchange 5.5, open relays and, 82
- Exchange Administration Delegation Wizard, 26, 30–35
- Exchange Administrator, 32
- Exchange Domain Servers group, 26, 27
- Exchange Edge services, 238
- Exchange Enterprise Servers group, 26, 27
- Exchange Full Administrator, 31
- Exchange Installable File System (ExIFS), 17
- Exchange Inter-Process Communication (ExIPC), 17
- Exchange Object Linking and Embedding Database (ExOLEDB), 17
- Exchange Server 2003
FE/BE deployment scenarios for, 133–156
installing
best practices for, 21–24
- components comprising, 16–18
dependencies and, 15
- management pack for, 269
- option for enabling as FE server, 139
- publishing protocols for, 153
- RPC over HTTP feature of, 195–211
- security and
best practices for, 9–24
features of (overview), 1–8
hardening guide for, 13, 150
safe computing practices for, 20
- utilities for, 118
- Exchange System Manager (ESM)
authentication methods, setting via, 94, 99
- connection limits for OWA virtual directories, setting via, 101
- permissions
for OWA virtual directories, setting via, 100
for public folders, creating/setting via, 49–53
viewing in, 29
- SMTP authentication settings in, 57, 59
- Exchange View Administrator, 32–34
- Exchange virtual directory, 95
- Exchange Virtual Server icon, 119
- Exchange Virtual Server, stopping, 119
- ExchWeb virtual directory, 95
- eXclaimer disclaimer software, 80
- ExIFS driver, 17
- ExIPC layer, 17
- ExMerge utility, 254–259
- ExOLEDB layer, 17
- Extensible Storage Engine (ESE), 246
monitoring software for, 269
- Extensible Storage Engine (ESE98), 17

F

- F-Secure Antivirus for Microsoft Exchange, 249
- FE servers. *See* front-end servers
- FE/BE deployment scenarios. *See* front-end/back-end deployment scenarios
- file attachments. *See* attachments

- file-level virus scanners, 247
File Replication log (Event Log Service), 262
 file servers, 274, 279
 securing, 298
 filtering
 attachments
 in Outlook 2003, 251–253
 in OWA, 168–170
 Bayesian, 222
 connection, 222, 223–229
 filtering rule warning box and, 232
 recipients, in Outlook 2003, 223,
 234
 senders
 in Outlook 2003, 219, 235–237
 in OWA, 162, 164–166
 spam
 client-side, 214–222
 server-side, 222–237
 firewalls, 250
 intranet, allowing/disallowing RPC traffic through, 145–148
 ISA Server. *See* ISA Server
 securing Web servers and, 301
Flexible Single Master of Operations (FSMO), 276
 footer (legal disclaimer), configuring, 79
 forms-based authentication, 170–176
 dual authentication and, 138
 enabling, 171
 reasons for not using, 176
 FQDN (fully qualified domain name), 110
 internal, specifying for Exchange server, 206
 front-end/back-end (FE/BE) deployment scenarios, 133–156
 affordability and, 139, 150
 deploying, 136–139
 SSL and, 116
 front-end servers
 attachment blocking feature and, 169
 disabling unneeded services on, 140
 forms-based authentication and, 176
 internal network, placing on, 150–152
 option for enabling Exchange 2003 as, 139
 perimeter network, placing in, 144
 recommended number of, 136
 RPC over HTTP, configuring on, 198–202
 securing, 139–152
FSMO (Flexible Single Master of Operations), 276
 fully qualified domain name (FQDN), 110
 internal, specifying for Exchange server, 206
- ## G
- GAL (global address list), 59, 86
 GC servers, RPC traffic and, 145–148
 GFI MailEssentials disclaimer software, 80
 GFI MailSecurity for Exchange/SMTP antivirus software, 248
 global address list (GAL), 59, 86
 Guest account, disabled by default, 295
- ## H
- hardware considerations, checklist for, 22
 hashes, forms-based authentication and, 170
 health monitoring and operations report (Exchange 2003 Management Pack), 269
 heuristics-based analysis
 Intelligent Message Filter and, 238
 unavailable with Exchange 2003, 222
 Hfnetchk (Network Security Hotfix Checker), 12
 “Host not found” error message, 228
 hotfixes, 293
 .htc files, password changes and, 127
HTTP (Hypertext Transfer Protocol), disabled on front-end server, 140
 “HTTP 403.4 Forbidden” error message, 128, 130
 HTTP authentication, 136
 HTTP Exchange Virtual Server, stopping, 119
 HTTP requests, redirecting to SSL requests, 127–131

- HTTP virtual servers. *See OWA*
 virtual directories
- Hypertext Transfer Protocol (HTTP),
 disabled on front-end server,
 140
- I**
- idle connections on OWA virtual di-
 rectories, limiting duration of,
 102
- IE. *See Internet Explorer*
- iHateSpam software, 221
- IIS. *See Internet Information Services*
- IIS Manager, ESM preferred to for
 setting authentication methods,
 94, 99
- IISADMPWD virtual directory
 creating, 121–124
 enabling anonymous access in, 123
- IKE (Internet Key Exchange), 149
- ILoveYou virus, 243
- IMAP4. *See Internet Message Access
 Protocol 4*
- IMAP4 banner, modifying, 78
- IMC (Internet Message Connector),
 open relays and, 82
- IMF (Intelligent Message Filter), from
 Microsoft, 222, 237–239
- Information Store, 17
 stopping/disabling, 143
- infrastructure master, 278
- inheritance
 permissions and, 27
 top-level public folders and, 53
- installing Exchange 2003, 15, 16–18
 best practices for, 21–24
- Integrated Windows authentication,
 98
 SMTP setting for, 59, 60
- Intelligent Message Filter (IMF), from
 Microsoft, 222, 237–239
- internal network
 attachment blocking and, 169
 placing front-end server on,
 150–152
- Internet Explorer (IE)
 compression and, 172
 Premium clients and, 173
 Version 6, S/MIME messages and,
 158
- Internet Information Services (IIS), 2,
 280–282
 endless loop problems and, 123
 Exchange 2003 dependency on, 14
 Web servers and, 300
 Windows 2000/2003 and, 4
- Internet Key Exchange (IKE), 149
- Internet kiosks, forms-based authenti-
 cation and, 176
- Internet mail headers, 89–92
- Internet Message Access Protocol 4
 (IMAP4)
 banner for, modifying, 78
 disabled on front-end server, 140
 encrypting traffic and, 190–192
 monitoring software for, 269
 vs. POP3, 190
 RPC traffic and, 146
- Internet Message Connector (IMC),
 open relays and, 82
- Internet Message Format settings, 69
- Internet Security and Acceleration
 server. *See ISA Server*
- intranet firewall, allowing/disallowing
 RPC traffic through, 145–148
- IP addresses
 Accept lists, adding to, 230
 Deny lists, adding to, 231
- IP Security (IPSec), 148–150, 180,
 298
 enabling between SMTP servers,
 188
- ISA Server, 136, 151
 2004 version of, 155
 deploying with Exchange 2003,
 152–156
 publishing Exchange protocols and,
 198
 single-server scenario and, 134
- J**
- junk e-mail filter
 for Outlook 2003, 214–222
 caution with option for deleting
 permanently, 217
 defense-in-depth systems and, 237
 protection levels for, configuring,
 216
- for OWA, 162–166
See also filtering

L

- legal disclaimers
 - configuring for outgoing e-mail, 79
 - software for, 80
- Level1/Level2 attachments (OWA), 168
- log-reporting utilities, 75

M

- mail. *See* mailboxes; *entries at e-mail*
- .mail domain antispam initiative, 92
- mail-enabled groups, 71
- Mail Exchanger records (MX records), 64
- Mail Security for Microsoft Exchange
 - antivirus software (Symantec), 248
- mail servers, 274, 282
 - securing, 302
- Mailbox Store, dismounting/deleting, 141
- mailboxes
 - automatic message replies and, 70
 - granting access and
 - via AD, 43–45
 - to administrators, 36
 - limiting size of, 67, 68
 - for mail-enabled groups, 72
 - permissions for, 36–45
 - opening another's mailbox and, 40–43
- MailSweeper Business Suite antivirus software, 249
- Manage Your Server tool, 272
- MAPI (Messaging Application Programming Interface), 245
 - permissions for, editing, 49
- MAPI over RPC (Messaging Application Programming Interface over Remote Procedure Calls), 189
- master roles, 276–278
- MBSA (Microsoft Baseline Security Analyzer), 10
- Melissa virus, 243
- Message Details Tab (ExMerge utility), 258
- message limits, setting, 67, 68
 - for mail-enabled groups, 72
- for public folders, 70
- message screeners, 154
- message-tracking logs, archiving
 - weekly or monthly, 19
- message transfer agent (MTA), 17
 - monitoring software for, 269
- messages. *See* e-mail messages
- MessageStats (log-reporting vendor), 75
- Messaging Application Programming Interface (MAPI), 245
 - permissions for, editing, 49
- Messaging Application Programming Interface over Remote Procedure Calls (MAPI over RPC), 189
- MetaEdit utility, changing SMTP banners and, 78
- Microsoft
 - Baseline Security Analyzer (MBSA), 10
 - Certificate Services, installing, 104–107
 - Exchange Information Store service, monitoring software for, 269
 - Intelligent Message Filter, 222, 237–239
 - Internet Explorer. *See* Internet Explorer
 - Network Security Hotfix Checker (Hfnetchk), 12
 - Security Bulletins, 13
 - SmartScreen technology, 214, 237
 - SQL Server, 301
 - Trustworthy Computing Initiative.
 - See* Trustworthy Computing Initiative
 - Microsoft Operations Manager (MOM), 264, 269
 - Microsoft-Server-Activesync virtual directory, 96
 - MOM (Microsoft Operations Manager), 264, 269
 - monitoring software, 264, 269
 - Msv.dk (open relay testing site), 85
 - MTA (message transfer agent), 17
 - monitoring software for, 269
 - MX records, 64
 - MxClaim disclaimer software, 80

N

Nachi worm, 243
 Name Service Provider Interface (NSPI), 16
 NDRs (nondelivery reports), 236
 .NET Passport authentication, 98
 NetLogon service, disabling, 146
 Netscape Navigator, compression and, 172
 Netsky e-mail worm, 168, 243
 Network Abuse Clearinghouse (open relay testing site), 85
 Network News Transfer Protocol (NNTP), disabled on front-end server, 140
 Network Security Hotfix Checker (Hfnetchk), 12
 NNTP (Network News Transfer Protocol), disabled on front-end server, 140
 nondelivery reports (NDRs), 236
 NSPI (Name Service Provider Interface), 16
 NTFS file system, 279, 296

O

OMA virtual directory, 97
 Open Relay Database (ORDB), 85
 Open Relay Test, 85
 Open Relay Tester, 85
 open relays, 82–85
 Relay Restrictions feature and, 63
 testing for, 83–85
 operating systems, 286–288
 operations masters, 276–278
 ORDB (Open Relay Database), 85
 organization permissions
 Exchange Administrator and, 32
 Exchange Full Administrator and, 31
 Exchange View Administrator and, 32
 list of, 34
 out-of-office responses, 70
 Outlook 2003
 attachment-blocking feature of, 251–253
 junk e-mail filter and, 162

mailbox permissions, granting via, 36–43
 without using delegation, 39
 public folder permissions, creating/setting via, 46–49
 S/MIME settings in, 194
 security enhancements in, 250
 Outlook Web Access (OWA)
 authentication methods for, 98–102
 FE/BE deployment scenarios and, 133–139
 public folders, creating via, 53
 restricting access to, 116–120
 security features in, 7, 157–177
 security flaw in, 102
 site publishing for, 154
 OWA 2003 server, configuring security for, 93–131
 OWA clients
 S/MIME, enabling for, 158–161
 security features for, 157–177
 OWA segmentation, 117, 119
 OWA virtual directories, 94–102
 connection limits for, setting, 101
 permissions for, setting via ESM, 100

P

“The Page Cannot Be Displayed” error message, 119
 “This Page Must Be Viewed Over a Secure Channel” error message, 114
 Panda BusinessSecure Antivirus with Exchange, 249
 pass-through authentication, 137, 138
 passwords
 changing via OWA, 120–127
 endless loop problems and, 123
 lag time and, 126
 testing for, 125–127
 strong, 3, 295
 patches, 293
 checking for weekly or monthly, 19
 keeping current, 10–13
 PDC emulator, 277
 per-server/per-user segmentation (OWA), 120
 performance
 diagnostics logging and, 266–268

- enabling OWA compression and, 172
- front-end server and 141, 145, TLS/SSL and, 186
- perimeter network
 - forms-based authentication and, 176
 - front-end server, placing in, 144
 - single-server scenario and, 134
 - virus protection and, 244, 248
- permission roles
 - folder permissions and, 47, 48
 - mailbox permissions and, 38, 39
- permissions, 25–53
 - mailbox, 36–45
 - MAPI, 49
 - printer, 299
 - specific to Exchange 2003, 26–30
 - viewing in ESM, 29
- Permissions tab (Outlook 2003), 39
- PestPatrol utility, 250
- physical security, 21, 292
 - printers and, 299
- PKI (Public Key Infrastructure), S/MIME for OWA and, 158
- pointer records (PTR records), 89
- Policy Patrol disclaimer software, 80
- Policy Patrol Enterprise antivirus software (Red Earth Software), 249
- Post Office Protocol 3 (POP3)
 - banner for, modifying, 78
 - disabled on front-end server, 140
 - encrypting traffic and, 190–192
 - vs. IMAP4, 190
 - monitoring software for, 269
 - RPC traffic and, 146
- Praetor for Microsoft Exchange Server antivirus software (CMS), 249
- Premium clients (OWA), 173
- primary domain controller emulator (PDC emulator), 277
- print servers, 274, 278
 - securing, 298
- printer permissions, 299
- private computers, OWA session de-fault timeout and, 174
- Promodag (log-reporting vendor), 75
- protocol logging (SMTP), 72–75
 - third-party products for, 75
- protocol logs, purging/archiving weekly or monthly, 19
- protocols, securing, 179–212
- PTR records, 89
- public computers, OWA session de-fault timeout and, 174
- Public Folder Store, 45
 - dismounting/deleting, 143
- public folders
 - permissions for, 45–53
 - top-level folders and, 53
 - setting limits on, 70
- Public Key Infrastructure (PKI), S/MIME for OWA and, 158
- Public virtual directory, 97
- Q**
- queue lengths, examining daily, 18
- R**
- RAV AntiVirus for Mail Servers, 249
- RBLs. *See* real-time blacklists
- reach clients (OWA), 173
- real-time blacklist service providers, 224, 228
 - list of, 226
- real-time blacklists (RBLs), 222, 224
 - limiting number of, 225
 - open relays and, 82
- recipient filtering, in Outlook 2003, 223, 234
 - filtering rule warning box and, 232
- Recipient Update Service (RUS process), 16
- recipients, safe
 - in Outlook 2003, 218
 - in OWA, 162
- Recovery Console, 296
- Red Earth Software's Policy Patrol Enterprise antivirus software, 249
- redirecting HTTP requests to SSL re-quests, 127–131
- registry
 - attachment blocking and, 168
 - default timeout and, for OWA sessions, 175
- relative ID master (RID master), 277

- relative IDs (RIDs), 277
 Relay Check, 85
 Relay Restrictions feature, 62–64
 caution with, 63
 relaying, 80–85
 caution with settings for, 82
 open relay testing and, 83–85
 remote access/VPN servers, 274
 Remote Procedure Call traffic (RPC traffic)
 allowing/disallowing through intranet firewall, 145–148
 MAPI and, 189
 pass-through authentication and, 137
 Remote Procedure Calls over Hypertext Transfer Protocol (RPC over HTTP), 195–211
 client-side configuration for, 205–211
 requirements for, 196–198
 server-side configuration for, 198–204
 specifying RPC proxy ports for, 202–204
 troubleshooting, 210
 reporting software, 264, 269
 Resolve anonymous e-mail setting (SMTP), 59, 87
 resources for further information
 administrators, mailbox access and, 36
 antispam software, 221
 antivirus software, 247
 blocking attachments, 253
 CAs, 105, 197
 DCOM, disabling support for in RPC over HTTP, 204
 disclaimer, adding to SMTP messages, 79
 Exchange 2000, e-mail spoofing and, 87
 Exchange Edge services, 239
 Exchange Server 2003, 8, 12
 Exchange Server 2003 Security Hardening Guide, 13, 150
 Hfnetchk utility, 12
 IIS, endless loop problems and, 123
 inheritance/Windows security, 27
 Intelligent Message Filter, 238
 Internet mail headers, 91
 IPSec, 150, 188
 ISA Server, 152, 155
 junk e-mail filter (Outlook 2003), 214
 .mail domain antispam initiative, 92
 MAPI permissions, 49
 MBSA utility, 11
 Microsoft Trustworthy Computing Initiative, 3
 open relays, 82
 OWA
 registry key settings for, 169
 security flaw in, 102
 segmentation of, 120
 POP3/IMAP4 banners, modifying, 78
 reporting software, 264, 270
 S/MIME, 158, 193
 SMTP connectors, 67
 Ten Immutable Laws of Security (The), 21
 upgrades, 8
 URLScan security tool, 127
 virus protection, 251
 VSAPI vendors, 246
 Windows 2000 Server, disabling services and, 141
 Windows event auditing, 263
 Return Status Code options (connection filtering), 227
 reverse DNS lookup feature, 87–89
 reverse records, 89
 rich clients (OWA), 173
 RID master, 277
 RIDs (relative IDs), 277
 rights. *See* permissions
 risks, security planning and, 289–291
 root certificate services, 105
 RPC over HTTP. *See* Remote Procedure Calls over Hypertext Transfer Protocol
 RPC traffic. *See* Remote Procedure Call traffic
 RUS process, 16
- S**
- SA (software assurance), IMF and, 222, 238, 239
 safe computing practices, 20

- safe recipients
 - in Outlook 2003, 218
 - in OWA, 162, 164
- safe senders
 - in Outlook 2003, 217
 - in OWA, 162, 163
- SANS Institute, 20
- Sawmill (log-reporting vendor), 75
- ScanMail Suite for Microsoft Exchange antivirus software, 248
- schema master, 276
- SCLs (spam confidence levels), 238
- secure by default initiative. *See* Trustworthy Computing Initiative
- Secure Mail Server Publishing Wizard (ISA Server), 153
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
 - OWA support for, 158–161
 - securing clients via, 192–195
 - version 3 of, 193
- Secure Password Authentication (SPA), 303
- Secure Sockets Layer (SSL)
 - OWA, enabled on, 103–116
 - Change Password feature and, 121
 - enabled manually vs. automatically, 113
 - forms-based authentication and, 170
 - front-end/back-end scenarios and, 116
 - testing functionality of, 113–115
 - RPC virtual directory, enabled on, 201
 - third-party certificates and, 185
- security
 - best practices for, 9–24
 - features of in Exchange 2003 (overview), 1–8
 - physical considerations and, 21
 - requirements in your organization and, 289–291
 - safe computing practices for, 20
- Security Bulletins (Microsoft), 13
- “This Security Certificate Was Issued by a Company That You Have Not Chosen to Trust” error message, 197
- security IDs (SIDs), 277
- Security log (Event Log Service), 262
- security principles, 277
- security updates, 293
 - checking for weekly or monthly, 19
 - keeping current, 10–13
- sender filtering
 - in Outlook 2003, 219, 235–237
 - filtering rule warning box and, 232
 - in OWA, 162, 164–166
 - senders, safe
 - in Outlook 2003, 217
 - in OWA, 162
- server availability report (Exchange 2003 Management Pack), 269
- server roles, 272–285
 - security issues and, 292–303
 - types of (list), 274
- server-side spam filtering, 222–237
 - antispam software and, 165
- server-side virus protection, 244–249
- server software, upgrading, 8
 - message limit settings and, 68
- servers, securing, 285–303
 - customizations for, 292–303
 - planning a strategy for, 285–292
- session limits, setting, 67, 68
- shared computers, OWA session default timeout and, 174
- Shinder, Thomas (Dr.)
 - ISA Server and, 152, 155
 - publishing Exchange protocols and, 198
- SIDs (security IDs), 277
- Simple Mail Transfer Protocol (SMTP), 55–92
 - disabled on front-end server, 140
 - e-mail spoofing and, 85–89
 - encrypting traffic and, 179–189
 - Exchange 2003 design and, 2
 - Mailbox Store and, 141
 - monitoring software for, 269
 - new implementation of, 238
 - Public Folder Store and, 143
 - securing, 56–80
 - See also* entries at SMTP
- single-server deployment scenario, 134
- Slipstick Systems, 253

- smart hosts, 80
 SmartScreen technology (Microsoft), 214, 237
S/MIME. *See* Secure/Multipurpose Internet Mail Extensions
 S/MIME e-mail error message, 161
SMTP. *See* Simple Mail Transfer Protocol
 SMTP addresses
 blocking via junk e-mail filter, 162
 exception lists and, 229
 SMTP Auth attacks, 3
 SMTP BADMAIL directory, examining weekly or monthly, 19
 SMTP banner, modifying, 75–78
 SMTP connectors, 64–67
 TLS/SSL and, 188
 SMTP filter, 154
 SMTP gateways
 single-server scenario and, 135
 virus protection for, 248
 SMTP relaying, 80–85
 caution with settings for, 82
 open relay testing and, 83–85
 SMTP Transport Event Sink, 79
 SMTP virtual servers, applying filtering rules to, 232–234
 smtpmd.exe utility, 78
 sniffer devices, 180
 software assurance (SA), IMF and, 222, 238, 239
SPA (Secure Password Authentication), 303
 spam confidence levels (SCLs), 238
 spam, combatting, 213–240
 antispam software for, 165, 221
 See also filtering; e-mail junk filter
 SpamLArt Open Relay Testing, 85
 SpamNet software, 221
 spoofing e-mail addresses, 59, 85–89
 SQL Server (Microsoft), 301
 SSL. *See* Secure Sockets Layer
 SSL certificates, 60, 103
 TLS/SSL and, 180–185
 SSL port, specifying, 111
 SSL requests, redirected from HTTP requests, 127–131
 status codes, for real-time blacklists, 228
 Storage Group, caution with, 144
 streaming media servers, 275
 strong passwords, 3, 295
 Sunbelt's iHateSpam software, 221
 Sybari's Antigen for Microsoft Exchange antivirus software, 249
 Symantec Mail Security for Microsoft Exchange antivirus software, 248
 system attendant service, 16
 System log (Event Log Service), 262
- T**
- Telnet, using for open relay testing, 83
 Ten Immutable Laws of Security (The), 21
 terminal servers, 274, 282, 285
 threats, security planning and, 289–291
 TLS encryption, setting for (SMTP), 59
TLS/SSL. *See* Transport Layer Security/Secure Socket Layer
 tools. *See* utilities
 Transport Layer Encryption (TLS encryption), setting for, 59
 Transport Layer Security/Secure Socket Layer (TLS/SSL)
 configuring, 180–185
 enabling, 185–188
 cautions with, 186, 187
 on POP3/IMAP4 virtual servers, 190
 Trend Micro's ScanMail Suite for Microsoft Exchange antivirus software, 248
 Trojan horses, 242
 Trustworthy Computing Initiative (Microsoft), 2–4
 antispam features and, 214
 enhanced attachment blocking and, 170
 Web beacon blocking and, 167
- U**
- “unable to expand folder” error message, 35
 upgrading server software, 8
 message limit settings and, 68
 UPNs (user principal names), OWA logon and, 173

URLScan utility, 150
 password changes and, 127
 usage and health report (Exchange 2003 Management Pack), 270
 user principal names (UPNs), OWA
 logon and, 173
 users
 defining acceptable-use policies and, 19
 educating about virus protection/e-mail handling, 87, 250–253
 outgoing e-mail messages and, configuring footer for, 79
 passwords for, changing via OWA, 120–127
 endless loop problems and, 123
 lag time and, 126
 testing for, 125–127
 restricting access to OWA, 116–120
 via bulk changes, 118
 Users setting (SMTP), 60, 63
 utilities
 Adaware, 250
 ADMModify, 118
 Configure Your Server, 272–275
 for disclaimers, 79
 for Exchange 2003, 118
 Exchange Administration Delegation Wizard, 26, 30–35
 ExMerge, 254–259
 for file attachment blocking, 253
 Hfnetchk, 12
 log-reporting, 75
 Manage Your Server, 272
 MBSA, 10
 MetaEdit, 78
 open relay testers, 85
 PestPatrol, 250
 smtpmd.exe, 78
 URLScan, 127, 150

V

virtual directories
 IISADMPWD, creating, 121–124
 OWA, 94–102
 Virtual Private Network connections
 (VPN connections), 195
 virus scanners, 245–248
 file-level, 247

Virus Scanning API (VSAPI), 245, 246
 viruses, protecting against, 241–260
 cleaning up after a virus outbreak, 254–259
 client-side protection, 249
 educating users and, 250–253
 server-side protection, 244–249
 VPN connections, 195
 VSAPI (Virus Scanning API), 245, 246

W

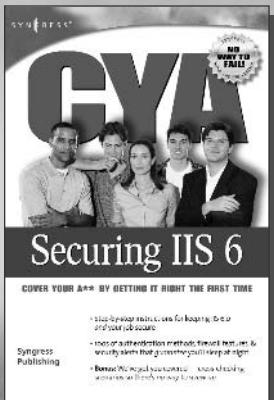
Web beacon-blocking feature, 166
 Web servers, 280–282
 securing, 300
 web sites
 EventID errors, 265
 InstantSSL, 195
 ISAservice, 155
 Microsoft Exchange Security, 8
 Microsoft Operations Manager, 264
 open relay test services, 85
 Windows updates, 293
 Windows 2000/2003, 2
 auditing, 262–264
 checklist for installing Windows 2003, 23
 disabling services in Windows 2000, 141
 Exchange 2003 dependencies on, 13–18
 list of, 14
 security, best practices for, 9–24
 See also operating systems
 Windows Management Instrumentation (WMI), 278
 Windows Update web site, 293
 WINS servers, 274, 280
 securing, 299
 WMI (Windows Management Instrumentation), 278
 worms, 168, 242

Z

.zip files, Bagle worm and, 243
 Zone Alarm firewall, 250

Syngress: The Definition of a Serious Security Library

Syn•gress (sin-gres): noun, sing. Freedom from risk or danger; safety. See *security*.



AVAILABLE MAY 2004!
ORDER at
www.syngress.com

CYA: Securing IIS 6.0

Networking professionals responsible for configuring, maintaining, and troubleshooting Microsoft's Internet Information Server 6.0 will find this book indispensable. They operate in high-stress environments where competitive business demands often run counter to "best practices." Design and planning lead times are non-existent and deployed systems are subject to constant end-runs. But at the end of the day, they are held accountable if things go wrong. They need help. They need to guarantee they've configured their network professionally and responsibly. They need to CYA.

ISBN: 1-931836-25-6

Price: \$39.95 US \$59.95 CAN

The Best Damn Windows Server 2003 Book Period

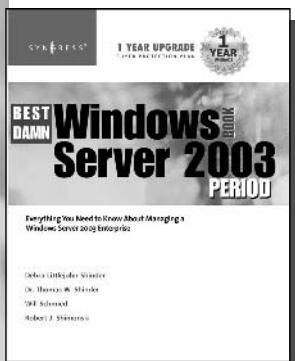
Susan Snedaker

Windows Server 2003 is certainly Microsoft's most robust, and complex, enterprise operating system developed to date. Any one of the component "services" in Server 2003 has more features and functionality than existed in the entire Windows NT 4 operating system! In addition, the audience of system administrators has now evolved to a highly professional, skills certified community of IT professionals with a need for the tens of thousands of pages of Microsoft documentation and web-based support to be distilled into a concise, applied format. This is the book that meets the needs of today's Windows Server 2003 professional.

ISBN: 1-931836-12-4

Price: \$59.95 US \$79.95 CAN

AVAILABLE JUNE 2004!
ORDER at
www.syngress.com



solutions@syngress.com

SYNGRESS®