Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveSync, MSDN, MS-DOS, Outlook, Visual Basic, Visual C++, Visual Studio, Win32, Windows, Windows Mobile, Windows NT and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Acknowledgments

Project Editor: Olinda Turner

Contributing Writers: Tammy Treit, Teresa Appelgate, Jon Hoerlein, Joey Masterson, Christopher Budd

Contributing Editors: Lindsay Pyfer, Diane Forsyth, Cathy Anderson, Alison Hirsch, Tony Ross, Lee Ross

Technical Reviewers: Amanda Langowski, Brad Owen, James O'Brien, Eric Dao, Brian Holdsworth, Max Cicciotosto, Simon Attwell, Wayne Cranston, Pretish Abraham, Khyati Vyas, Scott Landry, Aidan Delaney, Evan Dodds, Ryan Hurey; Ladislau Conceicao, Michael Lee, Julian Zbogar-Smith, Jeetendra Falodia, Dave Whitney, Andrew Moss, Chris Ahlers, David Emmick, Catalin Stafie, Jaya Matthew

Graphic Design: Kristie Smith

Production: Sean Pohtilla, Joe Orzech
Table of Contents

Introduction

Overview .......................................................................................................... 1
What Will You Learn from This Book?.................................................................1
Who Should Read This Book? ..........................................................................2
Terminology .......................................................................................................2
How is This Book Structured? .........................................................................3
What Are the Requirements to Complete the Procedures In This Book? ...........5

Chapter 1
Preparation to Administer Exchange Server 2003 .................................... 7
Understanding Exchange Administration Architecture .....................................8
    Interacting with Active Directory............................................................9
    Selecting the Right Management Tools................................................11
Working with Exchange System Manager.......................................................12
Working with Active Directory Users and Computers....................................14
    Creating Recipients.............................................................................16
    Performing Exchange Tasks...............................................................17
    Managing Exchange in Multiple Domains.............................................18
Deciding Where to Manage Exchange.............................................................18
    Setting Up a Management Station.......................................................19
Using Custom Consoles..................................................................................22
    Creating Custom Consoles...............................................................24
Automating Administrative Tasks..................................................................25
Chapter 2
Managing an Exchange Organization ......................................................... 27
Promoting an Exchange Organization from Mixed Mode to Native Mode .......... 28
Applying Global Settings ............................................................................. 30
  Associating File Name Extensions with MIME ........................................... 30
  Using SMTP Policies to Control Outbound Mail Formatting and Automatic Responses ......................................................... 32
  Selecting Message Delivery and Message Filtering Options ...................... 36
Creating and Managing Administrative Groups ........................................... 44
  Understanding the Types of Administrative Models ..................................... 45
  Displaying Administrative Groups .............................................................. 50
  Creating Administrative Groups ................................................................. 51
  Moving Objects Between Administrative Groups ........................................ 51
  Deleting Administrative Groups ................................................................. 52
Using System Policies ................................................................................. 52
  Understanding How System Policies Affect Individual Settings .................. 54
  Creating a Server Policy ............................................................................. 55
  Adding Servers to a Server Policy ............................................................... 57
  Viewing the Objects Controlled by a System Policy ..................................... 57
  Copying System Policies Between Administrative Groups ....................... 58
  Modifying or Removing a Policy ................................................................. 59
Managing Permissions .................................................................................. 60
  Understanding Exchange Objects and Exchange System Manager ............. 60

Chapter 3
Configuring Exchange Server Settings ....................................................... 67
Configuring Server-Specific Settings ......................................................... 68
Viewing Messages in Message Tracking Center ......................................... 69
Enabling Message Tracking ......................................................................... 69
  Managing Message Tracking Log Files ..................................................... 70
Designating a Front-End Server .................................................................. 71
Sending Error Information to Microsoft ...................................................... 72
Configuring Language Settings ................................................................. 73
Scheduling Mailbox Manager Processes ...................................................... 74
  Defining a Schedule ................................................................................ 76
  Setting Reporting Options ...................................................................... 76
Configuring Diagnostics Logging on a Server .............................................. 77
Customizing Public Folder Referrals .............................................................. 80
Assigning Costs on the Public Folder Referrals List ........................................ 82
Understanding Directory Access Options .......................................................... 83
Automatically Constructing a Topology for Directory Access .............................. 85
Manually Constructing a Topology for Directory Access ...................................... 86
Viewing System Policies Applied to the Server .................................................... 87
Setting Server-Specific Permissions ................................................................. 89
Configuring System Resource Usage During Full-Text Indexing .......................... 90

Chapter 4
Managing Recipients and Recipient Policies ....................................................... 93
Understanding Recipients .................................................................................... 93
Understanding Recipient Policies ........................................................................ 96
Managing E-Mail Addresses .................................................................................. 97
Managing Mailboxes Using Mailbox Manager ..................................................... 99
Creating Recipients ............................................................................................. 101
Mailbox-Enabled and Mail-Enabled Recipients .................................................... 102
Mail-Enabled Groups ......................................................................................... 104
Understanding Query-Based Distribution Groups .............................................. 107
Query-Based Distribution Groups Described ..................................................... 107
Modifying Exchange 2000 SP3 Servers for Use with Windows 2000 Global Catalog Servers ......................................................................................... 108
How Query-Based Distribution Groups Work .................................................... 109
Deployment Recommendations for Query-Based Distribution Groups ............. 109
Guidelines for Creating Query-Based Distribution Groups ............................... 111
Creating Query-Based Distribution Groups ....................................................... 112
Combining Multiple Query-Based Distribution Groups ..................................... 114
Managing Recipients .......................................................................................... 115
Notes for Exchange 5.5 Administrators ............................................................... 115
Managing Recipients with Recipient Policies ..................................................... 116
Managing Recipient Settings ............................................................................. 120
Configuring Message Settings for Mailbox-Enabled Recipients ......................... 121
Exchange Advanced Settings for Mailbox-Enabled Recipients ............................ 123
Configuring Message Settings for Mail-Enabled Recipients .............................. 127
Distribution Groups ......................................................................................... 128
<table>
<thead>
<tr>
<th>Understanding Address Lists</th>
<th>Address Lists Described</th>
<th>Creating Address Lists</th>
<th>Offline Address Lists</th>
<th>Customizing the Details Templates</th>
<th>Recipient Update Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>129</td>
<td>130</td>
<td>131</td>
<td>134</td>
<td>136</td>
<td>138</td>
</tr>
</tbody>
</table>

**Chapter 5**

**Understanding and Configuring Message Routing and Transport**

<table>
<thead>
<tr>
<th>Configuring Routing for Internal Mail Flow</th>
<th>Understanding Routing Groups</th>
<th>Creating Routing Groups</th>
<th>Moving Servers Between Routing Groups</th>
<th>Renaming a Routing Group</th>
<th>Deleting a Routing Group</th>
<th>Connecting Routing Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>141</td>
<td>142</td>
<td>146</td>
<td>148</td>
<td>148</td>
<td>149</td>
<td>150</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connecting to the Internet</th>
<th>Defining SMTP Dependencies</th>
<th>Configuring SMTP</th>
<th>Using a Wizard to Configure Internet Mail</th>
<th>Manually Configuring the Sending of Internet Mail</th>
<th>Manually Configuring the Receipt of Internet Mail</th>
<th>Enabling Filtering to Control Junk E-Mail Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>154</td>
<td>155</td>
<td>157</td>
<td>158</td>
<td>161</td>
<td>173</td>
<td>178</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connecting to Exchange 5.5 Servers and Other X.400 Systems</th>
<th>Customizing the X.400 Protocol</th>
<th>Understanding X.400 Connectors</th>
<th>Disabling or Removing Connectors</th>
<th>Using Queue Viewer to Manage Messages</th>
<th>Disabling Outbound Mail</th>
<th>Finding Messages</th>
<th>Using SMTP Queues to Troubleshoot Message Flow</th>
<th>Using X.400 (MTA) Queues to Troubleshoot Message Flow</th>
</tr>
</thead>
<tbody>
<tr>
<td>180</td>
<td>181</td>
<td>182</td>
<td>192</td>
<td>193</td>
<td>194</td>
<td>195</td>
<td>196</td>
<td>200</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuring Diagnostic Logging for SMTP</th>
<th>Modifying Logging Settings</th>
<th>Enabling Debugging Level Logging</th>
<th>Configuring Diagnostic Logging for the X.400 Service (MSExchangeMTA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>201</td>
<td>202</td>
<td>203</td>
</tr>
</tbody>
</table>
# Chapter 6

## Managing Client Access to Exchange .......................................................... 205

- Preparing to Manage Client Access ................................................................ 206
- Choosing a Topology ................................................................................. 207
- Configuring Security for Client Access ....................................................... 208
- Choosing Client Access Model and Protocols .............................................. 208
- Configuring Clients and Devices ................................................................. 209

## Managing Protocols ................................................................................. 209

- Enabling a Virtual Server ............................................................................ 210
- Assigning Ports and an IP Address to a Virtual Server ............................... 211
- Setting Connection Limits .......................................................................... 212
- Starting, Stopping, or Pausing a Virtual Server .......................................... 213
- Terminating Connected Users ...................................................................... 214
- Managing Calendaring Options for the POP3 and IMAP4 Virtual Servers ... 214
- Managing the HTTP Virtual Server .............................................................. 215
- Working with IMAP4-Specific Settings ....................................................... 217
- Configuring NNTP Posting Limits and Moderation Settings ....................... 218

## Managing Outlook 2003 ............................................................................ 220

- Configuring Cached Exchange Mode .......................................................... 220

## Managing Outlook Web Access ................................................................. 221

- Enabling and Disabling Outlook Web Access for Internal Clients Only ...... 222
- Using Browser Language ............................................................................ 223
- Setting Up a Logon Page ............................................................................. 224
- Enabling Outlook Web Access Compression .............................................. 227
- Blocking Web Beacons .............................................................................. 228
- Blocking Attachments ................................................................................ 229
- Filtering Junk E-Mail Messages .................................................................. 230
- Simplifying the Outlook Web Access URL ................................................. 231

## Managing Exchange ActiveSync ............................................................... 232

- Enabling Exchange ActiveSync for Your Organization ............................ 232
- Enabling Up-to-Date Notifications for Your Organization ....................... 234

## Managing Outlook Mobile Access ............................................................. 236

- Configuring Exchange to Use Outlook Mobile Access .............................. 236
- Enabling Outlook Mobile Access for Your Organization ......................... 237
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing Your Exchange Cluster Configuration</td>
<td>329</td>
</tr>
<tr>
<td>Configuring Exchange Virtual Server Settings</td>
<td>329</td>
</tr>
<tr>
<td>Configuring Exchange Cluster Resources</td>
<td>336</td>
</tr>
<tr>
<td>Taking Exchange Virtual Servers or Exchange Resources Offline</td>
<td>345</td>
</tr>
<tr>
<td>Adding IMAP4 and POP3 Resources</td>
<td>347</td>
</tr>
<tr>
<td>Adding a Node</td>
<td>349</td>
</tr>
<tr>
<td>Adding an Exchange Virtual Server</td>
<td>349</td>
</tr>
<tr>
<td>Removing an Exchange Virtual Server</td>
<td>350</td>
</tr>
<tr>
<td>Moving All Mailboxes and Public Folder Content</td>
<td>352</td>
</tr>
<tr>
<td>Taking the Exchange System Attendant Resource Offline</td>
<td>353</td>
</tr>
<tr>
<td>Using Cluster Administrator to Remove the Exchange Virtual Server</td>
<td>353</td>
</tr>
<tr>
<td>Deleting the Remaining Cluster Resources</td>
<td>354</td>
</tr>
<tr>
<td>Removing Exchange 2003 from a Cluster Node</td>
<td>354</td>
</tr>
<tr>
<td>Migrating an Exchange Cluster Node to a Stand-Alone (Non-Clustered) Server</td>
<td>356</td>
</tr>
<tr>
<td>Monitoring Performance of an Exchange Cluster</td>
<td>356</td>
</tr>
<tr>
<td>Monitoring Active/Passive Clusters</td>
<td>356</td>
</tr>
<tr>
<td>Monitoring Active/Active Clusters</td>
<td>357</td>
</tr>
<tr>
<td>Monitoring Virtual Memory in a Cluster</td>
<td>357</td>
</tr>
<tr>
<td>Enabling Exchange Logging</td>
<td>360</td>
</tr>
<tr>
<td>Tuning Servers in a Cluster</td>
<td>362</td>
</tr>
<tr>
<td>Removing Exchange 2000 Tuning Parameters</td>
<td>362</td>
</tr>
<tr>
<td>Setting the /3GB Switch</td>
<td>363</td>
</tr>
<tr>
<td>Configuring /Userva and SystemPages</td>
<td>363</td>
</tr>
<tr>
<td>Troubleshooting Your Exchange Clusters</td>
<td>363</td>
</tr>
<tr>
<td>Identifying the Cause of a Failure</td>
<td>364</td>
</tr>
<tr>
<td>Performing Disaster Recovery on Your Exchange Clusters</td>
<td>365</td>
</tr>
</tbody>
</table>

**Appendix A**

Tools Used with Exchange ........................................................................ 369

**Appendix B**

Services Used by Exchange ...................................................................... 383

**Appendix C**

Configuration Settings for a Four-Node Cluster ................................. 389
Appendix D
Identifying and Accessing Exchange Store Components ......................... 391

Appendix E
Controlling Public Folder Replication .......................................................... 395
How Replication Works ................................................................................. 396
The Basic Hierarchy and Content Replication Process ................................. 399
Status and Backfill Messages ........................................................................ 401
Configuring the Default Replication Schedule ............................................. 407
Configuring Replicas .................................................................................. 408
Adding or Removing Content Replicas ......................................................... 409
Setting a Folder-Specific Replication Schedule ........................................... 409
Setting Replication Message Priority ......................................................... 409
Checking Replication Status ....................................................................... 410
Replicating Data Manually ......................................................................... 412
Special Considerations for Mixed-Mode Topologies ..................................... 413
Connection Agreements and Public Folder Replication ................................. 413
Avoiding Common Replication Problems in Mixed Mode ............................ 418
Managing Inter-Organization Replication .................................................... 420

Appendix F
Using Full-Text Indexing ............................................................................. 423
Verifying Recommended Hardware Configurations ...................................... 423
Preparing Your Exchange 2003 Organization ............................................... 424
Deploying Full-Text Indexing ...................................................................... 424
Creating a Full-Text Index .......................................................................... 425
Optimizing Full-Text Indexing .................................................................... 425
Performing a Full Population ....................................................................... 432
Setting a Schedule for Incremental Populations ......................................... 434
Enabling Full-Text Indexing Queries ............................................................ 436
Notifying and Educating Users ................................................................... 436
Managing Full-Text Indexing ..................................................................... 436
Appendix G

Troubleshooting and Repairing Store Problems................................. 439

Problems with Full-Text Indexing................................................................. 439
  Safe Event Viewer Messages ................................................................. 440
  Population Process Is Slow ................................................................. 441
  Population Process Is Found in a Paused State ................................. 442
  Deleted Message Is Still Visible in Search Results ............................ 442
  Wrong Location Is Displayed After Moving the Index ......................... 442
  Using Gather Log Entries to Identify Problems ................................. 443
  Language Settings Problems ............................................................... 443
  Queries Fail During Server Startup ..................................................... 446
  Restoring Missing Performance Counters .......................................... 446
  Avoiding Disk Bottlenecks ................................................................. 447
  High Paging ....................................................................................... 447

Problems with Permissions in a Mixed Exchange 5.5-Exchange 2003 Environment.... 447
  Determine What is Preventing a User from Seeing the Public Folder in Outlook ... 448
  View Access Control Lists in Exchange System Manager .................. 448
  Monitor Permissions Events in Event Viewer ........................................ 449

Problems with Public Folder Replication .............................................. 453
  Replication Messages Not Being Received ....................................... 453
  Backfill Takes a Long Time ............................................................... 454
  Server Does Not Appear to Backfill .................................................. 454

Other Problems ..................................................................................... 454
  Unable to Access Permissions on a Public Folder (Invalid Windows Handle Error) 455
  One or More Users Could Not Be Added to the Folder Access List ........ 456
  Mail Messages to Public Folder Were Not Delivered .......................... 456
  Outlook Web Access Cannot View a Public Folder After the Tree Has Been Renamed ............................................................. 457
  Message "Operation Failed" When Attempting to Access a Tree Using Exchange System Manager ............................................. 457
  Exchange 5.5 Servers See Multiple Public Folder Stores on an Exchange 2003 Server ............................................................... 457
  In a Mixed Exchange 5.5-Exchange 2003 Environment, Users Cannot Access a Public Folder Using Outlook Web Access ......................... 458
  Attachment Exceeds Storage Limit on Public Folder .......................... 459
Appendix H

Additional Resources ................................................................. 461
  Web Sites ...................................................................................... 461
  Exchange Server 2003 Books ....................................................... 461
  Exchange 2000 Server Books ....................................................... 462
  Technical Articles ........................................................................ 462
  Tools .......................................................................................... 462
  Resource Kits ............................................................................. 463
  Microsoft Knowledge Base Articles ........................................... 463

Glossary ..................................................................................... 465
INTRODUCTION

Overview

Building on the solid foundation of Microsoft® Exchange 2000 Server, Microsoft Exchange Server 2003 offers new features and improvements in reliability, manageability, and security. This book will help you make the most of these improvements by explaining the core concepts of Exchange administration.

Within each chapter of this book, there is a discussion about particular Exchange features, how these features work within the Exchange architecture, and how to configure and manage these features for optimal results. The features and related tasks that are covered in this book range from configuring global settings at an organization level to managing individual servers to handling specific configuration needs such as Exchange clients and clustering. After reading this book you should have a solid understanding of what it takes to configure and manage your Exchange 2003 organization.

What Will You Learn from This Book?

Essentially, this document provides detailed answers to the following questions:

• What information do I need to know to prepare myself to administer Exchange 2003? (Chapter 1)

• How do I configure settings at both the organization level and the server level to achieve specific Exchange 2003 goals? (Chapter 2 and Chapter 3)

• What do I need to know about recipients, messaging, the Exchange store, e-mail clients, and Exchange clusters to manage these aspects of Exchange effectively? (Chapters 4–8)

• How do I manage e-mail recipients in my organization effectively? (Chapter 4)

• What do I need to understand about routing groups, Simple Mail Transfer Protocol (SMTP), and Internet connectivity to enable message flow in my organization? (Chapter 5)

• How do I provide and support e-mail clients for my users? (Chapter 6)

• How do mailbox stores and public folder stores work in Exchange 2003? What do I need to know to administer them effectively? (Chapter 7)
• How do I effectively administer clusters to achieve maximum reliability and availability? (Chapter 8)
• What tools and services are available for managing Exchange 2003? (Appendix A and B)
• What is the recommended configuration for a four-node Exchange 2003 cluster? (Appendix C)
• How do internal components interact in the Exchange store, and what I should know about these components? (Appendix D)
• What do I need to know about public folder replication and the replication process? (Appendix E)
• What is full-text indexing, and how can I effectively use full-text indexing in my organization? (Appendix F)
• What tools and processes can I use to troubleshoot and remedy mailbox and public folder store problems? (Appendix G)

Who Should Read This Book?

Although practically anyone with a technical background can benefit from reading this book, it is designed to produce maximum benefits for the following professionals:

**Enterprise Exchange Administrators**
Those individuals who are responsible for installation, maintenance, and administration of software in the enterprise.

**Exchange User Account Managers**
Those individuals who are responsible for setting up individual e-mail accounts and modifying individual Exchange accounts in the Microsoft Active Directory® directory service.

Terminology

Before reading this book, familiarize yourself with the following terms:

**A record**
An address resource record in DNS; specifically, a DNS record that associates a host name with an IP address.
Bridgehead Server

A computer that connects servers using the same communications protocol so that information can be passed from one server to another. In Exchange 2003 and Exchange 2000, a bridgehead server is a connection point from a routing group to another routing group, remote system, or other external system.

Connector

A component that enables information to flow between two systems. For example, connectors support message transfer, directory synchronization, and calendar querying between Exchange and other messaging systems. When connectors are in place, the basic user experience is maintained on both messaging systems. The exchange of mail and other information between Exchange and other messaging systems is transparent to the user, even if the two systems function differently.

Mail-enabled

A recipient that can receive e-mail but does not have a mailbox in your Exchange organization. Mail-enabled recipients do not use your Exchange organization to send e-mail.

Mailbox-enabled

A recipient that can both send and receive e-mail, and has a mailbox in your Exchange organization where e-mail and other items can be stored.

Recipient

Any Active Directory object that can receive e-mail. Users, InetOrgPerson objects, Groups, Contacts, and Public Folders can all be recipients.

How is This Book Structured?

This document is divided into eight chapters, eight appendixes, and a glossary:

Chapter 1, "Preparing to Administer Exchange Server 2003"

This chapter explains the dependency of Exchange on Active Directory, introduces the two primary tools used to administer Exchange, gives examples of how to efficiently use those tools, and briefly discusses the automation of administrative tasks using the Exchange Software Development Kit (SDK).

Chapter 2, "Managing an Exchange Organization"

This chapter covers the administrative tasks that affect an entire Exchange organization. Among the topics that are covered are promoting an organization from mixed mode to native mode, applying global settings, working with administrative groups, using system policies, and working with permissions.

Chapter 3, "Configuring Exchange Server Settings"

This chapter covers the administrative tasks that affect individual Exchange servers. Among the topics that are covered are configuring basic server settings, using language settings to support different languages, cleaning mailboxes, setting up diagnostic logging for specific components, using public folder referrals, configuring Directory Access options, using security settings on a server, and configuring full-text indexing settings.
Chapter 4, "Managing Recipients and Recipient Policies"
This chapter explains what recipients and recipient policies are, how to create and manage recipients, how to manage address lists, and how to use the new query-based distribution list feature in Exchange 2003.

Chapter 5, "Understanding and Configuring Message Routing and Transport"
This chapter explains how messages are sent within an organization, how to connect to the Internet, how to connect to Microsoft Exchange Server version 5.5 or X.400 systems, how to manage messages, and how to configure diagnostic logging for SMTP and the X.400 service.

Chapter 6, "Managing Client Access to Exchange"
This chapter looks at client access in the context of a front-end and back-end server architecture. The first part of this chapter explains what is meant by a front-end/back-end architecture, and what the dependencies are in selecting this architecture. The chapter then focuses on configuring individual clients for Exchange.

Chapter 7, "Managing Mailbox Stores and Public Folder Stores"
This chapter describes the permissions that protect the Exchange store, as well as how to work with different elements of the Exchange store, including managing mailboxes and public folders.

Chapter 8, "Managing Exchange Clusters"
This chapter begins with a brief review of what Exchange clusters are. It then covers the various administrative tasks that are associated with clusters, including customizing your cluster configuration; adding resources, a node, or an Exchange Virtual Server; removing either an Exchange Virtual Server or Exchange 2003 from a cluster; and monitoring cluster performance.

Appendix A, "Tools Used with Exchange"
This appendix lists a variety of tools that you can use to manage and troubleshoot your Exchange organization.

Appendix B, "Services Used by Exchange"
This appendix lists the various services that run on an Exchange server.

Appendix C, "Configuration Settings for a Four-Node Cluster"
This appendix describes the recommended configuration settings for a four-node cluster that contains three active nodes and one passive node.

Appendix D, "Identifying and Accessing Exchange Store Components"
This appendix lists the various components of the Exchange store, and how to work with them.

Appendix E, "Controlling Public Folder Replication"
This appendix includes procedures for configuring replication. It also describes how replication works, and what aspects of your Exchange topology affect the replication process.

Appendix F, "Using Full-Text Indexing"
This appendix describes how to set up full-text indexes, and how to optimize and maintain the indexes.
Appendix G, "Troubleshooting and Repairing Store Problems"
This appendix describes the common problems, events, and messages that are related to managing mailbox and public folder stores. It also includes information about what causes the problems and possible solutions.

Appendix H, "Additional Resources"
This appendix contains links to additional resources that are available to help you maximize your understanding of how to administer Exchange 2003.

Glossary
This appendix provides comprehensive definitions for the terms used within this book.

What Are the Requirements to Complete the Procedures In This Book?
To successfully complete all of the procedures that are covered in this book, ensure that you have fulfilled the following requirements. Keep in mind that these lists provide an overview of the maximum requirements for performing these procedures.

Security-specific Hardware Requirements
The following hardware is required to perform the procedures that are covered in this book. This list does not include your general Exchange servers, storage hardware, and so on. It only includes security-specific hardware requirements:

- 2 firewalls (or routers)
- RSA SecurID PIN generators (for each mobile client)
- Minimum of 1 front-end server running Microsoft Internet Security and Acceleration Server

Software Requirements
The following software is required to perform the procedures that are covered in this book:

- Microsoft Exchange Server 2003 Enterprise Edition
- Microsoft Internet Security and Acceleration Server
- Microsoft Windows 2000 Advanced Server
- RSA SecurID Server version 1.x
Before you start managing Microsoft® Exchange Server 2003, it is useful to understand the administration architecture that Exchange uses and how this architecture influences the tools that you use to manage Exchange. Exchange 2003 interacts with and depends upon data in the Microsoft Active Directory® directory service. It also stores and retrieves data from other places, including the mailbox store, the Microsoft Windows® registry, and the Exadmin virtual directory. To access and manage Exchange data, there are two Microsoft Management Console (MMC) snap-ins—Exchange System Manager and Active Directory Users and Computers—where you will spend the majority of your time as an administrator.

After understanding Exchange administration architecture and the tools that you use to interact with Exchange, the next step is to determine how to efficiently use those tools. You may decide to set up a dedicated management station from which to manage multiple servers in the organization. You may also decide to create a customized management console that combines separate MMC snap-ins into one console. You may even want to automate additional administrative tasks using the Exchange Software Development Kit (SDK). You will find information about these choices in the latter portion of this chapter.
Understanding Exchange Administration Architecture

Exchange 2003 uses Active Directory to store and share information with Windows. Thus, all of the directory information that you create and maintain in Windows, such as organizational unit structure and groups, can also be used from Exchange.

The Active Directory schema can be extended to include custom attributes and object types to centralize and minimize data administration, as well as to make data available to applications that can access Active Directory information. In fact, when you install your first Exchange server, Exchange 2003 extends the Active Directory schema to include Exchange-specific information. Extending the schema affects the entire forest and, depending on the size of Active Directory, may take a considerable amount of time to complete.

Because Active Directory serves as a single-source directory for all of the objects in your organization, Exchange uses this information to reduce administrative overhead. With Active Directory, you can store and organize information about users, such as names, e-mail addresses, and phone numbers. This information is stored as attributes of the user object. Exchange and other applications can use this information. For example, the address lists to which a recipient belongs are written as values to the ShowInAddressBook attribute in that recipient's Active Directory object. To create address lists, Exchange performs Lightweight Directory Access Protocol (LDAP) queries on each of these objects and retrieves the information stored in the ShowInAddressBook attributes.

Note
Because Exchange 2003 relies on Active Directory, it is important that you be familiar and comfortable with Active Directory terminology, structure, and navigation. For a comprehensive overview of Active Directory, review the documentation that came with your copy of Windows. For more information about Exchange integration with Active Directory, see the books Planning an Exchange 2003 Messaging System and Exchange Server 2003 Deployment Guide (www.microsoft.com/exchange/library).

Microsoft Exchange Server version 5.5 and earlier do not use Active Directory. If your messaging topology is in mixed mode (contains both Exchange 2003 and Exchange 5.5 or earlier), you can still use Active Directory by using Active Directory Connector (ADC) to replicate directory information between the Exchange 5.5 directory and Active Directory. For more information about ADC, see the book Exchange Server 2003 Deployment Guide (www.microsoft.com/exchange/library).
Interacting with Active Directory

When you make changes to your Exchange organization or to an individual user account, you often interact with data in Active Directory. This interaction occurs through one of two MMC snap-ins, Exchange System Manager or Active Directory Users and Computers. Figure 1.1 shows how these two tools interact with Active Directory.

**Note**
In addition to Exchange System Manager and Active Directory Users and Computers, there are other tools that are useful for Exchange administration. For more information, see Appendix A, “Tools Used with Exchange.”

![Diagram showing interaction between Exchange System Manager, Active Directory Users and Computers, and other tools like ADSI, Exchange Store (MAPI), Public Folders (WebDAV), DSAccess (WMI), and Queue (WMI).]
As shown in Figure 1.1, all of the information that you see (read) and manipulate (write) using Active Directory Users and Computers is stored in Active Directory. Most, but not all, of the information that Exchange System Manager reads and writes also comes from Active Directory. However, in addition to data in Active Directory, Exchange System Manager draws information from other sources, such as:

- **MAPI** Exchange System Manager uses MAPI to gather data from the Exchange store to display mailboxes (see Figure 1.2).

![Figure 1.2 Mailbox data gathered using MAPI and displayed in Exchange System Manager](image)

- **Windows Management Instrumentation (WMI)** Exchange System Manager uses the data supplied by WMI to display cached directory information (DSAccess, a cache of directory information that reduces the number of calls to your global catalog server) and queue information.

- **Web Distributed Authoring and Versioning (WebDAV)** Exchange System Manager uses the data supplied by WebDAV to display public folders using the Exadmin virtual directory.

  **Note**
  The location of the Exadmin virtual directory is in Internet Information Services (IIS) under the default Web site. If the default Web site service is stopped, you will not be able to display public folder information in Exchange System Manager.
Selecting the Right Management Tools

Although both Exchange System Manager and Active Directory Users and Computers provide access to Exchange-related data in Active Directory, typically you do not use them interchangeably. Generally speaking, you:

- Use Exchange System Manager for configuration data for the server and organization.
- Use Active Directory Users and Computers for recipient data.

To further highlight these usage differences, Table 1.1 provides specific examples of when you use Exchange System Manager, and when you use Active Directory Users and Computers.

**Table 1.1 Comparing Exchange System Manager and Active Directory Users and Computers**

<table>
<thead>
<tr>
<th>Use Exchange System Manager to</th>
<th>Use Active Directory Users and Computers to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage your Exchange organization.</td>
<td>Manage Active Directory objects (recipients).</td>
</tr>
<tr>
<td>Manage servers.</td>
<td>Manage users.</td>
</tr>
<tr>
<td>Move all mailboxes from one server to another server.</td>
<td>Move an individual's mailbox from one server to another server.</td>
</tr>
<tr>
<td>Create public folders.</td>
<td>Create distribution groups.</td>
</tr>
</tbody>
</table>

As Table 1.1 shows, some tasks can be performed using either Exchange System Manager or Active Directory Users and Computers. For instance, you could move mailboxes using either Exchange System Manager or Active Directory Users and Computers. The difference between the two approaches is whether you want to find all of the users on a server or only a selected subset. When you want to quickly find all of the users on a server, Exchange System Manager is the better choice. When you want to select users based on specific criteria, use Active Directory Users and Computers because this snap-in allows you to create custom LDAP filters that can filter using virtually any criteria.

**Tip**
In newsgroups or conversations with other Exchange administrators, some people refer to Exchange System Manager as ESM. Active Directory Users and Computers may be referred to as ADU&C or DSA (Directory Server Agent).

Building on the preceding overview of how Exchange System Manager and Active Directory Users and Computers work within the Exchange administration architecture, the next two sections explain Exchange System Manager and Active Directory Users and Computers in more detail. If you are already confident about using these tools, you can move ahead to the section, "Deciding Where to Manage Exchange," for information about whether to use these tools through Remote Desktop, Terminal Server, or a dedicated management station.
Working with Exchange System Manager

Exchange System Manager (Exchange System Manager.msc) is a specialized MMC console that helps you manage your Exchange organization. When you perform a typical installation of Exchange 2003 onto a server, the installation wizard automatically installs the Exchange System Management Tools onto that server as well.

Exchange System Manager provides a consistent administrative experience for administrators who deal with all facets of Exchange server management, including public folders, servers, routing, and policies.

Exchange System Manager is available on the Start menu of the Microsoft Exchange program group, as described in the following procedure.

To open Exchange System Manager

- On the Start menu, point to Programs, point to Microsoft Exchange, and then click System Manager.

Figure 1.3 shows how Exchange System Manager appears on the screen.
As shown in Figure 1.3, the left pane of Exchange System Manager is the console tree. The top node of this tree is the root organization node that contains all of the Exchange containers. Each of these containers gives you access to specific administrative features in Exchange. Table 1.2 describes what you can do with each of these containers.

Table 1.2  Exchange System Manager containers

<table>
<thead>
<tr>
<th>Container</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Settings</td>
<td>Includes features to configure system-wide settings. These settings apply to all servers and recipients in an Exchange organization.</td>
</tr>
<tr>
<td>Recipients</td>
<td>Includes features to manage objects and settings for recipients in your organization. You can manage address lists, offline address lists, recipient update services, recipient policies, mailbox management settings, details templates, and address templates.</td>
</tr>
<tr>
<td>Administrative Groups</td>
<td>Includes features to manage administrative groups. Each group is a collection of Active Directory objects that are grouped together for the purpose of permissions management. Each administrative group can contain policies, routing groups, public folder hierarchies, and servers.</td>
</tr>
<tr>
<td>Note</td>
<td>This container only appears if you have created administrative groups for your organization.</td>
</tr>
<tr>
<td>Servers</td>
<td>Holds server-specific configuration objects, such as Queues, Mailbox stores, Public Folder stores, and Protocols information.</td>
</tr>
<tr>
<td>System Policies</td>
<td>Contains policies that affect the system's configuration settings. Policies are collections of configuration settings that are applied to one or more Exchange objects in Active Directory.</td>
</tr>
<tr>
<td>Routing Groups</td>
<td>Defines the physical network topology of Exchange servers. An Exchange mail system, or organization, consists of one or more servers on which Exchange is installed. Unless you are planning a small Exchange installation, you will probably have more than one Exchange server. Within some organizations, these servers are connected by reliable, permanent connections. Groups of servers that are linked together in this way should be organized into the same routing group.</td>
</tr>
<tr>
<td>Note</td>
<td>This container only appears if you have created routing groups for your organization.</td>
</tr>
</tbody>
</table>
Container | Description
--- | ---
Folders | Displays public folder hierarchies. A public folder stores messages or information that can be shared with all designated users in your organization. Public folders can contain different types of information, from simple messages to multimedia clips and custom forms.
Tools | Contains tools that help you to monitor your Exchange organization, track messages, and recover mailboxes.

Using Exchange System Manager and its containers, you can:

- Use **Properties** of the root node to configure Exchange 2003 to display or not display routing groups and administrative groups in the console tree.
- Manage your Exchange organization by setting properties on different containers under the root node in the console tree. For example, you can delegate administrative permissions at the organization level in Exchange System Manager, or at an administrative group level using the Exchange Delegation Wizard.
- Set permissions on a specific server by modifying the permissions settings in the server's **Properties** dialog box.

To find detailed explanations of how to perform these tasks, as well as other organization-level or server-level tasks, refer to the appropriate chapter within this book.

---

**Working with Active Directory Users and Computers**

You use Active Directory Users and Computers to manage recipients. Active Directory Users and Computers is an MMC snap-in that is a standard part of Microsoft Windows Server™ operating systems. However, when you install Exchange 2003, the setup wizard automatically extends the functionality of Active Directory Users and Computers to include Exchange-specific tasks.

**Note**

If the Active Directory Users and Computers snap-in is installed on a computer that does not have Exchange or the Exchange management tools installed, you will not be able to perform Exchange tasks from that computer.

You launch Active Directory Users and Computers from either an Exchange server or from a workstation that has the Exchange System Management Tools installed.
To open Active Directory Users and Computers

1. On the Start menu, click Run.
2. In the Open box, type dsa.msc, and then click OK.

—or—

• On the Start menu, point to All Programs, point to Microsoft Exchange, and then click Active Directory Users and Computers.

Figure 1.4 shows how Active Directory Users and Computers appears on the screen.

![Active Directory Users and Computers hierarchy](image)

**Figure 1.4** Active Directory Users and Computers hierarchy

The left pane of Active Directory Users and Computers is the console tree that shows your fully qualified domain name at the root level. Click the + (plus) sign to expand the root container. Under the root container are several default containers:

- **Builtin** Container for built-in user accounts.
- **Computers** Default container for computer objects.
• **Domain Controllers**  Default container for domain controllers.

• **ForeignSecurityPrincipals**  Container for security principals from trusted external domains. Administrators should not manually alter the contents of this container.

• **Users**  Default container for user objects.

In addition to the default containers, you can organize directory objects into logical units by creating containers called organizational units. For example, you could create an organizational unit for your marketing group that holds all of the directory objects associated with your company's marketing department. Organizational units are useful for applying group policy and for organizing objects in a meaningful way. For more information about organizational units, see the Windows documentation.

After you have organized the containers within Active Directory Users and Computers, you can then use those containers to:

• Create recipients.

• Perform Exchange-specific tasks.

• Manage multiple Exchange domains.

### Creating Recipients

After Exchange has extended Active Directory Users and Computers, you can mail-enable or mailbox-enable an object, and thereby turn the Active Directory object into a recipient. However, not all objects can be mail-enabled or mailbox-enabled. For example, you can create a mailbox for a user object or a mail-enabled group object, but you cannot do either for a computer object. Thus, the Active Directory objects that are of most interest to you as an Exchange administrator are:

• Users

• InetOrgPerson objects

• Contacts

• Groups

• Query-based distribution groups

For more information about creating recipients, see Chapter 4, "Managing Recipients and Recipient Policies."
Performing Exchange Tasks

In Active Directory Users and Computers, you can select a user or a group object, and then use the Exchange Task Wizard to perform a variety of tasks that are specific to that object. These tasks depend on the type of object that you select and its current attributes. For example, the Exchange Task Wizard will not allow you to create a mailbox for a contact because contacts can only be mail-enabled, not mailbox-enabled. Likewise, selecting a user who already has a mailbox means that the Exchange Task Wizard allows you to delete the user's mailbox, but not to create another mailbox.

Here is the complete list of Exchange-specific tasks that Exchange Task Wizard can perform:

- Creation of mailboxes
- Moving of mailboxes
- Deletion of mailboxes
- Designation of an e-mail address
- Configuring of Exchange features
- Removing Exchange attributes
- Deleting e-mail addresses
- Hiding group membership
- Associating external accounts

To use Exchange Task Wizard to perform one of these tasks, use the following procedure.

To perform an Exchange-specific task

- In Active Directory Users and Computers, right-click a user or group object, and then click Exchange Tasks.
Managing Exchange in Multiple Domains

You can use Active Directory Users and Computers to manage Exchange in more than one domain in a forest. To do this, you need to connect to the desired domain using the following procedure.

To manage Exchange in a another domain

- In Active Directory Users and Computers, right-click the root object in the console tree, and then select **Connect to Domain**.

Note

You must have the appropriate permissions for the target domain.

Deciding Where to Manage Exchange

Knowing the basics of how to use Exchange System Manager and Active Directory Users and Computers is just the beginning of managing Exchange 2003. The next step is to decide where is the best location from which to use these tools within your Exchange environment.

During a typical installation of an Exchange 2003 server, the setup wizard installs Exchange System Manager and extends Active Directory Users and Computers directly on the server. To use these tools, you log on to the server itself. However, it is advisable to limit direct interaction with the server to avoid exposure to unwanted practices. For example, it may be necessary to directly log on to a server to move log files, but in doing so, you may accidentally delete system files or inadvertently introduce viruses.

To minimize directly logging on to the server, you can use Remote Desktop, Terminal Server, or a dedicated management station. Table 1.3 outlines some of the inherent advantages and disadvantages of these various approaches to Exchange management.
Table 1.3  Administration scenarios

<table>
<thead>
<tr>
<th>Management scenario</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging directly on to the server</td>
<td>• No extra setup required.</td>
<td>• Increased risk. Administrators can inadvertently delete files or introduce viruses.</td>
</tr>
<tr>
<td>(Console session)</td>
<td>• No extra hardware required.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using Remote Desktop or Terminal Server</td>
<td>• No extra setup required.</td>
<td>• Increased risk. Administrators can inadvertently delete files or introduce viruses.</td>
</tr>
<tr>
<td></td>
<td>• Can manage from outside of the data center.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Administrators can perform most tasks without leaving their desks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Number of remote connections is limited to the number of Terminal Server licenses purchased.</td>
</tr>
<tr>
<td>Using a dedicated management station</td>
<td>• Decreased risk.</td>
<td>• Extra setup required.</td>
</tr>
<tr>
<td></td>
<td>• Can place management station in convenient location.</td>
<td>• Extra hardware required.</td>
</tr>
</tbody>
</table>

Of the three approaches listed in Table 1.3, the only approach that is discussed further in this chapter is the dedicated management station. Directly logging on to the server requires no special setup. If you decide to use Remote Desktop or Terminal Server, the best source for setup information is the documentation that came with your copy of Windows.

**Setting Up a Management Station**

By installing Exchange System Manager and Active Directory Users and Computers on a dedicated management workstation, you can avoid some of the risks outlined in Table 1.3. The following checklist briefly lists the steps to set up a management station.

**Management Station Setup Checklist**

- Install Microsoft Windows XP Professional with Service Pack 1 (or later) on the workstation.
- Join the workstation to the domain with Exchange.
- Install the Windows Administrative Tools Pack on the workstation.
- Install the Simple Mail Transfer Protocol (SMTP) service on the workstation.
- Install the Exchange System Management Tools on the workstation.
- Shut down the SMTP service on the workstation.
For more information about installing Windows XP and adding the workstation to the domain, see your Windows documentation. For the remaining steps in the checklist, use the following procedures.

**Note**
To manage Exchange, the workstation must be joined to the same forest as your Exchange servers. You cannot manage domains in another forest.

### Installing the Windows Administrative Tools Pack

After you have installed Windows XP with Service Pack 1 onto the workstation, you need to install the Windows Administrative Tools Pack. Installing this tools pack enables you to use the workstation to remotely manage servers running Windows.

**To install the Windows Administrative Tools Pack**


### Installing the SMTP Service

After installing the Windows Administrative Tools Pack, you need to install the SMTP service on the workstation. Installing the SMTP service allows you to install the Exchange System Management Tools.

**To install the SMTP service**

1. On the dedicated management workstation, open **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. Select **Internet Information Services (IIS)**, and then click **Details**.
3. Select the **SMTP Service component** check box.
4. Click **OK**, click **Next**, and then click **Finish**.
Installing the Exchange System Management Tools

After completing the previous steps, you are ready to run Exchange setup.

To install the Exchange System Management Tools

1. On the dedicated management workstation, insert the Exchange 2003 Setup compact disc into the workstation’s CD drive, and then navigate to <drive>: \setup\i386\setup.exe.

2. On the Component Selection page, do the following:
   - Under Component Name, locate Microsoft Exchange. In the corresponding Action column, select Custom.
   - Under Component Name, locate Microsoft Exchange System Management Tools. In the corresponding Action column, select Install (see Figure 1.5).

3. Click Next, and continue with the wizard.
Shutting Down the SMTP Service

After installing the Exchange System Management Tools, you should disable the SMTP service because you only need this service to install the Exchange System Management Tools. In general, it is a good security practice to shut down any unneeded services.

Using Custom Consoles

MMC provides a framework for management tools (that is, snap-ins). Although MMC is not a tool itself, snap-in tools cannot be run independent of it. Opening a snap-in from the command prompt or the Start menu automatically results in the snap-in opening into its own MMC window.

As an alternative to opening an MMC snap-in in its own window, you can create a custom console. This custom console is a single instance of MMC that houses all of the snap-in tools that you use regularly. As an Exchange administrator, you may want to create a custom console that consolidates Exchange System Manager and Active Directory Users and Computers. For example, Figure 1.6 shows a custom console that houses Exchange System Manager, Active Directory Users and Computers, and Event Viewer.

Note
You can use a custom console regardless of where you decide to manage Exchange—by directly logging onto the server, by using Remote Desktop or Terminal Server, or by using a dedicated management workstation.
As shown in Figure 1.6, the user interface (UI) of a custom console is the same as that of the individual snap-ins. In the left pane is the console tree, which shows a hierarchical view of the different containers of the various snap-ins. On the right is the details pane, where you can manage the different objects in the containers by right-clicking an object and selecting an appropriate command for that object.
Creating Custom Consoles

In addition to creating a custom console to help you manage Exchange, you can create custom consoles for different administrators or different tasks.

To create a custom MMC console, there are two steps. First, you create a new instance of MMC, and then you add the desired snap-ins to that instance.

To create a new instance of MMC

1. On the Start menu, click Run.
2. In the Open box, type MMC, and then click OK.

This opens a blank MMC window (see Figure 1.7). The next step is to add the snap-ins that you want to use.

Figure 1.7  A new instance of MMC
To add snap-ins to MMC

1. In MMC, on the File menu, click Add/Remove Snap-in.
2. Click Add to open the Add Standalone Snap-in window.
3. Select the snap-in that you want to add from the list, and then click Add.
   For example, you can select Active Directory Users and Computers or Exchange System Manager.
4. Repeat Step 3 until you have added the desired snap-ins.
5. Click Close, and then click OK.

Automating Administrative Tasks

In addition to Exchange System Manager, Active Directory Users and Computers, and the other tools described in this book, Exchange Server 2003 provides technologies for accomplishing most administrative tasks programmatically. These technologies include Collaboration Data Objects for Exchange (CDOEX), CDO for Exchange Management (CDOEXM), and a large set of WMI providers.

The Exchange SDK contains complete information about writing applications to manage, control, and extend Exchange, including numerous reusable code samples. You can download the Exchange SDK, or view it online from the Exchange developer center (http://msdn.microsoft.com/exchange).
When you install Exchange, you can join an existing organization or create a new organization, if one does not already exist. An Exchange organization defines your messaging environment. An organization includes all of the Exchange servers, domain controllers, global catalog servers, users, and other Microsoft® Active Directory® directory service objects that function together as a single entity. Exchange organizations can include multiple Active Directory domains, but they cannot span multiple Active Directory forests.

**Note**

You cannot change the organization name after it is created.

The configuration settings that you apply to an Exchange organization have the potential to affect all components within the organization. This chapter explains the basic administrative tasks that you use to manage your Exchange organization. Use this chapter to understand what it means to promote an Exchange organization to native mode, how to apply global settings to control message formatting and Simple Mail Transfer Protocol (SMTP) message filtering, how to manage your organization and servers using administrative groups and system policies, and how permissions and standardized security roles work in Exchange.
Promoting an Exchange Organization from Mixed Mode to Native Mode

Microsoft Exchange Server 2003 and Exchange 2000 Server both take advantage of Active Directory, and therefore coexist in what is called a native mode organization. However, Exchange Server version 5.5 (and earlier) does not rely on Active Directory. This difference means that, when servers running either Exchange 2003 or Exchange 2000 coexist with servers running Exchange 5.5 (or earlier), the organization must run in what is called mixed mode. Some newer features and functionality in Exchange are unavailable when running in mixed mode. For example, routing groups function differently in mixed and native modes.

Note
For more information about routing groups, see Chapter 5, "Understanding and Configuring Message Routing and Transport."

By default, a new Exchange 2003 organization runs in mixed mode until it is promoted to native mode. You can only promote an Exchange organization to native mode if there are no servers running Exchange 5.5 (or earlier), and if no instances of Site Replication Service (SRS) are running. Ensure that you have properly upgraded all servers and any connectors before you switch to native mode. After you switch an organization to native mode, it can never return to mixed mode. This means you cannot add an Exchange 5.5 server to a native mode topology.
To switch from mixed mode to native mode

1. In Exchange System Manager, right-click your Exchange organization, and then click Properties.

2. On the General tab (see Figure 2.1), click Change Mode.

![Figure 2.1 Change Mode option on the General tab](http://www.microsoft.com/exchange/library)

Applying Global Settings

Using global settings, you can configure system-wide settings in your Exchange organization. These settings can apply to all servers and recipients in an Exchange organization.

This section focuses on using global settings to configure the following:

- How SMTP converts MAPI messages to Multipurpose Internet Mail Extensions (MIME).
- How policies for SMTP domains control the formatting of messages that are destined for a domain and the types of automatic responses that can be sent to the domains.
- How Exchange delivers messages organization-wide.

Global settings are also available for Exchange ActiveSync® and Microsoft Outlook® Mobile Access. For more information about Mobile Services and Outlook Mobile Access, see Chapter 6, "Managing Client Access to Exchange."

Associating File Name Extensions with MIME

Internet message formats are used when messages are sent to or received from an Internet client. When a user sends mail from a MAPI client, such as Microsoft Outlook®, to an Internet client, such as Outlook Express, SMTP converts the message from Microsoft rich text format (RTF) to MIME. The file name extensions that you define for each MIME type enable clients to recognize mail attachments and open them. By default, several content types are associated with file name extensions. Generally, the default associations are sufficient for content conversion.
To manage associations for file name extensions

1. In Exchange System Manager, expand **Global Settings**, right-click **Internet Message Formats**, and then click **Properties**.

2. On the **General** tab (see Figure 2.2), use the following options:
   - To associate a new file name extension with a MIME type, click **Add**.
   - To prioritize the associated extension that Exchange uses with each MIME type, click **Move Up** to move the extension up the list or **Move Down** to move the extension down the list. If two associated extensions exist for a single MIME type, Exchange uses the extension that appears higher on the list.

![Figure 2.2 List of MIME content types on the General tab](image-url)
Using SMTP Policies to Control Outbound Mail Formatting and Automatic Responses

You can use Internet message formats to define SMTP policies that control the format of messages that are sent to the Internet, or to specific external SMTP domains. These policies also control what types of automatic responses, such as out-of-office notifications, can be sent to Internet domains from users in your organization.

For each domain that is defined in Internet Message Formats, you can set the following properties:

- Message formatting options that determine how messages sent to this domain are encoded, and which language character set is used to display these messages.
- Advanced options that determine when messages are sent in Exchange RTF, how text is formatted, and what types of automatic responses, such as non-delivery reports (NDRs) or out-of-office notifications, are sent to this domain.

Important
Do not send mail exclusively in RTF because many non-Microsoft mail servers cannot read rich-text messages. Servers that cannot read rich-text messages provide their users with e-mail messages that include a Winmail.dat file attachment. To avoid this problem, ensure that your message settings do not use Exchange RTF exclusively.

The following sections explain the default policy, and how to create new policies for specific domains.
Understanding the Default Policy

By default, an SMTP policy exists for the domain *, which encompasses all messages that are destined for the Internet. All messages that Exchange sends to the Internet use the settings on this policy. You can view this policy in the details pane when you select Internet Message Formats in Exchange System Manager, as shown in Figure 2.3.

Figure 2.3 Default SMTP policy for all Internet domains

A policy must exist for the * domain. This policy controls how messages are sent to all external domains. If necessary, you can modify the properties on this policy.

Creating a Policy for a New SMTP Domain

In addition to modifying the policy for the * domain, you can create other policies for specific SMTP domains. For example, you want to communicate with a business partner who has an SMTP domain named contoso.com, and you want to allow out-of-office replies to be sent to this domain, but not to other external domains. You can create a new policy for the contoso.com domain that does exactly that. Because Exchange uses the SMTP policy that most closely matches the SMTP domain, all messages sent to Contoso users use the policy for the Contoso domain, but messages sent to any other SMTP domain use the default policy for the * domain.
To create a new policy

1. In Exchange System Manager, expand Global Settings, right-click Internet Message Formats, point to New, and then click Domain.

2. On the General tab (see Figure 2.4), enter a policy name and the SMTP domain.

![Figure 2.4 Entering a policy name and an associated SMTP domain](image)

Setting Message Formatting Options for a Policy

You can control how Exchange formats the messages that are sent to the domain or domains on a particular policy. You can have Exchange format these messages in either MIME or uuencode, so that non-MAPI clients can read these messages. Additionally, you can specify the character set that Exchange uses for outgoing messages. By default, all messages use the Western European (ISO-8859-1) character set.
To set the message formats for a policy

1. In Exchange System Manager, right-click the policy, and then click **Properties**.
2. On the **Message Format** tab (see Figure 2.5), select the message encoding and character sets that you want to use with this policy.

![Figure 2.5 Message Format tab for the Contoso policy](image)

**Controlling Automatic Replies and Advanced Formatting for a Policy**

Beyond specifying the message encoding and character sets to be used with a policy, you can also specify the following options:

- When the policy uses Exchange rich-text format.
- Whether messages sent using the policy allow message text wordwrapping.
- What types of auto-responses can be sent to users in the domain or domains on the policy. For security purposes, you can prevent automatic responses to external domains. For example, you may want to prevent out-of-office responses.
To set advanced properties for a policy

1. In Exchange System Manager, right-click the policy, and then click Properties.
2. On the Advanced tab (see Figure 2.6), select the appropriate options.

Note
As stated earlier, do not select Always use under Exchange rich-text format, unless you are configuring a policy for a domain whose users always use MAPI clients.

Figure 2.6 Advanced tab for the Contoso policy

Selecting Message Delivery and Message Filtering Options

You can use the Message Delivery Properties dialog box to configure the following message delivery options:

- Default message delivery options, including message size restrictions for sending and receiving messages, and the maximum number of recipients that a message can have.
- SMTP message filtering to control unsolicited commercial e-mail (also known as spam), using sender, connection, and recipient filtering.
To access the Message Delivery Properties dialog box
- In Exchange System Manager, expand Global Settings, right-click Message Delivery, and then click Properties.

Configuring Default Message Size and Recipient Limits

The Defaults tab in the Message Delivery Properties dialog box (see Figure 2.7) is where you configure the default restrictions for the following message delivery options:

- **The maximum message size that can be sent by users** This is the Sending message size option, and it defaults to No limit (users can send a message of any size). Based on your available network bandwidth and your user requirements, you may want to limit the maximum message size that is allowed in your organization. If a user attempts to send a message that exceeds the specified size limit, the user receives a non-delivery report (NDR) and Exchange will not send the message.

- **The maximum message size that can be received by users** This is the Receiving message size option, and it defaults to No limit (users can receive a message of any size). Again, based on network bandwidth and user requirements, you may want to limit the message size. Senders within your organization receive an NDR if they attempt to send a message to a user that exceeds the specified size limit. Depending on the NDR settings that you configure in Internet Message Formats, external senders may or may not receive an NDR.

  **Note**
  For more information about Internet Message Formats, see “Using SMTP Policies to Control Outbound Mail Formatting and Automatic Responses” earlier in this chapter.

- **The maximum number of recipients to which a single message can be sent** This is the Recipient limits option, and it defaults to 5000 recipients. Recipients include all users on the To, Cc, and Bcc lines, as well as expanded distribution lists. Select No limit to allow users to send and receive messages regardless of how many recipients to which the messages are addressed.

Exchange applies the settings for these options globally to all users. However, you can override these settings on a per-user basis in Active Directory Users and Computers. For information about how to override these settings, see Chapter 4, "Managing Recipients and Recipient Policies."
To change the default message delivery options

- In the **Message Delivery Properties** dialog box, on the **Defaults** tab (see Figure 2.7), select the appropriate options.

![Figure 2.7 Defaults tab in the Message Delivery Properties dialog box](image)

**Configuring SMTP Message Filters**

Although you configure SMTP message filtering options in the **Message Delivery Properties** dialog box, you must enable the filtering options on the individual SMTP virtual servers where you want to apply the filtering. Exchange applies these filters during the SMTP session when a remote SMTP server connects to the SMTP virtual server.

In Exchange 2003, you can configure sender filtering, connection filtering, and recipient filtering. Enabling filtering on an SMTP virtual server results in the virtual server checking the enabled filters when another SMTP server attempts to send mail into the organization.

**Note**

Exchange applies SMTP message filters only to messages sent from external SMTP servers. Exchange does not apply SMTP message filters when servers send messages between themselves within an Exchange organization. This is because Exchange servers automatically authenticate with each other and filter only mail that is submitted anonymously.
Configuring Sender Filtering

Sender filtering allows you to block messages sent by specific senders. This is useful if you receive unsolicited commercial e-mail from particular domains or sender addresses. You can block these messages by enabling sender filtering.

To enable sender filtering

1. On the **Sender Filtering** tab of the **Message Delivery Properties** dialog box (see Figure 2.8), click **Add** to add the SMTP address of a user or a particular domain from whom you want to block messages.

You can block an individual sender, an entire domain, or a display name (by entering the display name in quotes).

![Figure 2.8 Sender Filtering tab in the Message Delivery Properties dialog box](image)

2. To have Exchange save any messages that sender filtering blocks to an archive folder (instead of automatically deleting these filtered messages), select **Archive filtered messages**.

The archive folder is in the `<drive>:` \Program Files\Exchsrvr\Mailroot\vsi \archive folder, where `n` is the virtual server instance of the SMTP virtual server where sender filtering is enabled.
3. To block messages with a blank sender address (a technique that some senders of unsolicited commercial e-mail messages use), select **Filter messages with blank sender**.

4. To end the SMTP session when a sender matches an address on the sender filter, select **Drop connection if address matches filter**.

5. To accept messages from senders on the block list without sending notification to the sender that mail was not delivered, select **Accept messages without notifying sender of filtering**.

---

**Configuring Connection Filtering**

Connection filtering blocks messages based on the Internet Protocol (IP) address of the connecting SMTP server. With regard to connection filtering, you can configure connection filtering rules, configure exceptions, and configure global accept and deny lists.

**Note**


---

**Configuring Connection Filtering Rules**

You can subscribe to a third-party block list provider and configure a connection filtering rule that checks against the provider's list of specific IP addresses.

**Note**

Specific configuration of connection filtering rules is dependent upon the block list provider.
To configure a connection filtering rule

- On the **Connection Filtering** tab (see Figure 2.9) of the **Message Delivery Properties** dialog box, under **Block List Service Configuration**, click **Add**.

![Message Delivery Properties dialog box](image)

**Figure 2.9** Connection Filtering tab in the Message Delivery Properties dialog box

**Configuring Exceptions**

You can specify whether specific SMTP addresses within your organization are allowed to receive messages from blocked IP addresses. For example, a connection filtering rule blocks a legitimate organization from sending mail to your organization. By entering your postmaster address as an exception to this connection filtering rule, an administrator from the legitimate organization can send an e-mail message to the postmaster in your organization to find out why his or her organization is blocked from sending mail.

**To create a list of exceptions to connection filtering rules**

- On the **Connection Filtering** tab (see Figure 2.9) of the **Message Delivery Properties** dialog box, click **Exception**.
Configuring Global Accept and Deny Lists
If there are IP addresses from which you either always want to accept mail or reject mail, you can configure a global accept or deny list.

Global accept list
This list contains all of the IP addresses from which you always want to accept mail. Exchange checks this list before checking any other filters. If the connecting server's IP address appears on the global accept list, Exchange automatically accepts the mail and does not check any additional filters.

Global deny list
This list contains all of the IP addresses from which you always want to reject mail. Exchange checks this list immediately after checking the global accept list. If an IP address appears on the global deny list, Exchange automatically rejects the mail and does not check any additional filters.

To create either a global accept or deny list
- On the Connection Filtering tab (see Figure 2.9) of the Message Delivery Properties dialog box, click Accept to add an IP address to the global accept list or click Deny to add an IP address to the global deny list.

Configuring Recipient Filtering
Exchange 2003 also supports recipient filtering, so you can filter e-mail messages that are addressed to users who are not in Active Directory, or e-mail messages that are addressed to recipients who are commonly targeted by distributors of unsolicited commercial e-mail messages.

You can use recipient filtering to filter messages that a sender sends to any e-mail address, valid or invalid, within your organization. If a message is sent to any of the specified recipients, Exchange returns a 500-level error during the SMTP session.

By default, Exchange accepts mail addressed to any recipient (invalid or valid), and then Exchange sends NDRs for all invalid recipients. Usually, unsolicited commercial e-mail is sent from invalid addresses, so Exchange retries delivery of NDRs to non-existent senders and thereby wastes more resources. Enabling recipient filtering prevents Exchange from wasting resources in this way because you can filter e-mail that is sent to invalid recipients.
You can use recipient filtering to reject mail that a sender sends to invalid recipients (recipients that do not exist in Active Directory). However, doing so potentially allows malicious senders to discover valid e-mail addresses. The SMTP virtual server issues different responses for valid and invalid recipients. By comparing the responses issued by the SMTP virtual server for valid and invalid recipients, malicious users can identify valid e-mail addresses in your organization.

**Note**
Recipient filtering rules apply only to anonymous connections. Authenticated users and Exchange servers bypass these validations.


To add a recipient to the recipient filtering list

- On the **Recipient Filtering** tab (see Figure 2.10) of the **Message Delivery Properties** dialog box, click **Add**.

![Recipient Filtering tab in the Message Delivery Properties dialog box](image)

**Figure 2.10** Recipient Filtering tab in the Message Delivery Properties dialog box
Creating and Managing Administrative Groups

In Exchange 5.5 (and earlier), a site defined both the administrative boundary and the physical routing topology for a group of servers. Exchange 2000 (and later) split the concept of a site into physical and logical components, as follows:

- Routing groups define the physical network topology of your Exchange servers.
- Administrative groups define a logical grouping of servers and other objects for the purpose of administration.

For more information about routing groups, see Chapter 5, "Understanding and Configuring Message Routing and Transport." This section focuses solely on administrative groups.

An administrative group can contain any of the following Exchange objects:

- Servers
- Policies
- Routing groups
- Public folder trees

Administrative groups allow you to delegate specific administrative permissions, and define system policies for the administrative groups and the objects within the group. You can create system policies that control the administration of servers, mailbox stores, and public folder stores within an administrative group. Permissions and system policies are discussed in more detail later in this chapter.
The remainder of this section focuses on the following topics:

- Understanding the types of administrative models
- Displaying administrative groups
- Creating administrative groups
- Creating a system policy
- Moving objects between administrative groups
- Deleting administrative groups

**Note**
You should use the Exchange Administration Delegation Wizard to assign a specific group permission to manage an administrative group. For more information about the Exchange Administration Delegation Wizard, see "Managing Permissions" later in this chapter.

---

**Understanding the Types of Administrative Models**

Because administrative groups are logical, you can create administrative groups based on locations, departments, or functions. For example, a global company with branches in different countries could create administrative groups to delegate functional tasks. In a native-mode organization, you could create a single administrative group that contains servers only and use this specialized server administration group to create policies for all of the servers in your organization. You could then create another administrative group solely for the purpose of public folder administration, and then have a specialized team administer all public folders trees using this administrative group.

However, before creating these various functional administrative groups, you should understand your organization's administrative model, as dictated by your organizational structure and your security policy. When you understand your organization's administrative model, you can then implement administrative groups to accurately reflect this model.
This section presents the types of administrative models, and how these models affect your implementation of administrative groups. The administrative models discussed in this section are:

- Decentralized administrative model
- Centralized administrative model
- Mixed administrative model

To illustrate these administrative models, the following sections show how to apply each of these models to a fictitious company called Contoso, Ltd. This fictitious company has global branches in North America, Europe, and Asia, as shown in Figure 2.11.

![Figure 2.11  Branches in Contoso, Ltd](image)

**Note**

In a mixed-mode organization, each site becomes a single administrative group, and you cannot use the administrative models discussed in this section.
Using a Decentralized Administrative Model

In a decentralized administrative model, complete control over management of the Exchange system is distributed among the company's geographical regions or divisions. In this type of model, each region or division controls its own assets and performs its own system administration.

This type of organization probably has at least one administrative group in each division or group. Each location has its own team of Exchange administrators, who have full administrative control over objects within its administrative group.

Many companies implement a decentralized model to enable each company branch to function autonomously. For example, Contoso's global branches in the United States, Europe, and Asia each have control over an administrative group, a routing group, policies, servers, public folder trees, and other objects that are specific to that branch (see Figure 2.12).

Figure 2.12  Decentralized administrative model
Using a Centralized Administrative Model

In a centralized model, one or a few controlled administrative groups maintain complete control of the Exchange system. For example, Figure 2.13 shows how Contoso's administrative group in Seattle has complete control over the Exchange system of the company.

![Contoso, Ltd Exchange Organization](contoso.png)

**Figure 2.13 Centralized administrative model**

This administrative model is similar to a data center where all administration tasks are performed by a single information technology group. This administrative model is typical in small-sized or medium-sized organizations, but can also be used in larger organizations that have high-bandwidth connectivity to all regional offices.

Using a Mixed Administrative Model

In a mixed model, administrative groups reflect both functional and geographic distribution. You create specialized administrative groups to restrict the management of certain functions to specific people, and create other groups to delegate administration along geographical lines. To illustrate this type of model, here are some sample administrative groups that you might want to create:

- To restrict who can create and maintain policies, you can create an administrative group solely for the purpose of managing policies, which is a functional task.
- To manage public folders in a specific region, you can create an administrative group solely for the purpose of managing a region's public folders, which is a geographical consideration.
You typically use the mixed administrative model in larger organizations that have many divisions or offices in many geographical locations. The mixed model can also apply when one company acquires another company.

Figure 2.14 shows how Contoso applies a mixed administrative model to its organization. To centrally administer public folders and policies, Contoso created one central administrative group for administering public folders and another for administering policies. The remaining administrative groups are regional and allow regional control of other functions, such as routing groups.

![Contoso, Ltd Exchange Organization](image)

**Figure 2.14 Mixed administrative model**
Displaying Administrative Groups

After installing Exchange in an Exchange 2003 or Exchange 2000 organization, Exchange System Manager does not automatically display administrative groups and routing groups. You must configure your Exchange organization to display administrative groups. After you have configured this setting, you can view the Administrative Groups container and create additional administrative groups for your organization.

Note
If you install Exchange 2000 (or later) in an Exchange 5.5 site, Exchange enables administrative and routing groups by default. In this case, every Exchange 5.5 site appears as an administrative group.

To display administrative groups

1. In Exchange System Manager, right-click your Exchange organization, and then click Properties.

2. On the General tab (see Figure 2.15), select Display Administrative groups.

3. Restart Exchange System Manager for the changes to apply.
Creating Administrative Groups

In the default configuration of an Exchange organization, only one administrative group exists. You can either install all servers into this single administrative group, which is useful in a centralized administrative model, or you can create additional administrative groups and install servers into the appropriate administrative groups, based on your administrative model.

By default, Exchange installs all servers into the **First Administrative Group** in the Server container. You can rename **First Administrative Group**, and add new system containers, but you cannot remove servers from the Server container in this group.

**Note**
In a mixed-mode organization, each Exchange 5.5 site becomes its own administrative group, and the administrative group name matches the site name.

You can add servers to an administrative group only during installation. Ideally, you should create the necessary administrative groups on the first Exchange server in your organization, and then install additional servers into the appropriate administrative groups. You can never move servers between administrative groups.

To create a new administrative group

- In Exchange System Manager, right-click **Administrative Groups**, point to **New**, and then click **Administrative Group**.

Moving Objects Between Administrative Groups

You can move some of the objects in an administrative group to a different group. However, there are other objects that cannot be moved.

Objects that you can move between administrative groups are as follows:

- System policies
- Public folders
- Routing group member servers (native mode only)

Objects that you cannot move between administrative groups are as follows:

- Servers
- Containers

You can move objects only between containers of the same type. For example, you can move a system policy from one system policy container to another system policy container in a different administrative group, but you cannot move a system policy into a public folder container. This type of action is blocked by default.
To move system policies or public folders between administrative groups

- Cut the system policy or public folder from the source container, and paste it into the target container.
- Drag the system policy or public folder from the source container to the target container.

**Note**
When you are moving or copying objects between administrative groups, click Refresh to see the object in the new container.

Deleting Administrative Groups

You can delete only administrative groups that contain no objects. After you have removed all of the objects within an administrative group, you can delete it.

**To delete an administrative group**

- In Exchange System Manager, expand Administrative Groups, right-click the administrative group that you want to delete, and then click Delete.

Using System Policies

A system policy is a collection of configuration settings that you apply to one or more servers, mailbox stores, or public folder stores. For example, to enable message tracking across multiple servers, you can define a single policy, rather than performing the lengthy task of setting individual policies to enable message tracking on each server. After defining and implementing the policies, you can change the configuration of all of the servers within the organization by editing the policies and applying the changes.

The system policies that you create for an administrative group typically apply to objects within that group. However, a system policy can apply to objects outside of its own administrative group. For example, you can implement consistent message tracking options for all servers by creating a server policy in a central administrative group and applying it to all servers in your organization.
Policies appear in the **System Policies** container under an administrative group (see Figure 2.16).

![System Policies container](image)

**Figure 2.16 System Policies container**

There are three types of system policies:

- **Public folder store policies**  Allow you to configure settings across public folder stores.
- **Mailbox store policies**  Allow you to configure settings across mailbox stores.
- **Server policies**  Allow you to enable message tracking options on servers.

Of the three types of system policies, this section discusses only server policies in more detail. For information about configuring public folder store policies or mailbox store policies, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores."
Understanding How System Policies Affect Individual Settings

System policies use an *apply-time* implementation to affect configuration changes. You can create a policy, define settings for that policy, associate that policy with one or more servers or public folder stores, and then apply the policy. After you apply the policy, the corresponding settings that are specific to that individual object become unavailable and appear dimmed. This is because the policy, not the individual object, now controls those settings. For example, if you create a policy that enables message tracking and apply the policy to an Exchange server, the message tracking options for the server are unavailable (see Figure 2.17). This configuration enables administrators to prevent further changes from being made to settings on individual objects that a policy controls.

![Figure 2.17 Message tracking options disabled on a server](image-url)
Creating a Server Policy

You use a server policy for message tracking and maintenance settings for message tracking log files. When you enable message tracking to track messages, Exchange stores messages in the message tracking log file. By enabling subject logging and display, you store message subjects in Message Tracking Center, through which you can view the messages. Message tracking and subject logging are explained in more detail in Chapter 3, "Configuring Exchange Server Settings."

Before you can create a server policy (or, for that matter, any other system policy) within an administrative group, you must add a system policy container. After you have created the system policy container, you can then create a server policy.

To create a system policy container

- In Exchange System Manager, expand Administrative Groups, right-click the administrative group, point to New, and then click System Policy Container.

To create a server policy

1. In Exchange System Manager, expand Administrative Groups, expand the appropriate administrative group, right-click System Policies, point to New, and then click Server policy.

2. On the General (Policy) tab (see Figure 2.18), select the following options:
   - To log the message subject and make this subject visible when messages are tracked, select Enable subject logging and display.
   - To track all messages that flow to and from the server, select Enable message tracking.
Handling Policy Conflicts

If you create a new policy that conflicts with settings in an existing policy, Exchange displays a dialog box that notifies you of the conflict. By default, the newer policy replaces an older policy. For example, you create a server policy with specified configurations, and you want to add the policy to a particular server. However, if the server is already under the control of another policy, a dialog box prompts you to verify whether you want to remove the server from the control of the other policy. You can choose to remove the server from the control of the previous policy, or apply the new policy you just created. If you do not resolve the policy conflict, the following message appears:

The objectname (for example, Server1) could not be associated with policy policymame (ServerPolicy) because you refused to remove the object from the control of conflicting policies.
Adding Servers to a Server Policy

After you create a server policy, you need to add servers to the policy.

To add servers to a server policy

1. In Exchange System Manager, expand Administrative Groups, expand the administrative group that contains the server policy to which you want to add servers, expand System Policies, right-click the server policy, and then click Add server.

2. In the Select the items to place under the control of this policy dialog box (see Figure 2.19), type the server name, and then click OK.

![Select the items to place under the control of this policy dialog box](image)

**Figure 2.19** Selecting items for a server policy

**Note**

Figure 2.19 shows the dialog box that appears when you run Exchange 2003 on Microsoft Windows Server™ 2003. If you run Exchange on Windows® 2000 Server, this dialog box offers the same functionality but appears slightly different.

Viewing the Objects Controlled by a System Policy

Using Exchange System Manager, you can view either the objects that the system policy controls or the policies that Exchange applies to an object:

- To view the objects that a policy controls, click a policy in the System Policies container. The objects appear in the details pane under Policy Applied To.
- To view the policies that Exchange applies to a particular object, click the Policies tab in the server's Properties dialog box.
Copying System Policies Between Administrative Groups

In Exchange 2003, policies can be copied or moved between policy containers that are in different administrative groups. Copying policies allows you to delegate administrative control while maintaining consistent or similar settings in policies across various administrative groups. For example, you could create the server policy once, and then copy it to the system policy container in each of the other desired administrative groups. Then, the administrator of each individual administrative group could customize policies (from this template) to manage objects that are associated with his or her administrative group.

**Note**
Remember that you can copy only individual policies between administrative groups. You cannot copy the system policy container from one administrative group to another.

**To copy policy objects between administrative groups**

1. In Exchange System Manager, right-click the policy, click **Copy**, and then paste the policy in your target container.
2. Right-click the target container, and then click **Refresh** to view the policy in the container. After you copy a policy, you need to apply it to the individual servers, mailbox stores, or public folder stores in the administrative group where you copied the policy.
Modifying or Removing a Policy

You can modify a policy that is applied to one or more objects to change the properties on all of the objects.

To modify a policy

1. In Exchange System Manager, right-click the policy that you want to modify, click Properties, and then use the tabs to modify the policy.
2. After you have made the necessary modifications, right-click the policy, and then click Apply now to apply the changes.

To change the properties on all of the objects individually, you can also remove an object from the control of a policy or delete the policy itself.

To remove an object from the control of a policy

1. In Exchange System Manager, expand System Policies, and then click the appropriate system policy.
2. In the Policy Applied To column, right-click the object, point to All Tasks, and then click Remove from policy.

To delete a policy

- In Exchange System Manager, right-click the policy that you want to delete, and then click Delete.

After a policy has been applied, settings associated with that policy remain intact on associated objects, even after an object has been removed from policy control or a policy itself has been deleted. If you want to change the settings that a policy applies, you must change them on the individual server, mailbox store, or public folder store.
Managing Permissions

As you manage your Exchange organization, some of your most important security tasks will involve permissions. The correct management of permissions in Exchange 2003 ensures that users and administrators can successfully complete those tasks that they need to perform, while preventing users and administrators from intentionally or inadvertently performing inappropriate tasks.

In Exchange 2003, there are three sets of permissions that you can manage:

- Permissions for Exchange objects. These settings are stored in Active Directory and the Microsoft Internet Information Services (IIS) metabase.
- Store permissions.
- File permissions on NTFS volumes.

Together, these permissions provide the means to implement security on all elements in an Exchange 2003 installation.

This section focuses on using Exchange System Manager to manage permissions on Exchange objects in Active Directory and the IIS metabase. For detailed information about managing store permissions, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores." For detailed information about understanding and managing NTFS permissions, see the Windows documentation and resource kits.

**Important**

You should only use Exchange System Manager to set permissions on Exchange objects.

Understanding Exchange Objects and Exchange System Manager

Almost every element in an Exchange installation is represented by an object. For example, the server itself, an SMTP virtual server, and a mailbox store are all represented as objects. Controlling each of these objects is a set of security permissions. Permissions on objects in Exchange 2003 build on permissions that the Windows operating system makes available through Active Directory and IIS. Exchange 2003 uses both Active Directory and the IIS metabase to store permissions information about Exchange objects.

To accommodate the fact that information regarding Exchange objects is in two places, you manage these objects using Exchange System Manager. This tool seamlessly presents objects that are stored in Active Directory and the IIS metabase. Thus, you are able to administer objects stored in two places through a single interface.
The permissions model that Exchange System Manager exposes builds on the Windows security model—an object-oriented security model, based on the concept of discretionary access control. This means that each Exchange object has its own discrete permissions that govern access to the object, and that these permissions can be administered by anyone who has the appropriate permission level. This security model makes it possible to implement delegated security models in which certain roles are assigned varying permissions based on the functional tasks performed by these roles in those environments whose security policy requires that capability.

However, the profusion of objects and permissions that enables Exchange to support complex security requirements can also make it seem complex to administer. Fortunately, Exchange System Manager simplifies managing permissions with the following:

- Support for inheritance
- Standardized security roles
- Exchange Administration Delegation Wizard

Together, these features simplify the management of permissions so that most Exchange implementations can implement their security requirements without having to set permissions on individual attributes on individual objects.

**Benefiting from Support for Inheritance**

In Windows, *inheritance* describes the process by which the creation of an object results in the object assuming, by default, the permissions of its parent object.

Inheritance simplifies the task of managing permissions in your Exchange system as follows:

- It eliminates the need to manually apply permissions to child objects as they are created.
- It ensures that the permissions attached to a parent object are applied consistently to all child objects.
- When permissions on all objects within a container must be modified, you change the permissions on the container only once. The objects inside the container inherit the changes automatically.

For some Exchange objects, you can customize this inheritance. These objects are public folder trees, address lists, and mailbox stores. For these objects, you can specify that the child does not inherit permissions. Or, you can specify that only the following containers or subcontainers inherit permissions:

- This container only
- This container and all subcontainers
- Subcontainers only
Inheritance makes it possible for permissions to be applied consistently within an object hierarchy. In itself, inheritance is an important tool for simplifying the application of permissions.

**Benefiting from Standardized Security Roles in Exchange**

To help simplify the process of managing permissions, Exchange 2003 provides three predefined security roles that are available in the Exchange Administrative Delegation Wizard. These roles are a collection of standardized permissions that can be applied at either the organization or the administrative group level.

**Note**

For information about administrative groups, see "Creating and Managing Administrative Groups" earlier in this chapter.

When these roles are applied, the accounts or groups against which they are applied are immediately granted a set of standardized permissions on the object in question. Roles rely strongly on permission inheritance to ensure that permissions are applied consistently. When a role is applied, the standard permissions associated with that role are applied down the object hierarchy using inheritance.

Because the roles have been designed to meet the security requirements that are commonly found in an Exchange deployment, you should try to use these roles as much as possible.

The standard security roles that Exchange 2003 provides are:

- **Exchange Full Administrator** This role can fully administer Exchange system information and modify permissions. This role is appropriate for those who need to be able to modify permissions, and view and administer Exchange configuration information.

- **Exchange Administrator** This role can fully administer Exchange system information. This role differs from the Exchange Full Administrator primarily in that it cannot modify permissions. This role is appropriate for those who need to be able to view and administer Exchange configuration information without being able to modify permissions.

- **Exchange View Only Administrator** This role can view but cannot administer Exchange configuration information. This role is appropriate for those who need to be able to view Exchange configuration information without being able to change that configuration information. As with the Exchange Administrator role, this role cannot modify permissions.

**Note**

The Exchange security roles should not be confused with security groups in Active Directory. The roles are a collection of standardized permissions that are applied to users or groups within Active Directory. The roles can best be thought of as a template, rather than as a security group.
Because these roles are a set of standardized permissions, unlike security groups, roles inherently supersede one other. Therefore it is not necessary to apply both a higher and a lower privileged role. It is enough to apply the higher privileged role. Roles differ slightly, depending on whether they are applied to an organization or an administrative group. Consequently, the effective permissions that result when a role is applied can differ slightly.

Tables 2.1 to 2.3 list the effective permissions, based on the role applied and where it has been applied. These tables help explain how roles supersede each other, and the impact of differences at the organization level and administrative level.

**Note**
There is no table that shows the effective role at the organization level from roles applied at the administrative group level. This is because roles applied at the administrative group level apply only to the local administrative group. Because administrative groups are underneath the organization level in the hierarchy, the administrative group can inherit permissions from the organization, but not vice versa.

### Table 2.1 Effective roles at the administrative group level from roles applied at the administrative group level

<table>
<thead>
<tr>
<th>Granted Exchange Administrator role</th>
<th>Effective Exchange Administrator role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>View Only</td>
</tr>
<tr>
<td>Exchange View Only Administrator</td>
<td>Yes</td>
</tr>
<tr>
<td>Exchange Administrator</td>
<td>Yes</td>
</tr>
<tr>
<td>Exchange Full Administrator</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Table 2.2 Effective roles at the administrative group level from roles applied at the organization level

<table>
<thead>
<tr>
<th>Granted Exchange Administrator role</th>
<th>Effective Exchange Administrator role</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>View Only</td>
</tr>
<tr>
<td>Exchange View Only Administrator</td>
<td>Yes</td>
</tr>
<tr>
<td>Exchange Administrator</td>
<td>Yes</td>
</tr>
<tr>
<td>Exchange Full Administrator</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 2.3 Effective roles at the organization level from roles applied at the organization level

<table>
<thead>
<tr>
<th>Granted Exchange Administrator role</th>
<th>Effective Exchange Administrator role</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Only</td>
<td>Administrator</td>
</tr>
<tr>
<td>Exchange View Only Administrator</td>
<td>Yes</td>
</tr>
<tr>
<td>Exchange Administrator</td>
<td>Yes</td>
</tr>
<tr>
<td>Exchange Full Administrator</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Benefiting from Exchange Administration Delegation Wizard**

The Exchange Administration Delegation Wizard applies the standardized security roles at either the organization level or the administrative group level within Exchange System Manager.

It is important to remember that the Exchange Administration Delegation Wizard applies well-tested permissions in a consistent manner against objects in the Exchange hierarchy. Because of this consistency in application of permissions, the wizard is the recommended and preferred method of managing permissions in your Exchange environment. You should only apply customized permissions to individual objects when it is required by your security policy, and after thorough testing. Manually creating customized permissions increases the likelihood of problems, due to human error. It also increases the likelihood of creating inappropriate permissions, due to a misunderstanding of how permissions work. In addition, customized security settings will require increased maintenance because they must be documented, and the customized settings must be verified. Although there are instances where customized security is appropriate, the risks and costs should be weighed carefully.

You can launch the Exchange Administration Delegation Wizard from either the organization level or the administrative group level. As noted in "Benefiting from Standardized Security Roles in Exchange" earlier in this chapter, the permissions associated with the role will then be applied down the hierarchy from the object from which you started the wizard. For example, if you start the wizard at the organization level, the permissions associated with the role will be applied to all objects underneath the organization in the hierarchy, including all administrative groups. Alternately, if you start the wizard at an administrative group, the permissions associated with the role will be applied only to the objects within the administrative group.
When you start the Exchange Administration Delegation Wizard, it prompts you to specify the users and groups to which you want to apply the security role. Generally, it is recommended that you place your users into security groups, and then use the wizard to apply roles against those groups. Applying permissions to individual users can quickly become difficult to manage.

After the wizard is finished, Exchange System Manager applies permissions to the group or the user selected within the hierarchy that the wizard was started from. The permissions are propagated down the hierarchy through inheritance. By using the wizard, it is possible to set all of the permissions on the Exchange objects in both Active Directory and the IIS metabase with only a few clicks.

**Note**

For more information about managing store permissions, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores."
Chapter 2, "Managing an Exchange Organization," focused on how to apply settings globally within your organization, how to use and manage administrative groups, and how to use system policies to administer groups of servers consistently.

This chapter shifts the focus from the organization-specific settings to server-specific settings. It provides you with information about how to configure settings on individual Exchange servers in your organization. Individual server settings that you can configure include enabling message tracking, configuring language support for clients, scheduling Mailbox Management processes, troubleshooting specific issues with diagnostic logging, using public folder referrals and Directory Access options, and other settings that are important to managing your Exchange server.

Although this chapter does not cover them, you can also manage protocol settings, services, and backup and restore processes on an individual server basis. For more information about:

- Configuring protocols, see Chapter 5, "Understanding and Configuring Message Routing and Transport," and Chapter 6, "Managing Client Access to Exchange."
- Exchange services, see Appendix B, "Services Used by Exchange."
- Backup and restore practices, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores."
Configuring Server-Specific Settings

When you configure server-specific settings, you use the Properties dialog box (see Figure 3.1) that is associated with each server.

To open a server's Properties dialog box

- In Exchange System Manager, right-click an Exchange server, and then select Properties.

![ Figure 3.1 The Properties dialog box for SERVER01](Image)

Of the eleven tabs in the Properties dialog box, this chapter focuses on those tasks associated with the following tabs: General, Locales, Mailbox Management, Directory Access, Policies, Security, Full-Text Indexing, Diagnostic Logging, and Public Folder Referrals.
Viewing Messages in Message Tracking Center

Message Tracking Center tracks messages across servers in both mixed- and native-mode Exchange organizations. Message Tracking Center can also track messages that are destined to or arriving from another messaging system, such as Lotus Notes. Through Message Tracking Center, you can search for all types of messages, including system messages (alerts that are displayed when problems occur), public folder messages, and e-mail messages.

Note
To search for a specific system message in Message Tracking Center, search for the Message ID. If you do not know the Message ID, you can find system messages manually by reviewing the message tracking logs. Exchange automatically creates these logs if you have message tracking enabled on a server. To search for other types of messages, you can search by sender, recipient, or server.

Before enabling a server's messages to appear in Message Tracking Center, you must enable subject logging on the Exchange server. However, enabling this type of logging results in the subject lines of messages in Simple Mail Transfer Protocol (SMTP) and MAPI queues to be displayed in the Subject column of Queue Viewer. By default, the Subject column is left empty to preserve confidentiality. (For example, some Exchange organizations prefer to keep low-level administrators from viewing message subjects.) Therefore, verify your organization's policy about revealing subject line information prior to enabling subject logging.

To enable a server's messages to appear in Message Tracking Center

- On the General tab in the server's Properties dialog box, select the Enable subject logging and display check box.

Note
If the Enable subject logging and display check box is unavailable (or appears dimmed), there is a server policy object applied to this server. You must either enable subject logging and display on the policy, or remove the server from this policy. To view which policies are applied to this server, look at the Policies tab. For more information about server policies, see Chapter 2, "Managing an Exchange Organization."

Enabling Message Tracking

You can create a server policy to control the message tracking options of a group of servers in an administrative group. However, you can also enable message tracking on an individual server basis. For example, if you do not track messages on all of your servers, but users on a specific Exchange server are experiencing mail flow problems, you may want to enable message tracking on the server that is experiencing mail flow problems. Alternatively, you may want to track messages only on your Internet gateway servers.
When you enable message tracking on an individual server, messages routed through the server are added to the message tracking logs. These logs are text files that you can review to monitor and troubleshoot message flow. The Exchange System Attendant service on each server maintains these log files.

To enable message tracking

- On the General tab in the server's Properties dialog box, select the Enable message tracking check box.

Note
If the Enable message tracking check box is unavailable (or appears dimmed), there is a server policy object applied to this server. You must either enable message tracking on the policy, or remove the server from this policy. To view which policies are applied to this server, look at the Policies tab. For more information about server policies, see Chapter 2, "Managing an Exchange Organization."

Managing Message Tracking Log Files

If you enable message tracking, you may want to customize how Exchange manages the resulting log files. By default, Exchange stores the message tracking log files in the C:\Program Files\Exchsrvr folder and removes these log files on a seven-day interval. These default settings may or may not fit the needs of your Exchange environment.

Selecting a Location for the Log Files
To specify a path and folder for message tracking log files, you use the Log file directory text box on the General tab of the server's Properties dialog box. When you change the path of the log file directory, Exchange saves future log files to the new path. However, Exchange does not move existing log files to the new location. You must do this manually.

Removing Log Files
If you allow log files to accumulate on the server, they can consume a large portion of disk space and may affect performance. You should review and remove log files periodically. However, make sure to leave log files on the server long enough for you to review files if a problem occurs with the message flow. As an additional step, you can move log files to another disk that has the bandwidth to accommodate larger log files.

To specify how often log files are removed

1. On the General tab in the server's Properties dialog box, select Remove log files.
2. In the Remove files older than (days) text box, type the number of days that you want the files to remain on the server before being deleted.
Designating a Front-End Server

When you configure a server to be a front-end server, you are usually dedicating the server to receive requests from messaging clients, such as HTTP, Internet Message Access Protocol version 4 (IMAP4), and Post Office Protocol version 3 (POP3), and to relay client requests to the appropriate back-end server.

The services that an Exchange front-end server requires depend on the protocols that you use on the server, and whether you will be making configuration changes after the initial setup. Table 3.1 lists which Exchange services are required for each protocol or tool that an Exchange front-end server uses.

Table 3.1  Services required on an Exchange front-end server

<table>
<thead>
<tr>
<th>Protocol/tool on server</th>
<th>Services required</th>
</tr>
</thead>
</table>
| POP3                    | Exchange POP3 (POP3Svc)  
                          | Microsoft Exchange System Attendant (MSExchangeSA) |
| IMAP4                   | Exchange IMAP4 (IMAP4Svc)  
                          | MSExchangeSA |
| SMTP                    | Microsoft Exchange Information Store (MSExchangeIS)  
                          | MSExchangeSA |
| Exchange System Manager | MSExchangeSA |
| Routing Engine          | Microsoft Exchange Routing Engine (RESvc) |
| NNTP                    | Network News Transfer Protocol (NNTP) must be enabled on a server during upgrades. |

**Note**

The routing engine must be running on all Exchange servers, both front-end and back-end servers.

**Note**

You can disable this protocol if you are not offering it to your users.

To designate a front-end server

- On the **General** tab in the server's **Properties** dialog box, select the **This is a front-end server** check box.
After designating a server as a front-end server, you should remove any unnecessary components or disable any unnecessary services on the server. Removing these components or disabling these services allows the front-end server to relay client requests more efficiently and improves security by reducing the number of services or components that are vulnerable to attack. In particular, you can remove public folder stores and storage groups from an Exchange front-end server. Also, if your front-end users are not sending mail using SMTP, you can remove mailbox stores from the front-end server.

**Important**
To stop or disable services, use the Services snap-in in Microsoft Management Console (MMC).

For more information about using a front-end and back-end topology, see Chapter 6, "Managing Client Access to Exchange."

---

### Sending Error Information to Microsoft

Microsoft personnel monitor error reports to identify and correct common problems that customers encounter. If you do not enable the automatic error reporting option, a dialog box appears that prompts you to manually send the fatal error report.

**Important**
It is recommended that you send fatal error reports to Microsoft. When you send these reports, Microsoft personnel can respond to you with any available fixes for your reported issue. However, before sending information regarding any fatal service error to Microsoft, you should confirm that sending this information is permitted under your organization's security policy.

#### To send error information to Microsoft

- On the General tab in the server's Properties dialog box, select the **Automatically send fatal service error information to Microsoft** check box.

When you send error reports to Microsoft, they are sent over Secure HTTP (HTTPS), which is a more secure connection than HTTP.

**Note**
To send reports, the server must have HTTP access to the Internet.

For more information about automatic error reporting, see the "Microsoft Online Crash Analysis" Web site ([http://go.microsoft.com/fwlink/?LinkId=18428](http://go.microsoft.com/fwlink/?LinkId=18428)).
Configuring Language Settings

Different countries and regions have differing conventions regarding the formatting and presentation of information such as date, time, and currency. To accommodate these differences, you use the **Locales** tab to define how to display date, currency, and time values, and to define how to control other international settings, such as sorting order.

For each locale listed on the **Locales** tab, the server is able to supply clients with data sorted and formatted according to the conventions used in that locale. For example, if Hindi appears in the list, Hindi language clients that connect to the server see information sorted and formatted in Hindi.

**To add a locale to the server**

1. On the **Locales** tab in the server's Properties dialog box, click **Add** (see Figure 3.2).

![Figure 3.2 Locales tab](image)
2. In the **Add Locale** dialog box (see Figure 3.3), select a language, and then click **OK**.

![Add Locale dialog box](image)

**Figure 3.3** Add Locale dialog box

**Note**
You can also remove locales by selecting a locale on the **Locales** tab and then clicking **Remove**.

---

**Scheduling Mailbox Manager Processes**

Exchange Mailbox Manager policies set age and size limits for messages. After you create and configure a recipient policy for Mailbox Manager settings, you must schedule when the Mailbox Manager process runs on a server and whether the process generates a report. When a policy runs, the policy processes messages that exceed its defined limits. For more information about Mailbox Manager and recipient policies, see Chapter 4, "Managing Recipients and Recipient Policies."

**Important**
Mailbox Manager works only on local mailboxes on an individual Exchange server. You cannot configure Mailbox Manager on one server to process mailboxes on a different server.
To schedule when the Mailbox Manager process runs and whether the process generates a report, you use the **Mailbox Management** tab (see Figure 3.4) in the server's **Properties** dialog box.
Defining a Schedule

In the Start mailbox management process drop-down list, you select when you want the Mailbox Management process to start (on that particular server) according to the rules defined by associated recipient policies. The recipient policies that are associated with the server determine which mailbox or mailboxes that Mailbox Manager cleans.

To define a schedule

- On the Mailbox Management tab in the server's Properties dialog box, in the Start mailbox management process list, select a schedule, and then click OK.

  Tip
  You can manually start Mailbox Manager at any time by right-clicking the server object and then selecting Start Mailbox Management Process. If you use this command, Mailbox Manager still runs at its next scheduled interval.

You can also customize the mailbox management schedule to suit your organizational needs. For example, you could create a custom schedule that runs Mailbox Manager on Saturday at midnight.

To define a custom schedule

- On the Mailbox Management tab in the server's Properties dialog box, in the Start mailbox management process list, select Use custom schedule, click Customize, and then enter the schedule information.

Setting Reporting Options

When you schedule Mailbox Manager, you can designate a mailbox that receives Mailbox Manager reports. You can also select the type of report to be generated. The report can include different types of information, such as when Mailbox Manager ran, which mailbox recipient policies were applied, which mailboxes were processed, which folders were processed, the number of messages that were moved or deleted, and the size of messages that were moved or deleted.
To set reporting options

1. On the Mailbox Management tab in the server's Properties dialog box, in the Reporting drop-down list, select the type of report that you want created whenever mailboxes are processed:
   - A summary report that contains basic information, including the total size of all messages that Mailbox Manager moved or deleted.
   - A detailed report that includes the specific policies that Mailbox Manager ran, the specific mailboxes that were processed, and the specific folders within each mailbox that were processed each time Mailbox Manager runs.

2. In the Administrator text box, click Browse, and then select a mailbox in your organization to receive these reports.

Configuring Diagnostics Logging on a Server

Diagnostics logging levels determine which additional Exchange events are written to the Application event log in Event Viewer, a Microsoft Windows Server™ 2003 component that you can use to monitor hardware and software activities. You can use diagnostics logging to record significant events that are related to authentication, connections, and user actions.

The first step in configuring diagnostics logging is to decide which services on an Exchange server should be enabled for diagnostics logging (see Table 3.2).

Note
You configure diagnostics logging separately for each service on each server. For example, if you enable protocol logging on an individual virtual server, it is the setting on the Exchange server on which the virtual server runs that determines the logging capabilities for the protocol.
## Table 3.2  Diagnostics logging services

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMAP4Svc</td>
<td>Allows users to access mailboxes and public folders through Internet Message Access Protocol version 4 (IMAP4).</td>
</tr>
<tr>
<td>MSADC</td>
<td>Runs connection agreements if Active Directory Connector is installed.</td>
</tr>
<tr>
<td>MSExchangeAL</td>
<td>Logs events when the Recipient Update Service updates address lists and e-mail addresses in the Microsoft® Active Directory® directory service.</td>
</tr>
<tr>
<td>MSExchangeDSAccess</td>
<td>Allows Exchange access to Active Directory.</td>
</tr>
<tr>
<td>MSExchangeIS</td>
<td>Allows access to the Exchange store.</td>
</tr>
<tr>
<td>MSExchangeMTA</td>
<td>Allows X.400 connectors to verify whether the message transfer agent (MTA) is being used.</td>
</tr>
<tr>
<td>MSExchangeMU</td>
<td>Replicates Exchange configuration information changes to the Internet Information Services (IIS) metabase.</td>
</tr>
<tr>
<td>MSExchangeSA</td>
<td>Handles many core Exchange tasks, such as mailbox management, e-mail proxy generation, offline address list generation, and monitoring.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This service is also known as Microsoft Exchange System Attendant.</td>
</tr>
<tr>
<td>MSExchangeSRS</td>
<td>Replicates computers running Microsoft Exchange 2000 Server (or later) with computers running Microsoft Exchange Server version 5.5.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This service is also known as Site Replication Service (SRS).</td>
</tr>
<tr>
<td>MSExchangeTransport</td>
<td>Controls message routing and transport functions in Exchange. If you experience mail flow problems, set diagnostics logging for this service.</td>
</tr>
<tr>
<td>POP3Svc</td>
<td>Controls the operation of POP3.</td>
</tr>
</tbody>
</table>
After selecting a service, the next step is to set the logging levels for those services. There are four logging levels of detail (see Table 3.3). When Exchange generates an event less than or equal to the logging level, the event is logged. Events range from significant events (such as application failures) to moderately important events (such as the receipt of messages across a gateway) to events that are relevant only to debugging. Usually, you log only critical events. However, when problems occur, diagnostics logging enables you to change the logging levels to capture more events in greater detail.

Table 3.3 Logging levels

<table>
<thead>
<tr>
<th>Logging levels</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Only critical events, error events, and events with a logging level of zero are logged.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This is the default level for all services on Exchange servers.</td>
</tr>
<tr>
<td>Minimum</td>
<td>Events with a logging level of 1 or lower are logged.</td>
</tr>
<tr>
<td>Medium</td>
<td>Events with a logging level of 3 or lower are logged.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Events with a logging level of 5 or lower are logged.</td>
</tr>
</tbody>
</table>

After selecting a logging level, logging begins automatically whenever you start Exchange. You can view the log entries in Event Viewer.

**To configure diagnostics logging**

1. On the Diagnostics Logging tab in the server's Properties dialog box, in the Services list, select an Exchange 2003 service (see Table 3.2) on which you want to set category logging levels.

2. In the Categories list, select the categories and logging levels (see Table 3.3) that you want to configure.
Customizing Public Folder Referrals

When a user connects to a public folder store that does not contain a copy of the public folder content that the user is looking for, Exchange redirects or refers the user to another public folder store that does have a copy of the content. By default, Exchange attempts to redirect the user to a server within the local routing group. If those servers do not have the required content, Exchange follows the organization's routing group topology to find an appropriate server. Exchange finds an appropriate server based on the most efficient routing path, using costs of connectors between routing groups.

Note
For additional information about public folder referrals, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores." For more information about routing in Exchange, see Chapter 5, "Understanding and Configuring Message Routing and Transport."

Because Exchange keeps track of available connections between routing groups and uses the most efficient route possible, it is recommended that you use routing groups (the default) to determine how Exchange refers a user to another public folder. However, if you need to troubleshoot a specific server, or if you are performing maintenance on part of your network and want to designate specific servers that are available during this maintenance, you can create a custom list of servers for public folder referrals.

Note
A custom list for public folder referrals is new in Exchange 2003. In Exchange 2000, you could only specify whether or not to allow public folder referrals among routing groups.

To create a custom list of servers for public folder referrals, you use the Public Folder Referrals tab (see Figure 3.5). When you create a custom list of servers, you also assign costs to prioritize the servers in your referral list.
To specify a custom list for public folder referrals

1. On the Public Folder Referrals tab in the server's Properties dialog box (see Figure 3.5), in the Public folder referral options list, select Use Custom List.

![Figure 3.5  Public Folder Referrals tab](image)

2. Click Add to add the appropriate servers.
Assigning Costs on the Public Folder Referrals List

Costs are a method of prioritizing servers in the public folder referral list. You define costs for each connector within your organization using network connectivity and available bandwidth as criteria. You then assign the lowest cost to the connectors that have the best network connectivity and the most available bandwidth. Exchange uses higher-cost servers only if lower-cost servers are not available.

When you select the Use Custom List option and create a list of servers that are available for referrals, the Public Folder Referrals tab displays both the name of each server in the list and any costs that are associated with those servers. If you want to prioritize the order in which Exchange uses the listed servers, you need to change the costs associated with each server, assigning lower costs to those servers that you want Exchange to use first.

To change a server's priority in a custom public folder referrals list

1. On the Public Folder Referrals tab in the server’s Properties dialog box, select a server in the list, and then click Modify.

2. In the Modify Referral Cost dialog box (see Figure 3.6), specify a cost for that server.

Figure 3.6 Modify Referral Cost dialog box
Understanding Directory Access Options

As discussed in Chapter 1, "Preparing to Administer Exchange Server 2003," and Chapter 2, "Managing an Exchange Organization," Exchange is tightly integrated with Active Directory. This integration requires that the core components of Exchange 2003 access directory information in Active Directory. The shared component called Directory Access (DSAccess) controls how most components (see Table 3.4) in Exchange interact with Active Directory.

Table 3.4 Exchange components dependent on DSAccess

<table>
<thead>
<tr>
<th>Component</th>
<th>Dependency on DSAccess</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Metabase Update (DS2MB)</td>
<td>Directory changes tracked by update sequence number (USN)</td>
</tr>
<tr>
<td>Exchange Routing Engine (RESVC)</td>
<td>User and configuration lookups</td>
</tr>
<tr>
<td>SMTP Categorizer (SMTP CAT)</td>
<td>List of global catalog servers in the topology</td>
</tr>
<tr>
<td>Directory Service Proxy (DSProxy)</td>
<td>List of global catalog servers in the topology</td>
</tr>
<tr>
<td>Exchange Information Store</td>
<td>User and configuration lookups</td>
</tr>
<tr>
<td>WebDAV</td>
<td>User and configuration lookups</td>
</tr>
<tr>
<td>Message transfer agent (MTA)</td>
<td>User and configuration lookups</td>
</tr>
</tbody>
</table>
In Exchange 2003, DSAccess is the centralized mechanism that determines the Active Directory topology, opens the appropriate Lightweight Directory Access Protocol (LDAP) connections, and works around server failures. DSAccess is responsible for the following functions:

- Retrieving and writing information from Active Directory, such as configuration data and recipients.
- Caching information from Active Directory for better performance when querying Active Directory. DSAccess caches configuration and recipient data locally so that this information is available for subsequent queries from other Exchange servers. Caching information locally has the additional benefit of preventing the network traffic that is caused by additional queries to Active Directory.
- Constructing a list of available domain controllers and global catalog servers that other Exchange components can query. For example:
  - The MTA routes LDAP queries through the DSAccess layer to Active Directory.
  - To connect to databases, the store process uses DSAccess to obtain configuration information from Active Directory.
  - To route messages, the transport process uses DSAccess to obtain information about the connector arrangement.

Of the previously listed functions, the only function that you can control on a server is the one that deals with constructing a list of available domain controllers and global catalog servers. You can have this list constructed automatically by DSAccess, or you can manually create this list for DSAccess to use.
Automatically Constructing a Topology for Directory Access

By default, on each Exchange server, DSAccess automatically detects the appropriate domain controllers and global catalog servers in Active Directory for the Exchange server to query. The setting that controls this default behavior is the Automatically discover servers check box near the bottom of the Directory Access tab in the server's Properties dialog box (see Figure 3.7).

![Figure 3.7 Directory Access tab](image-url)
Selecting the **Automatically discover servers** check box enables DSAccess components to automatically discover the following servers in an Exchange organization:

- **Configuration domain controller** The single domain controller that reads and writes information in the configuration naming context in Active Directory. DSAccess chooses a domain controller or global catalog server to act as the configuration domain controller. All configuration data is written and read by this configuration domain controller.

- **Working domain controllers** As many as ten domain controllers that perform Active Directory lookups for objects in the local domain. These domain controllers are primarily used to update objects within the local domain or read non-configuration data that is not replicated to global catalog servers.

- **Working global catalog servers** As many as ten global catalog servers that perform forest-wide queries. All user data is looked up on the global catalog servers.

To discover these servers, Directory Access locates domain controllers and global catalog servers that run Microsoft Windows Server 2003, or Microsoft Windows® 2000 Server Service Pack 3 (SP3) or higher. Directory Access then tests these servers and chooses suitable servers for Exchange services to use to perform Active Directory queries.

**Note**
Because manually constructed topologies do not update automatically, it is strongly recommended that you use the **Automatically discover servers** setting.

---

**Manually Constructing a Topology for Directory Access**

To troubleshoot problems with a specific global catalog server or domain controller, you may want to override the automatic discovery of servers by clearing the **Automatically discover servers** check box. For example, to determine whether queries to a global catalog server are working correctly, you can manually set this server as the only available global catalog server.
When you manually create a topology for DSAccess, you no longer have the advantages of automatic failover and load balancing that you have when DSAccess automatically discovers the topology. If a server that you set manually becomes unavailable, the list does not update and Exchange still attempts to use the unavailable server, thereby causing Exchange to fail.

If you manually set a domain controller or global catalog server on the Directory Access tab in the Properties dialog box of a server that is not running Windows 2000 Server SP3 or later, Exchange will not use the domain controller or global catalog server, and Exchange logs an Event 2116.

To manually create a topology for Directory Access

1. On the Directory Access tab in the server's Properties dialog box, in the Show list, select the type of servers that you want to view.

   **Note**
   You cannot clear the Automatically discover servers check box if you select All Domain Controllers in the Show list.

2. Clear the Automatically discover servers check box.
   This clears the current list of servers.

   **Warning**
   By default, DSAccess automatically discovers servers. It is strongly recommended that you keep this setting.

3. Click Add to add servers to or click Remove to remove servers from the topology.

Viewing System Policies Applied to the Server

System policies facilitate flexible administration of large numbers of Exchange services. A system policy defines settings that you apply to one or more Exchange servers. For example, you can use a system policy to create a consistent method of tracking messages across a group of servers.
Because policies affect a group of servers, you can only view the policies that have been applied to a server on the Policies tab (see Figure 3.8) in the server's Properties dialog box. You cannot modify or remove those policies using this tab. To modify or remove a system policy that has been applied to a particular server, you must change the policy itself. For more information about system policies, see Chapter 2, "Managing an Exchange Organization."

![Figure 3.8 Policies tab](image)
Setting Server-Specific Permissions

Permissions control access to Exchange objects. You can set permissions on some Exchange objects individually. These objects include public folder trees, address lists, mailbox stores, protocols, and servers. For these objects, Exchange uses and extends Active Directory permissions. Examples of Active Directory permissions are Read, Write, and List contents. Examples of extended Exchange permissions are Create public folder and View Information Store status. When you look at an object's permissions, Active Directory permissions appear first in the list, followed by Exchange extended permissions.

Permissions in Exchange are inherited by default. For example, the permissions that you apply to a particular server are inherited by the objects that the server contains, such as the public folder and mailbox stores on that server. Inherited permissions are convenient because you do not have to set the permissions for every object in your Exchange organization manually.

Important
When setting permissions on Exchange objects, use Exchange System Manager. Do not set permissions on Exchange objects using Windows Server 2003 MMC snap-ins, such as the Active Directory Sites and Services or Active Directory Users and Computers.

You can set permissions using the Exchange Delegation Wizard and apply these settings to an entire Exchange organization or to a specific administrative group. Because permissions are inherited, these permissions control who can view or modify settings at the server level. By default, these permissions are configured to support the standard Exchange administrator types (Exchange View Only Administrator, Exchange Administrator, and Exchange Full Administrator). You are strongly advised to use the standard Exchange administrator types and only change the settings if more granular settings are required by your organization's security policy.

Note
For more information about the Exchange Delegation Wizard, see Chapter 2, "Managing an Exchange Organization."
To modify permissions on a specific server

1. On the Security tab (see Figure 3.9) in the server’s Properties dialog box, in the Group or user names list, select the group or user name for which you want to modify permissions.

![Figure 3.9 Security tab](image)

2. In the Permissions for <selected entry> list, select the appropriate permissions.

---

**Configuring System Resource Usage During Full-Text Indexing**

Exchange can create and manage indexes for fast searches and lookups. With full-text indexing, Exchange indexes every word in a database, making faster searching possible. Full-text indexing is a feature that you can configure for individual stores on a server, and optimize on a server-by-server basis across your Exchange organization. For more information about how to configure full-text indexing to support your Exchange organization, see Chapter 4, "Managing Recipients and Recipient Policies" and Appendix F, "Using Full-Text Indexing."
Full-text indexing allows IMAP4 clients and MAPI clients, such as Microsoft Office Outlook®, to conduct full-text searches. For Outlook users, the version of Outlook determines what search options the user has:

- In Outlook 2002, both the **Find** and **Advanced Find** options on the **Tools** menu initiate a full-text search.
- In Outlook 2000, only the **Advanced Find** option initiates a full-text search. The **Find** option initiates a character-based search.

Indexing is a resource-intensive feature that requires considerable CPU cycles. Indexing gigabytes of data can take hours or days. You should schedule indexing at times when the server is not under usage load.

**To control server performance during indexing**

- On the **Full-Text Indexing** tab (see Figure 3.10) in the server's **Properties** dialog box, in the **System resource usage** list, select a usage level: **Minimum**, **Low**, **High**, or **Maximum**.

  
  **Note**
  
  To limit the CPU resources that the indexing service occupies, set the server usage level to a lower value (**Minimum** or **Low**).

![Figure 3.10 Full-Text Indexing tab](image)
This chapter explains what recipients and recipient policies are, and how to create and manage recipients. The chapter also includes information about address lists and the Recipient Update Service. Basic concepts about recipients are explained in the beginning of this chapter. The remainder of the chapter focuses on creating and managing recipients, recipient policies, and address lists. This chapter also includes detailed information about a new feature in Microsoft® Exchange Server 2003—the query-based distribution list.

Understanding Recipients

Central to any messaging system are the people and resources that receive messages. An individual may receive a message from a coworker, or a public folder may receive a message from a participant in a particular discussion.

Although messages are received by people, the term *recipients* refers to Microsoft Active Directory® directory service objects, not people. Recipients are Active Directory objects that have messaging capabilities. However, the object itself does not receive messages. The messages are not stored in Active Directory. Instead, they can reside in a mailbox on an Exchange server, in a public folder, or in another messaging system.

People access messages that are sent to them by using a client application. Examples of client applications include Microsoft Outlook®, Outlook Web Access, and Outlook Mobile Access. Each of these clients receives notification when a new message arrives and receives pointers to the location of the message, so that the message can be opened and read.
The following scenario explains the distinction between the person who receives e-mail messages and Active Directory objects. Carole, a member of the marketing team, has a user account that allows her to type her user name and password to log on to her computer and her company's network. After logging on, she has access to several network resources, one of which is her Exchange mailbox. Carole accesses her mailbox with an e-mail client, Outlook 2002. Outlook queries her Exchange mailbox and presents Carole a list of messages in her Outlook Inbox. When Carole opens one of these messages, Outlook retrieves the contents of the message from the message store on the Exchange server that houses her mailbox.

As shown in Figure 4.1, there is a recipient that is an Active Directory user object named carole. Mail that is addressed to carole is stored in an associated mailbox on an Exchange server. When the proper credentials are sent to the domain controller for user object carole, the contents of the mailbox become available to the e-mail client.

So, in Exchange, the term recipient refers to an Active Directory object that is mailbox-enabled or mail-enabled. Mailbox-enabled recipients can send, receive, and store messages. Mail-enabled recipients can only receive messages.

Table 4.1 describes the Active Directory objects that can be Exchange recipients.
### Table 4.1  Exchange recipient objects

<table>
<thead>
<tr>
<th>Active Directory object</th>
<th>Type of recipient</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Mailbox-enabled</td>
<td>Users can log on to networks and access domain resources. Users can be added to groups and appear in the global address list (GAL). Mailbox-enabled users can send and receive messages and store messages on their Exchange server. Mail-enabled users can receive messages at an external e-mail address only. They cannot send or store messages on Exchange.</td>
</tr>
<tr>
<td></td>
<td>Mail-enabled</td>
<td></td>
</tr>
<tr>
<td>InetOrgPerson</td>
<td>Mailbox-enabled</td>
<td>A user object that has had its properties extended to improve compatibility with directory services that use the InetOrgPerson object. As a recipient, InetOrgPerson has the same characteristics as a user object. To mail-enable or mailbox-enable an InetOrgPerson object, you must have a Microsoft Windows Server™ 2003 domain controller and an Exchange 2003-only environment (no servers running Exchange 2000 Server or Exchange Server version 5.5).</td>
</tr>
<tr>
<td></td>
<td>Mail-enabled</td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td>Mail-enabled</td>
<td>Contacts are objects that contain information about people or organizations outside of the Exchange organization. Mail-enabled contacts can receive e-mail messages at an external e-mail address. They can be added to distribution lists and appear in the GAL. Contacts cannot access network resources.</td>
</tr>
<tr>
<td>Groups</td>
<td>Mail-enabled</td>
<td>A group is an object that can contain users, InetOrgPerson objects, contacts, public folders, and other groups.</td>
</tr>
<tr>
<td><strong>Active Directory object</strong></td>
<td><strong>Type of recipient</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Query-based distribution groups</td>
<td>Mail-enabled</td>
<td>Query-based distribution groups are similar to standard distribution groups, except that they use an LDAP query to dynamically build the group membership. The query is run when a message is sent to the query-based distribution group. When you create a query-based distribution group, you select the criteria for the query.</td>
</tr>
<tr>
<td>Public folders</td>
<td>Mail-enabled</td>
<td>Public folders are repositories for messages and other files that can be accessed by users on the network.</td>
</tr>
</tbody>
</table>

**Note**
Although public folders are recipients, they are different from the other recipient types mentioned here. For more information about public folders, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores."

---

### Understanding Recipient Policies

To receive letters and packages, a person must have a mailing address to give to senders. This mailing address could be a business address, the physical address of his or her home, or a post office box. Likewise, for a recipient to receive messages in an Exchange mailbox, the recipient must have an e-mail address.

To generate e-mail addresses for each recipient in an organization, you use recipient policies. This section focuses on how recipient policies manage these e-mail addresses, as well as how recipient policies manage mailboxes using the Mailbox Manager.

**Note**
Recipient policies also establish the mail domain for which Exchange accepts incoming mail. For more information, see Chapter 5, "Understanding and Configuring Message Routing and Transport."
Managing E-Mail Addresses

A recipient policy that manages e-mail addresses has the following characteristics:

- It applies to a selected group of recipients.
- It always contains information about the address types that are to be applied to those recipients.
- It is given a priority, so that administrators can control which address is applied as the primary address to a recipient that may appear in more than one policy.

**Example Scenario**
The Exchange administrator for Fourth Coffee wants to create three e-mail addresses for recipients in the organization. The first is for the board of directors, the second is for the employees of the company who work in New York, and the third is for the remainder of the employees at the home office. He creates three recipient policies, as shown in Table 4.2.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Priority</th>
<th>SMTP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board of Directors</td>
<td>1</td>
<td>@board.fourthcoffee.com</td>
</tr>
<tr>
<td>New York Employees</td>
<td>2</td>
<td>@newyork.fourthcoffee.com</td>
</tr>
<tr>
<td>Default</td>
<td>lowest</td>
<td>@fourthcoffee.com</td>
</tr>
</tbody>
</table>
Table 4.3 shows information for three different users.

Table 4.3  User information for Fourth Coffee personnel

<table>
<thead>
<tr>
<th>Name</th>
<th>Office</th>
<th>Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jonathan Haas</td>
<td>New York</td>
<td>Yes</td>
</tr>
<tr>
<td>Yale Li</td>
<td>New York</td>
<td>No</td>
</tr>
<tr>
<td>Britta Simon</td>
<td>Portland</td>
<td>No</td>
</tr>
</tbody>
</table>

The first recipient policy, Board of Directors, runs and finds Jonathan Haas in the list of board members. His address is set to <alias>@board.fourthcoffee.com. The next policy, New York Employees, runs. It finds Jonathan Haas again. However, because a policy with a higher priority has already been applied to him, no action is taken. The policy continues running and finds Yale Li. No previous policy has applied to Yale, and Yale Li's address becomes <alias>@newyork.fourthcoffee.com. Finally, the default policy runs. Because no previous policy has applied to Britta Simon, her address becomes the default address, <alias>@fourthcoffee.com.

You may want to apply more than one address to a group of recipients. In the preceding example, if everyone in the company should receive e-mail messages at <alias>@fourthcoffee.com, that address must be included in all three recipient policies. When you have more than one address in a recipient policy, only one address is considered the primary address per address type. This means that you can only have one primary Simple Mail Transfer Protocol (SMTP) address and one primary X.400 address. You could have 10 SMTP addresses for one recipient, but only one of those can be the primary SMTP address.

The difference between primary and secondary addresses is that the primary address serves as the return e-mail address. When mail is received from a recipient, the primary address determines which address the mail appears to have come from. Recipients can receive mail sent to any of the addresses associated with them. Table 4.4 shows the primary and secondary e-mail addresses of the three people in the scenario.
Table 4.4  Primary and secondary e-mail addresses

<table>
<thead>
<tr>
<th>Name (alias)</th>
<th>Receive mail sent to</th>
<th>Send mail from (primary e-mail address only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jonathan Haas (Jon)</td>
<td><a href="mailto:Jon@board.fourthcoffee.com">Jon@board.fourthcoffee.com</a></td>
<td><a href="mailto:Jon@board.fourthcoffee.com">Jon@board.fourthcoffee.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:Jon@fourthcoffee.com">Jon@fourthcoffee.com</a></td>
<td></td>
</tr>
<tr>
<td>Yale Li (Yale)</td>
<td><a href="mailto:Yale@newyork.fourthcoffee.com">Yale@newyork.fourthcoffee.com</a></td>
<td><a href="mailto:Yale@newyork.fourthcoffee.com">Yale@newyork.fourthcoffee.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:Yale@fourthcoffee.com">Yale@fourthcoffee.com</a></td>
<td></td>
</tr>
<tr>
<td>Britta Simon (Britta)</td>
<td><a href="mailto:Britta@fourthcoffee.com">Britta@fourthcoffee.com</a></td>
<td><a href="mailto:Britta@fourthcoffee.com">Britta@fourthcoffee.com</a></td>
</tr>
</tbody>
</table>

Notice that Jonathan Haas is in the New York office, yet does not have the `<alias>@newyork.fourthcoffee.com` address. To have this secondary address, it would be necessary to include it in the recipient policy that applies to him. However, the policy with the highest priority that applies to Jonathan is the Board of Directors policy. Because the members of the board of directors all work in different states, the policy does not include `<alias>@newyork.fourthcoffee.com`. To add `<alias>@newyork.fourthcoffee.com` to Jonathan, you can manually add a secondary address in Active Directory Users and Computers, or you can programmatically add `<alias>@newyork.fourthcoffee.com` as a secondary address to all employees in the New York office.

**Note**
This example scenario shows how recipient policies are applied. The behavior of recipient policies differs when co-existing with Exchange Server 5.5.

### Managing Mailboxes Using Mailbox Manager

In addition to generating and assigning addresses to recipients, recipient policies can be used to manage mailboxes using Exchange Mailbox Manager. Mailbox Manager sets age and size limits for messages, and then it finds and processes messages that exceed those limits.

There is no default policy that enforces age or size limits for messages. When you create the first such policy, the default limits of 30 days and 1,024 kilobytes (KB) are applied to every folder in a mailbox. A message must exceed both limits before Mailbox Manager will process it. Under the default settings, a 500-KB message will never be processed, no matter how old it is.
Before Mailbox Manager will run, you must start the mailbox management process on the server object in Exchange System Manager. To start the mailbox management process, you use the **Mailbox Management** tab of the **Properties** dialog box for the server object (see Figure 4.2). For more information, see "Scheduling Mailbox Manager Processes" in Chapter 3, "Configuring Exchange Server Settings."

What happens when Mailbox Manager processes a message depends on the setting that you choose when creating the policy. By default, only a report is generated. No further action is taken. In addition to the default setting, there are three other options for how Mailbox Manager processes messages that exceed the specified limits. Table 4.5 describes all four of these Mailbox Manager options.
### Table 4.5 Mailbox Manager options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate report only (default)</td>
<td>No messages are moved or deleted, but an administrator report is generated that indicates which mailboxes contain items that exceed the limits defined by the mailbox recipient policy.</td>
</tr>
<tr>
<td>Move to Deleted Items folder</td>
<td>Messages are moved to the Deleted Items folder in each client mailbox. Messages are handled as if deleted by the client. Users can remove them from the Deleted Items folder if they want to.</td>
</tr>
<tr>
<td>Move to System Cleanup folders</td>
<td>A partial replica of the folder hierarchy of the mailbox is created under a root folder called System Cleanup. Affected messages are moved into the appropriate subfolder of the System Cleanup folder. This feature gives users a way to recover recently deleted items, without losing information about the original folder location of the items.</td>
</tr>
<tr>
<td>Delete immediately</td>
<td>Messages are immediately deleted from client view without being moved to either the Deleted Items or System Cleanup folder.</td>
</tr>
</tbody>
</table>

You can use the same limits for every folder that the mailbox recipient policy applies to, or set custom limits on a folder-by-folder basis. Each folder must be configured individually if its limits differ from the default limits.

### Creating Recipients

Recipients can either be created manually using Active Directory Users and Computers or programmatically using APIs. This section focuses on manually creating mailbox-enabled and mail-enabled objects, including distribution groups. For information about public folder creation, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores." For information about programmatically creating recipients, download the Exchange Software Development Kit (SDK) or view it online from the Exchange developer center (http://msdn.microsoft.com/exchange).
Mailbox-Enabled and Mail-Enabled Recipients

This section focuses on creating mail-enabled objects with the following notes and exceptions:

- Public folders are mail-enabled recipients that differ significantly from other recipients. For more information about public folders, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores."
- InetOrgPerson objects can be mail-enabled only if you have a Windows Server 2003 domain controller and have only Exchange 2003 servers in your organization.
- Mail-enabled groups are covered in their own section that follows.
- Some Active Directory objects, such as computers and printers, cannot be made into recipients.

To create a new Active Directory object that can be mail-enabled or mailbox-enabled, use Active Directory Users and Computers, as shown in Figure 4.3.
When you create a recipient object on a network where Exchange is already installed, the recipient will be mailbox-enabled or mail-enabled by default. Clear the **Create an Exchange mailbox** check box (as shown in Figure 4.4) if you do not want to mail-enable or mailbox-enable the Active Directory object.

**Note**
To see the options that are specific to Exchange, you must have the Exchange system tools installed on the computer that is being used to create users in Active Directory Users and Computers. Users created on computers without Exchange system tools installed will not have mailboxes created by default.

![Figure 4.4 Clear the check box for the object not to be a recipient](image)
To make an existing Active Directory object a recipient

1. In Active Directory Users and Computers, right-click the object, and then select **Exchange Tasks**.

2. On the **Available Tasks** page (see Figure 4.5) in the Exchange Task Wizard, select **Create Mailbox** or **Establish E-mail Address**.

![Exchange Task Wizard](image)

**Figure 4.5** Using Exchange Task Wizard to mail-enable or mailbox-enable an existing user object

**Note**
If **Create Mailbox** is not available, the object cannot be mailbox-enabled. However, if **Delete Mailbox** is listed instead, the object already has a mailbox associated with it. Each recipient can have only one Exchange mailbox.

**Mail-Enabled Groups**

Groups are used to assemble Active Directory objects under one name. This reduces the overhead required to manage users, especially those with similar needs. For example, you may have a network resource, such as a public folder, that everyone on your marketing team needs to access. You could give each individual on the team permissions to that folder, or you could create a security group called "marketing" and add each member of the marketing team to that group. Then, you can give the group permission to the folder. After a group has been established, you can give that group access to other resources, such as additional public folders, without having to locate every member of the marketing team each time.
There are two main types of groups: security and distribution. Security groups are security principals in Active Directory. This means that security groups can be set in the access control list (ACL) of a resource, such as a network share or public folder. Distribution groups exist for sending e-mail messages to collections of users. In a Microsoft Windows® environment without Exchange, there are limited uses for distribution groups. Both security and distribution groups can be mail-enabled. They cannot be mailbox-enabled because they represent a collection of users.

**Creating Mail-Enabled Groups**

A mail-enabled group represents a collection of recipient objects. Its purpose is to expedite the distribution of messages to multiple e-mail addresses. Create a group as you would any other recipient object. Notice, however, that *Create an Exchange e-mail address* is not selected by default for groups. To enable the group for mail, select *Create an Exchange e-mail address* during the process of creating the group (see Figure 4.6).

![Figure 4.6 Creating a group that is enabled for mail](image-url)
To enable an existing group for mail

1. In Active Directory Users and Computers, right-click the group, and then click Exchange tasks.

2. On the Available Tasks page (see Figure 4.7) in the Exchange Task Wizard, select Establish E-mail Address on Groups.

![Figure 4.7 Using Exchange Task Wizard to enable an existing group for mail](image)

Expanding Mail-Enabled Groups

When mail is sent to a mail-enabled group, the group is first expanded, and then mail is sent to each of the recipients in the group. Unless an expansion server (a server that is responsible for expanding distribution groups) is specified, the group will be expanded on the first Exchange server that handles the message.

Expansion of large groups can tax system resources on an Exchange server. For large distribution groups, you may want to designate a dedicated expansion server to alleviate the workload of the other production servers. Mail sent to large distribution groups will not slow the Exchange servers that your users use to access their mailboxes.

There is a drawback to setting a specific server as the expansion server for a group: If that server is unavailable, no member of the distribution group receives the message. However, if you leave the default setting, Any Server in the Organization, most of the users receive their messages if one server fails. Also, if all members of a distribution group are on well-connected servers, setting a specific expansion server may be unnecessary.
For information about setting specific expansion servers, see "Managing Recipient Settings" later in this chapter.

### Using Mail-Enabled Groups in Multi-Domain Environments

To expand distribution lists into individual recipients, Exchange contacts a global catalog server. The global catalog server has a copy of all global and universal groups in its domain and a copy of universal groups from other domains, but it does not have a copy of global groups from other domains. This becomes important in multi-domain environments because if a message is destined for a global distribution group in a domain that is separate from the global catalog server, Exchange cannot expand the distribution group on that message. Because the global catalog server does not have copies of the membership of global groups for domains outside of its own, it does not contain any information about the distribution list. Therefore, the categorizer cannot expand the distribution list. To avoid this problem, you should always use universal distribution groups in multi-domain environments. Use global groups within single domains only.

### Understanding Query-Based Distribution Groups

A query-based distribution group is a new type of distribution group introduced in Exchange 2003. This section explains what a query-based distribution group is, how it works, and how to create one.

#### Query-Based Distribution Groups Described

A query-based distribution group provides the same functionality as a standard distribution group. However, instead of specifying static user memberships, you can use an LDAP query (for example, "All full-time employees in my company") to dynamically build membership in a query-based distribution group. This results in much lower administrative costs because of the dynamic nature of the distribution group. However, query-based distribution groups have a higher performance cost for queries whose outcome produces a large number of results. This cost is in terms of server resources, such as high CPU usage and increased memory usage. This increased usage occurs because every time an e-mail message is sent to a query-based distribution group, an LDAP query is executed against Active Directory to determine its membership.

**Important**

You cannot view the membership of a query-based distribution group in the GAL because it is dynamically generated each time mail is sent.
Query-based distribution groups work reliably in the following topologies:

- Exchange 2003-only environment (no Exchange servers prior to Exchange 2003) running in native mode.
- Exchange 2000 Service Pack 3 (SP3) and Exchange 2003 in native mode. If you have Windows 2000 global catalog servers in this scenario, you can modify a registry key on the Exchange 2000 SP3 servers to increase reliability. This modification is covered in the next section.

If you are running versions of Exchange prior to Exchange 2000 SP3 in your environment, query-based distribution groups will not work reliably.

### Modifying Exchange 2000 SP3 Servers for Use with Windows 2000 Global Catalog Servers

Use the following procedure to configure an Exchange 2000 SP3 server for improved reliability in environments where query-based distribution groups will be expanded with Windows 2000 global catalog servers.

**Warning**
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To modify your Exchange 2000 SP3 server

1. Start Registry Editor.
2. In Registry Editor, locate the following registry key:
   
   ```plaintext
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SMTPSVC\Parameters
   ```
3. In the details pane, right-click, point to New, and then click DWORD Value.
4. Type `DynamicDLPageSize` for the name.
5. Right-click `DynamicDLPageSize`, and then click Modify.
6. Under Base, click Decimal, and then click OK.
7. In Edit DWORD Value, under Value Data, type 31.

**Note**
You need only do this for Exchange 2000 servers that use Windows 2000 global catalog servers.
How Query-Based Distribution Groups Work

When a message is submitted to a query-based distribution group, Exchange handles the message slightly differently from messages destined for other recipients. A query-based distribution group flows through Exchange to the proper recipients as follows:

1. E-mail messages are submitted through the Exchange store driver or SMTP to the submission queue.
2. The categorizer, a transport component that is responsible for address resolution, determines that the recipient is a query-based distribution group.
3. The categorizer sends the LDAP query request to the global catalog server.
4. The global catalog server runs the query and returns the set of addresses that match the query.
5. After receiving the complete set of addresses that match the query, the categorizer generates a recipient list containing all of the users. The categorizer must have the complete set of recipients before it can submit the e-mail message to routing. Therefore, if an error occurs during the expansion of the query-based distribution group to its individual recipients, the categorizer must restart the process.
6. After the categorizer sends the complete, expanded list of recipients to routing, the standard message delivery process continues, and e-mail messages are delivered to the mailboxes of the recipients.

The process differs if a dedicated expansion server is used for query-based distribution groups. In this case, rather than sending a query to the global catalog server for expansion as discussed in Step 3, the e-mail message is first routed to the dedicated expansion server. After the message arrives at the expansion server, the expansion occurs, and the delivery follows the same process as described earlier. The expansion server must be an Exchange 2000 SP3 server or later.

Deployment Recommendations for Query-Based Distribution Groups

The time that Exchange requires to expand a query-based distribution group and run the query depends on several factors, as follows:

- **Type of hardware deployed in your organization** The categorizer can require up to 2 KB of memory for each recipient. This is a conservative metric that you can use as a baseline. Using this baseline, if you send an e-mail message to a query-based distribution group of 6,000 users (meaning that the query returns 6,000 records), the categorizer requires 12 megabytes (MB) of RAM solely to expand the query-based distribution group. Although this use of memory is temporary, it does occur every time the group is expanded. Similarly,
sending an e-mail message to a larger query-based distribution group of 100,000 users, the categorizer requires approximately 200 MB of RAM. The processor speed and amount of available physical memory affects how long it will take to deliver the e-mail messages after the expansion.

- **Global catalog or expansion server availability affects the expansion and delivery of e-mail messages that users send to query-based distribution groups** If all global catalog servers are unavailable, the message is placed in retry mode in the categorizer, which means that the complete expansion restarts after one hour.

The general recommendation is to divide large query-based distribution groups into combinations of standard distribution groups, and assign different expansion servers for each large distribution group. The following options describe three approaches to doing this.

**Option 1** Designate an Exchange 2003 server with no mailboxes, such as a public folder replica server or a bridgehead server, as the expansion server for a large query-based distribution group. Because this server has more bandwidth and resources to expand the query-based distribution group, expansion and delivery are more efficient.

**Option 2** Create a query-based distribution group for every Exchange server, and limit each query-based distribution group to the mailboxes on that Exchange server. Designating this same server as the expansion server optimizes mail delivery. Then, use aggregate standard distribution groups that contain these query-based distribution groups as members. For example, to create a query-based distribution group for all full-time employees, you could create a query-based distribution group on each server for full-time employees, and name them "Server1 Full Time" and "Server2 Full Time." Then, create a distribution group composed of these server-based groups called "AllFullTime."

**Note** The distribution group that you use to combine the query-based distribution groups cannot itself be a query-based distribution group.

**Option 3** The following example illustrates a third approach for improved handling of large query-based distribution groups.

You want to create a query-based distribution group called "All employees" with 100,000 users. Consider dividing the group into the following smaller query-based distribution groups and combining these groups into a single standard distribution group:

- "All Temps" 10,000 users
- "All Vendors" 5,000 users
- "All Full-Time" 65,000 users
- "All Interns" 2,000 users
- "All Contractors" 18,000 users

In this case "All Full-Time" would be a large distribution group, so you may want to assign a specific expansion server to it. The other query-based distribution groups can be assigned an
expansion server based on how the users are distributed across your Exchange servers. For example, if all of the interns reside on one Exchange server, you may want to designate the same server as the expansion server for "All Interns." Overall, this proposed approach will perform much better than a single query-based distribution group with 100,000 recipients.

Guidelines for Creating Query-Based Distribution Groups

Use the following guidelines when you create query-based distribution groups:

- Use query-based distribution groups in an Exchange 2003-only environment, or a native mode environment with Exchange 2003 and Exchange 2000 in which all Exchange 2000 servers are running Service Pack 3 or later.

- Use universal groups in multi-domain environments when you create distribution groups that span domains. Although query-based distribution groups can be added to global distribution groups, domain local groups, and global security groups, and can contain any of these groups, membership in these types of groups is not replicated to global catalog servers in other domains. Universal distribution groups should be used in situations where distribution will span a multi-domain environment.

- When you combine query-based distribution groups into an aggregate group, combine them in a universal group. Only universal groups are available on global catalog servers across domains.

- When you build query-based distribution groups, include only universal groups if the membership is to be available in all of the domains in a multi-domain environment.

- Index the attributes that you use in the query. Indexing greatly improves the performance of the query, and it reduces the time that Exchange requires to expand the distribution group and deliver the e-mail message to the intended recipients. For more information about indexing attributes, see Microsoft Knowledge Base Article 313992, "How To Add an Attribute to the Global Catalog in Windows 2000" (http://support.microsoft.com/?kbid=313992).

- If the filter string contains incorrect formatting or incorrect LDAP syntax, the global catalog server will not run the query. Using Active Directory Users and Computers to create your query can help prevent you from constructing an incorrect query. You can also use the Preview button to view the result of the query. This will confirm the validity and expected results of the query. If you create a query-based distribution group based on an incorrect LDAP query, when a user sends mail to the query-based distribution group, the user receives a non-delivery report (NDR) with the code 5.2.4. If you enable categorizer logging, Exchange logs one of two events with event identifiers of 6024 or 6025.
• If the filter string is well-formatted, but produces no results, the sender will not get an NDR. This is the same outcome that occurs if you send to an empty distribution group. As previously stated, use the Preview button in Active Directory Users and Computers to confirm the expected results of your query.

• Use Exchange System Manager in a security context where its permissions for reading objects in Active Directory are the same as those of the Exchange server. Exchange System Manager runs in the security context of the user that is currently logged on. If an administrator is running with lower security privileges than the Exchange server, it is possible that the query will show a subset of the actual results in the preview pane. The preview pane will show only those Active Directory objects that the administrator has permissions to read. When mail is sent to the query-based distribution groups, however, the categorizer will run with the Exchange server permissions. Assuming the Exchange server has permissions for all the objects in the query, the query will return the correct results.

There will be issues when a base distinguished name is deleted. Query-based distribution expansion relies on its base distinguished name referring to a valid container in the directory. If the base distinguished name container for a query-based distribution group is deleted, the categorizer cannot run the query, and the sender receives an NDR with the code 5.2.4. If categorizer logging is enabled, an event ID of 6024 or 6025 is logged. For example, you create a sales container within the users container for all sales employees and build a query-based distribution group using the sales container. If you delete the sales container, the query will no longer work.

Creating Query-Based Distribution Groups

To create a query-based distribution group, you must use the Exchange 2003 version of Exchange System Manager and Active Directory Users and Computers. You cannot create query-based distribution groups without upgrading your administration console.

Note
It is recommended that you upgrade all of your administrative consoles to Exchange 2003 before you deploy query-based distribution groups in your environment.

When creating a query-based distribution group, Active Directory Users and Computers provides a way to format the LDAP query using standard attributes, without requiring specific knowledge of LDAP. For example, you can select all mailboxes under the organizational unit, or even customize the query to select all mailboxes under an organizational unit that exist on a particular server.

After you create a query-based distribution group, you can ensure that your query works the way that you intended it to work by using the preview feature. This feature is useful not only for query validation, but also to determine how long it takes a query to run. Based on this time, you can decide whether or not to divide the query into smaller queries for better performance and faster delivery times.
To create a query-based distribution group

1. In Active Directory Users and Computers, in the console tree, right-click the container where you want to create the query-based distribution group, point to New, and then click Query-based Distribution Group.

2. In Query-based Distribution Group name, type a name for the query-based distribution group, and then click Next.

3. Under Apply filter to recipients in and below, verify that the parent container shown is the one that you want the query-based distribution group to be run against. If this is not the correct container, click Change to select another container.

   \[\textbf{Note}\]
   The query returns only recipients in the selected container and its child containers. To achieve the results that you want, you may need to select a parent container or create multiple queries.

4. Under Filter, select one of the following options:
   - To filter the query based on a set of predefined criteria, click Include in this query-based distribution group, and then select from the following criteria:
     - Users with Exchange mailboxes
     - Users with external e-mail addresses
     - Groups that are mail-enabled
     - Contacts with external e-mail addresses
     - Public folders that are mail-enabled
   - To create your own criteria for the query, click Customize filter, and then click Customize.

5. Click Next to see a summary of the query-based distribution group that you are about to create.

6. Click Finish to create the query-based distribution group.

   The new query-based distribution group appears underneath the container that you selected in Step 3.

To verify that a query-based distribution group works correctly

1. In Active Directory Users and Computers, right-click the query-based distribution group that you just created, and then click Properties.

2. Select the Preview tab to view the query results, and verify that the correct recipients are included in the distribution group.

   \[\textbf{Note}\]
   The results that are displayed in the preview pane may vary from the actual results when the query is run, depending on permissions settings.
Combining Multiple Query-Based Distribution Groups

In Exchange System Manager, you can create query-based distribution groups based on the **AND** operator. To create distribution groups based on the **OR** operator using query-based distribution groups, create multiple query-based distribution groups and combine them in a single distribution group.

Consider the following example, in which you want to create a query-based distribution group that includes all employees in the marketing department or all employees in the Paris office. If you create a query-based distribution group using an LDAP query that contains all marketing users and all Paris employees, this query returns only those users who are in both groups. Anyone who is not a member of both groups is excluded. To achieve **OR** functionality, and thereby include members of either group, you need to do the following:

1. Create a query-based distribution group for all employees in the marketing department, called Marketing.
2. Create a query-based distribution group for all employees in the Paris office, called Paris employees.
3. Create a distribution group (not a query-based distribution group, however) and add the query-based distribution groups, Marketing and Paris employees, as members of this group.

When you add query-based distribution groups as members of a distribution group, you cannot do so in the same way that you add users to a group. You must right-click the group, and then select **Add Exchange query-based distribution group**. The following procedure describes in detail the process of adding query-based distribution groups as members of a standard distribution group.

**To add query-based distribution groups as members of a distribution group**

1. In Active Directory Users and Computers, in the console tree, navigate to the container where the distribution group resides, right-click the distribution list, and then click **Add Exchange Query-based Distribution Groups**.
2. In **Select Exchange Query-based Distribution Groups**, under **Enter the object names to select**, enter the name of the query-based distribution group that you want to add as a member of this group.
3. Click **Check Names** to verify the entry.
4. Click **OK**.
5. Repeat Steps 1 through 4 for each query-based distribution group to be added as a member of this distribution group.

---

**Managing Recipients**

Managing recipients involves assigning e-mail addresses to recipients with recipient policies, and managing settings for recipient objects with Active Directory Users and Computers.

---

**Notes for Exchange 5.5 Administrators**

If you have servers running Exchange 5.5 in your Exchange 2003 organization (that is, your organization is in mixed mode), it is still possible to manage recipients using the Exchange 5.5 Administrator Program, and it is recommended that you do so, with the exception of moving mailboxes. When you move mailboxes, use Exchange 2003 System Manager or Active Directory Users and Computers, where Exchange 2003 System Management tools have been installed.

**Note**

Before you use Active Directory Users and Computers to move recipients from Exchange 5.5, you must first create a connection agreement between each Exchange 5.5 site and Active Directory. It is strongly recommended that all objects in your Exchange 5.5 directory be represented in Active Directory before you deploy your first Exchange 2003 or Exchange 2000 server. This greatly reduces the risk of future problems. For more information about planning connection agreements, see Chapter 4, "Migrating from Exchange Server 5.5," in the book *Exchange Server 2003 Deployment Guide* ([http://www.microsoft.com/exchange/library](http://www.microsoft.com/exchange/library)).

Exchange objects in Exchange 2003 are different from the Exchange objects in Exchange 5.5. It is important to understand how these objects have changed. Table 4.6 associates the Exchange objects in Exchange 5.5 with their equivalents in Exchange 2003.
### Table 4.6 Terminology differences between Exchange 5.5 and Exchange 2003

<table>
<thead>
<tr>
<th>Exchange 5.5 term</th>
<th>Exchange 2003 equivalent term</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mailbox</strong></td>
<td><strong>Mailbox-enabled user</strong></td>
</tr>
<tr>
<td></td>
<td>When a user is mailbox-enabled, the user has an e-mail address and a corresponding mailbox. Mailbox-enabled users can send, receive, and store e-mail messages within an Exchange organization.</td>
</tr>
<tr>
<td><strong>Custom recipient</strong></td>
<td><strong>Mail-enabled user</strong></td>
</tr>
<tr>
<td></td>
<td>When a user is mail-enabled, they have an associated e-mail address external to the Exchange organization, but they do not have an associated Exchange mailbox. Mail-enabled users can receive messages at a specified external address, but they cannot store messages on Exchange servers in your organization.</td>
</tr>
<tr>
<td></td>
<td>—or—</td>
</tr>
<tr>
<td></td>
<td><strong>Mail-enabled contact</strong></td>
</tr>
<tr>
<td></td>
<td>A mail-enabled contact does not have a Windows logon account or a mailbox. A contact can represent someone outside of the Exchange organization, such as a customer or a business partner.</td>
</tr>
<tr>
<td><strong>Distribution list</strong></td>
<td><strong>Mail-enabled group</strong></td>
</tr>
<tr>
<td></td>
<td>E-mail messages that are sent to a group are routed to the e-mail address of each group member.</td>
</tr>
</tbody>
</table>

### Managing Recipients with Recipient Policies

When Exchange is installed, a default recipient policy is created that applies SMTP and X.400 addresses to all recipients in your Exchange organization. You can modify the default policy or create new policies. However, you cannot delete the default policy. All recipients in an Exchange organization must have both SMTP and X.400 addresses.
Chapter 4: Managing Recipients and Recipient Policies

The default policy is always set to the lowest priority. Priority determines the order in which policies are applied to the recipients specified in the policy. Priority 1 represents the first policy to be applied. In mixed mode, where servers running Exchange 2003 or Exchange 2000 coexist with servers running Exchange 5.5, the Site policy has a priority of highest and is the only policy that Exchange applies, regardless of any other policies that you create. You can reorder recipient policies at any time, with the exception of the default policy, which is always set to lowest.

**Note**
The default policy is special in the sense that every user in the organization must be stamped with the same proxy address, so that users can take advantage of features like Outlook Web Access, Outlook Mobile Access, and Exchange ActiveSync®.

Creating a Recipient Policy

To begin the process of creating a recipient policy, right-click the *Recipient Policies* container in Exchange System Manager, point to *New*, and then click *Recipient Policy* (see Figure 4.8).

![Figure 4.8 Creating a new recipient policy](image-url)
After you click **Recipient Policy**, you then begin the process of completing the steps that are outlined in the following checklist and described in the following sections.

**Recipient Policy Checklist**
- Select the property sheets (e-mail address or Mailbox Manager settings).
- Name the new policy.
- Create a filter.
- Configure the settings.
- Set the priority of the policy.
- Apply the policy.

**Select the Property Sheets**
The first step in creating a recipient policy is to choose the type of policy to create. A single recipient policy can contain an address policy, a Mailbox Manager policy, or both (see Figure 4.9). Selecting both will add property pages for both address and Mailbox Manager features to one recipient policy.

![Figure 4.9 Selecting property pages for a new policy](image-url)
Name the New Policy

After you select the property pages, give the new policy a name. To help you identify the recipients to which the policy applies, give the policy a descriptive name.

Create a Filter

Initially, there are no filter rules applied to the policy (see Figure 4.10). If you do not create a filter, the policy will not be applied to any recipients. To create the filter using an LDAP query, click Modify on the General tab.

Figure 4.10  Policy does not apply to anyone because no filter rules are set
Configure the Settings
To customize the recipient policy, switch to either the **E-Mail Addresses (Policy)** tab or the **Mailbox Manager Settings (Policy)** tab in the policy's **Properties** dialog box. Use the settings on these tabs to configure the recipient policy to meet the needs of the associated recipients. After configuring the settings, click **OK** to create the policy.

Set the Priority and Apply the Policy
After you create a new recipient policy, the policy and its assigned priority appear in Exchange System Manager. If you want to change the priority of a recipient policy, right-click the policy, select **All Tasks**, and then move the policy up or down the list of recipient policies shown in Exchange System Manager.

After you create a new recipient policy, you also need to apply the policy by right-clicking the policy in Exchange System Manager, and then clicking **Apply Policy Now**.

Managing Recipient Settings
Some recipient settings are configured in Exchange System Manager, so that they are applied to all recipients in an organization or to large groups of recipients. Examples include mailbox size (which can be set on a per-store basis), global send and receive limits, and limits on the maximum number of recipients to which users can send. You can configure exceptions to these settings for individual recipients in Active Directory Users and Computers. For example, you may have a user who needs a larger mailbox, or one who needs to be able to send large messages.

For information about using Exchange System Manager to set message settings for an entire organization, see Chapter 2, "Managing an Exchange Organization." For information about setting mailbox size limits on mailbox stores, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores."

The following sections explain three of the four Exchange-specific tabs that you see in Active Directory Users and Computers, where Exchange system tools have been installed. The fourth tab, Exchange Features, is discussed in Chapter 6, "Managing Client Access to Exchange."
Configuring Message Settings for Mailbox-Enabled Recipients

To set individual message settings for mailbox-enabled recipients, start by navigating to the Exchange General tab (see Figure 4.11).

Figure 4.11   Exchange General tab

To navigate to the Exchange General tab

1. In Active Directory Users and Computers, right-click the object to be modified, and then click Properties.
2. Click the Exchange General tab.
Delivery Restrictions

To maintain system performance and to prevent users from wasting valuable system resources by sending large files through your e-mail infrastructure, message size limits are set at the global level in Exchange System Manager, as explained in Chapter 2, "Managing an Exchange Organization." In most cases, e-mail messages for legitimate business purposes can be sent under the threshold set at the global level. Use the Delivery Restrictions dialog box to override the global setting for those users who have special requirements and need to send larger files than the global limit allows.

Tip
Consider setting up users who need to transfer large files with an FTP account, instead of trying to use your Exchange server as though it were an FTP server.

In addition to setting message size limits, you can use the Delivery Restrictions dialog box to specify to whom users can send messages and from whom they can receive messages (see Figure 4.12). This is similar to the global setting.

Important
When you make these changes for individuals, you can only set restrictions that reference other Active Directory objects. Blocking mail from a specific Internet mail source or IP address must be done at the global level.

Figure 4.12   Delivery Restrictions dialog box

You can further restrict delivery of messages to recipients by selecting the From authenticated users only check box. This prevents anyone who is not authenticated by your Windows network
from sending mail to this recipient. Selecting this check box effectively stops all Internet mail to this recipient. After selecting this check box, select how messages will further be restricted by choosing to allow messages from everyone (all authenticated users), only from users in the restricted list at the bottom of the **Delivery Restrictions** dialog box, or from everyone except users in the restricted list. To add users to the restricted list, use the **Add** button.

### Delivery Options

One delivery option is the use of delegates. In many organizations, delegates are given permission to send mail on behalf of someone else. For example, an administrative assistant may send a meeting request on behalf of a manager. You can assign delegates to a mailbox-enabled user in the **Delivery Options** dialog box.

Another delivery option is address forwarding, wherein mail sent to the user is forwarded to another address in the organization. You can also choose to have copies of the message sent to both the forwarding address and the user’s mailbox. In this case, deleting one copy of the message does not delete the other. You may want to use forwarding to protect the identity of the actual recipient, or for administrative assistants who help sort e-mail messages for others.

Recipient limits control the number of recipients to which a user can send a single message. By default, there is no set limit.

### Storage Limits

Individuals in your organization may need more storage space on their Exchange servers than the threshold for the mailbox store allows. You can set storage limits for individual users in the **Storage Limits** dialog box. Users can be warned as they approach the limit, subsequently denied the ability to send, and then denied the ability to send and receive mail.

Also, you can override the setting for deleted item retention that is set on the mailbox store. When a user deletes an item, it appears deleted to the user. However, a copy is kept in the user's mailbox store for a specified amount of time, allowing the item to be recovered if it was unintentionally deleted. Some users in your organization may need extra recovery protection, and you can override the setting in the **Storage Limits** dialog box. If you choose to override the limit set on the mailbox store, you will also have the choice to not permanently delete an item until the store is backed up, adding even greater recovery opportunities for that user.

### Exchange Advanced Settings for Mailbox-Enabled Recipients

Navigate to the **Exchange Advanced** tab to change advanced settings for mailbox-enabled recipients.
To navigate to the Exchange Advanced tab

1. In Active Directory Users and Computers, right-click the object that you want to modify, and then click Properties.

2. On the Exchange Advanced tab (see Figure 4.13), select the following options:
   - In Simple display name, set a display name that will be used by systems that cannot interpret all of the characters in the normal display name.
     This situation may occur when more than one language version of Exchange System Manager is used to manage an Exchange organization. For example, the English version of Exchange System Manager cannot display all of the characters in the Kanji character set. Because the simple display name takes ASCII characters only, all versions of Exchange System Manager are able to display the simple display name.
   - To prevent the recipient from being displayed in address lists, select Hide from Exchange address lists.
   - To prevent the recipient from sending mail that is marked high priority to an X.400 mail system, select Downgrade high priority mail bound for X.400.

Figure 4.13   Exchange Advanced tab
Setting Custom Attributes

Using the Custom Attributes button on the Exchange Advanced tab, you can assign up to 15 custom values for a recipient. By default, recipients have attributes such as phone number, office number, or manager. If there is information that you would like to display in the GAL that does not fit in any of the existing attributes, you can create up to 15 other entries. For example, you may want to include an attribute for the divisions or cost centers of your company.

Assigning Mailbox Rights

Using the Mailbox Rights button on the Exchange Advanced tab, you can assign rights to the mailbox of a recipient to users or to groups, add users to the list, and then allow or deny them the following rights:

- **Delete mailbox storage**  The mailbox from the mailbox store can be deleted. By default, only administrators have permission to do this. Users cannot delete their own mailboxes.
- **Read permissions**  The specified user can read the contents of a mailbox.
- **Change permissions**  The user can modify or delete items in the mailbox.
- **Take ownership**  The user is granted ownership of a mailbox.
- **Full mailbox access**  The delegated user has the same access rights as the owner.
- **Associated external account**  This option is used when a user's Windows account resides in a different forest than the Exchange mailbox.

**Note**

Each Exchange mailbox must be associated with an Active Directory object, such as a user, in the same forest as the mailbox. If the intended user account resides outside of the forest where Exchange is, Exchange first associates the mailbox with an account in its same Active Directory forest. That account is disabled. Then, the mailbox is associated with the external account.

- **Special permissions**  Click Advanced to work more granularly with permissions, including changing inheritance.
You assign these rights on the **Mailbox Rights** tab in the user's **Permissions** dialog box (see Figure 4.14).

![Permissions for Chris Meyer](image)

**Figure 4.14 Assigning rights to read another user's mailbox**
Configuring Message Settings for Mail-Enabled Recipients

When you need to set individual message settings for mail-enabled recipients, start by navigating to the Exchange General tab for that recipient (see Figure 4.15).

![Exchange General tab for mail-enabled recipients](image)

Figure 4.15  Exchange General tab for mail-enabled recipients
The **Exchange General** tab for mail-enabled recipients is slightly different than that for mailbox-enabled recipients. It has fewer features, omitting those features that apply only to mailbox-enabled users. For more information, see "Configuring Message Settings for Mailbox-Enabled Recipients" earlier in this chapter.

The **Exchange Advanced** tab adds one option that is not included for mailbox-enabled users, **Use MAPI Rich Text Format (RTF)**. When you select this option, mail sent to this recipient will be sent using MAPI RTF, overriding the settings configured in **Internet Message Formats** in Exchange System Manager. Select this option only if you are sure that the recipient can view MAPI-rich text.

### Distribution Groups

Distribution groups are similar to other mail-enabled recipients, but they have the following unique features on the **Exchange Advanced** tab (see Figure 4.16):

- **Expansion server**  Use the Expansion server drop-down list to select the server where the group is expanded. If this is set to any server in the organization, the group is expanded on the first Exchange server in your organization that receives the message. For more information about expansion servers, see "Expanding Mail-Enabled Groups" earlier in this chapter.

- **Hide group from Exchange address lists**  Select this check box to prevent this distribution group from appearing in the GAL or any other address list. You may want to do this for groups that you do not want everyone in the company to know about. For example, you may have a team of auditors who are investigating unethical business practices. You may not want to show that such a group exists.

- **Send out-of-office messages to originator**  When someone sends a message to a group, by default, out-of-office messages are not sent to the sender. Select this check box to enable out-of-office replies from group members. For large groups, out-of-office replies may be unnecessary. For example, if the chief security officer of a company sends mail describing new security policies to a group called All Fulltime Employees, out-of-office replies are not needed.

- **Delivery reports for groups**  Delivery reports warn about delayed or failed delivery of messages. Choose to send delivery reports to either the owner of the group, the sender of the message, or not at all.
Understanding Address Lists

When users connect to Exchange with a client, such as Outlook 2003, they expect to communicate with other people in the organization easily. Users need to do more than simply compose e-mail messages with their messaging client. Whether they want to send an e-mail message, call a coworker, look up an office number, or schedule a meeting, they need to find information about another recipient quickly. Address lists help you to organize this type of information in a meaningful way.
Address Lists Described

An address list organizes recipients so that they can be easily found by users who want to contact them.

The most familiar address list is the global address list (GAL). By default, the GAL contains all recipients within an Exchange organization. In other words, any mailbox-enabled or mail-enabled object in an Active Directory forest where Exchange 2003 is installed is listed in the GAL. To look up the e-mail address or phone number of a recipient, the user can use the GAL to locate this information. The GAL is organized by name, rather than e-mail addresses, for ease of use.

Client applications, such as Outlook 2003, display the available address lists that Exchange provides (see Figure 4.17). Users choose from the available address lists when they search for information. Several address lists, such as the GAL, are created by default. Address lists reside in Active Directory, so mobile users who disconnect from the network are also disconnected from these (server-side) address lists. However, offline address lists can be created for use in a disconnected environment. These offline lists can be downloaded to a user's hard drive. Often, to conserve resources, the offline lists are subsets of the information in the actual address lists that reside on your servers.

Figure 4.17  Address lists displayed in Outlook 2003
An Exchange organization can contain thousands of recipients. Compiling all of your users, contacts, mail-enabled groups, and other recipients can result in many entries. As an administrator, you can create address lists to help users in your organization find what they are looking for more easily.

For example, consider a company that has two large divisions and one Exchange organization. One division, called Fourth Coffee, imports and sells coffee beans while the other, Contoso, Ltd, underwrites insurance policies. For most day-to-day activities, the workers in the coffee division have little to do with those in the insurance division. To make it easier for people to find each other, you create two new address lists—one for Fourth Coffee and one for Contoso. Users can now choose to use the smaller address lists when looking up people in a certain division, or they can always use the GAL, if they are not sure which division a coworker is part of.

Address lists can be sorted by any attribute that is associated with a recipient. City, title, company, office building, or any other attribute that you can filter recipients with can be the basis for a new address list.

You can also create subcategories of address lists. For example, you could create an address list for everyone in Manchester and another for everyone in Stuttgart. You could then create an address list under Manchester for everyone who works in research and development. Because the research and development list is under the Manchester list, the research and development list contains only those recipients who are in research and development and in Manchester.

Address lists are created dynamically. When new users are added to your organization, they are automatically added to all of the appropriate address lists. These updates are one of the primary responsibilities of both the Recipient Update Service and Exchange System Attendant.

Creating Address Lists

Address lists can be useful tools for users, but poorly planned address lists can be frustrating. Before you create address lists, make sure that they will make sense to users. Avoid creating so many address lists that users are unsure where to go to find a recipient. If possible, consider surveying users to find out how they would interpret your proposed address lists. Finally, be sure to name your address lists in such a way that when users glance at them, they know immediately whom they can expect to find. When in doubt, have fewer address lists, and remind users that they can find anyone in your organization by using the global address list.
When you are planning your address lists, consider whether to use subcategories. For example, you may want address lists for both city and state, with city being a subcategory of state (see Figure 4.18). Notice that both New York and Washington have cities named Auburn. When the query for Auburn, New York runs, it first finds all recipients with the state attribute New York, and then queries the result list (all recipients in New York) for all recipients in Auburn. In this way, you get different lists for Auburn, New York and Auburn, Washington.
To further simplify the user experience and help organize your lists, you may want to create an empty address list. Because no query has been created for an empty address list, it returns no recipients, and serves strictly as a parent container that organizes other lists. In the preceding example, you may create an empty address list called States (see Figure 4.19).

Figure 4.19 Adding an empty address list
To create an address list

1. In Exchange System Manager, expand the **Recipients** container.

2. Expand **All Address Lists**, right-click the node that the new list belongs in, point to **New**, and then click **Address List**.

3. On the **Create Exchange Address List** page (see Figure 4.20), name your new address list, and then modify the filter rules appropriately.

![Create Exchange Address List screenshot](image)

**Figure 4.20 Creating an Exchange address list**

You can move address lists to create a new hierarchy, using a drag-and-drop operation. As explained in "Managing Recipient Settings" earlier in this chapter, you can hide recipients from address lists using Active Directory Users and Computers.

### Offline Address Lists

MAPI clients such as Outlook 2003 can download offline address lists, so users can compose e-mail messages even when they are disconnected from their Exchange server. For clients to download these address lists, they must first be created on the server.

By default, there is an offline address list called the Default Offline Address List, which contains the global address list. If necessary, you can populate this list with any other address list that you have created. You can also create multiple offline address lists that can be individually associated with each mailbox store in your organization. If the users on your different mailbox stores share something in common, such as all being part of the same division, providing different offline address lists for each mailbox store may make sense.
At any time, you can set any offline address list in your Exchange organization as the default offline address list. This new default list is then associated with all newly created mailbox stores. There can be only one default list at a time in your Exchange organization. If you delete the current default list, Exchange does not automatically assign another list as the default. If you want to use a default list after you delete the existing default list, you must manually designate another offline address list as the default.

**To populate the default offline address list**

1. In Exchange System Manager, click the **Offline Address Lists** container, and then right-click **Default Offline Address List**.

2. In the **Default Offline Address List Properties** dialog box (see Figure 4.21), click **Add** to add any address list that you have created. You can add as many address lists as you require. Click **OK**.

![Figure 4.21  Default Offline Address List Properties dialog box](image)
Offline address lists use system public folders to contain the necessary address list information. Their associated public folders are created during the public store maintenance interval, and the content of the public folder is updated according to the **Update interval** that you specify on the **Properties** dialog box of each offline address list. The Offline Address List (System) public folders are hidden from users by default.

**To see the System public folders**

1. In Exchange System Manager, expand the administrative group, and then expand the folders container.

2. Right-click the **Public Folders** container, and then click **View System Folders**.

In a mixed environment where some users connect to Exchange 2003 or Exchange 2000 servers, and others connect to Exchange 5.5 servers, you need multiple address lists. Those users who connect to Exchange 5.5 need to use the offline address book that is generated by that version of Exchange.

### Customizing the Details Templates

Details templates control the appearance of object properties that are accessed by using address lists in both MS-DOS 16-bit and MAPI 32-bit client applications. When a user opens an address list in Outlook, for example, the properties of a particular object are presented as defined by the details template in the Exchange organization. You can use the default details template shown in Figure 4.22, or you can customize the template to better suit the needs of your users.

![Figure 4.22 Default details template as viewed from Outlook 2003](image)
To customize the details template

1. In Exchange System Manager, expand the **Recipients** container, and then select the language for the template that you want to modify.
   
   For example, the English language has been selected in Figure 4.23.

![Exchange System Manager](image)

**Figure 4.23** Selecting English

The following languages are supported:

- Arabic, Basque, Brazilian, Bulgarian, Catalan, Chinese Simplified, Chinese Traditional, Croatian, Czech, Danish, Dutch, German, Greek, English, Estonian, Finnish, French, Hebrew, Hungarian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, and Ukrainian.

Other languages may be supported by the client, but they will not be able to display the **Properties** pages.

2. In the list of templates displayed in the right-pane, right-click the template to be changed, and then click **Properties**.
3. On the Templates tab, resize fields, add or remove fields, add and remove tabs, and rearrange the order of the fields (see Figure 4.24).

![Figure 4.24  Modifying the user details template](Image)

4. To see how the changes you made affect the template, click Test. To revert to the original template, click Original.

# Recipient Update Service

Exchange uses the Recipient Update Service primarily to generate and update default and customized address lists, and to process changes made to recipient policies. This service ensures that when new recipient policies or address lists are created, their content is applied to the appropriate recipients in the organization. The Recipient Update Service also applies existing policies to new recipients that are created after the policy or address list has already been established. In this way, information is kept current with minimal administrative overhead.

You must have at least one Recipient Update Service for each domain in your organization, and it must be run from an Exchange 2003 or Exchange 2000 server. For domains that do not have these Exchange servers, the Recipient Update Service must be run from an Exchange server outside of the domain. You can set up more than one Recipient Update Service for a domain, if
there are multiple domain controllers. Each Recipient Update Service must read from and write to a unique domain controller.

**Note**
If you do not have a Recipient Update Service for a domain, you cannot create recipients in that domain.

In situations where you have high network latency within a domain, set up the Recipient Update Service at the local sites. For example, if you have one domain that has sites in Seattle and in Beijing, there could be a long delay before a mailbox that an administrator creates in Beijing is processed by the Recipient Update Service in Seattle. In this case, having a Recipient Update Service on the local domain controller in Beijing will decrease the time the user has to wait to be able to access the mailbox after it has been created.

**To create a new Recipient Update Service**

1. In Exchange System Manager, expand the **Recipients** container.

2. Right-click the **Recipient Update Service** container, point to **New**, and then click **Recipient Update Service**.

The Recipient Update Service Wizard starts and guides you through the creation process. Figure 4.25 shows the final step in the creation process.

![Figure 4.25 The final step in creating a Recipient Update Service](image)

**Note**
If all of the domain controllers are currently associated with a Recipient Update Service, you receive an error when you try to create the next Recipient Update Service. You can have only one Recipient Update Service per domain controller.
You can choose to have the Recipient Update Service run at customized intervals. By default, the Recipient Update Service is set to **Always Run**, and when it runs, only necessary changes are made. Changes are necessary when a recipient, recipient policy, or address list is changed or created. Any changes that have occurred since the last time the Recipient Update Service ran are applied.

**To change the update interval**

- Right-click the Recipient Update Service to be modified, click **Properties**, and then change the **Update interval** option.
Together, message routing and transport are responsible for message delivery internally and externally. Message routing is the way that messages flow between servers within the organization and to other servers outside of the organization. Your routing topology, based on the routing groups and connectors you define, dictates the path these messages take to reach their final destination. Transport determines the way that messages are delivered.

Simple Mail Transfer Protocol (SMTP) is the transport protocol that Exchange servers use to communicate with each other and send messages using the routing topology. SMTP is part of the Microsoft® Windows Server™ 2003 or Microsoft Windows® 2000 Server operating system. When you install Microsoft Exchange on a server running Windows Server 2003 or Windows 2000 Server, Exchange extends SMTP to support additional SMTP commands for additional functionality. This functionality includes the ability to communicate the link state status, available messaging routes status, and other Exchange functionality.

Configuring Routing for Internal Mail Flow

Because routing is the path messages travel from a sender to a recipient, a well-planned routing topology is essential for efficient mail flow within your Exchange organization. You should carefully evaluate your existing network infrastructure, before you plan your routing topology.

Note
Although this section focuses on the components of your routing topology and how they affect message flow within your organization, it does not discuss all of the planning considerations and various routing topologies in detail. For information about planning your routing topology, see the book Planning an Exchange 2003 Messaging System (http://www.microsoft.com/exchange/library).

In its default state, Exchange Server 2003, like Exchange 2000 Server, functions as though all servers in an organization are part of a single, large routing group. That is, any Exchange server can send mail directly to any other Exchange server within the organization. However, in environments with varying network connectivity and geographical distribution, you can increase
message flow efficiency by creating routing groups and routing group connectors in accordance with your network infrastructure. By creating routing groups and routing group connectors, servers within a routing group still send messages directly to each other, but they use the routing group connector on those servers with the best network connectivity to communicate with servers in another group.

This section discusses what routing groups are, as well as how to create and configure routing groups and routing group connectors to manage internal mail flow. Then, because network topologies and environments change, this section also covers how to make adjustments to your routing topology, such as moving servers between routing groups, renaming routing groups, and deleting routing groups.

**Note**

If you are operating Exchange on a single server, most of the topics about routing groups do not apply to your organization. However, you may find these topics useful if you are planning to expand your messaging system to support multiple servers.

### Understanding Routing Groups

A routing group is a collection of servers connected by high-bandwidth, reliable network connections, such as a local area network (LAN). Within a routing group, all servers communicate and transfer messages directly to one another, as follows:

1. A user in your Exchange organization uses a mail client to send mail to another user.
2. Using SMTP, the sender's client submits this mail to the SMTP virtual server on the Exchange server on which the client's mailbox resides.
3. The Exchange server looks up the recipient of the mail message to determine which server the recipient's mailbox resides on.
4. One of two things happens:
   - If the recipient's mailbox is on the same Exchange server, Exchange delivers the message to the recipient's mailbox.
   - If the recipient's mailbox is on another Exchange server, the first Exchange server sends the message to the recipient's home mailbox server, and it is the recipient's home mailbox server that delivers the message to the recipient's mailbox.

Although all servers communicate with each other directly within a routing group, this is not the case when a server in one routing group needs to communicate with a server in another routing group. To allow servers to communicate with servers in other routing groups, you need to create a routing group connector. Although you can use an X.400 connector or an SMTP connector to connect routing groups, the routing group connector is specifically designed for this purpose and is the preferred method of connecting routing groups.
By default, all servers within a routing group can send mail over the routing group connector. Servers that are capable of sending mail over a routing group connector are *bridgehead servers*. These bridgehead servers are each a combination of an SMTP virtual server and an Exchange server responsible for delivering all messages through a connector.

When creating a routing group connector, you have the option of keeping all the servers as bridgehead servers for that connector or of specifying that only a selected set of servers act as bridgehead servers for that connector. Table 5.1 compares the advantages of each approach.

**Table 5.1 Number of bridgehead servers in a routing group**

<table>
<thead>
<tr>
<th>Number of bridgehead servers</th>
<th>Advantages</th>
</tr>
</thead>
</table>
| All servers in a routing group | • Provides more efficient message flow because all of the servers in the routing group can directly deliver messages to other routing groups.  
• Capitalizes on those configurations where all of the servers in a routing group have the same network connectivity to the servers in other routing groups. |
| Only a select few servers in a routing group | • Makes troubleshooting message flow easier because there are limited points of contact between routing groups.  
• Distributes messaging if you anticipate heavy message flow between routing groups.  
• Makes mail flow more reliable and efficient in those configurations where some servers have better network connectivity than others. |

Figure 5.1 illustrates the basic components of routing discussed thus far. Figure 5.1 shows message flow between servers within a routing group and between routing groups. It also illustrates a topology that uses only a single bridgehead server in each routing group.
When a topology is as simple as that shown in Figure 5.1, you do not have to consider how to best route messages between routing groups. As topologies become more complex, with large numbers of routing groups spread over varying geographical distances, message routing among groups becomes critical. You configure routing among routing groups by assigning costs to the routing group connectors used by these groups. When a user on a server in one routing group sends mail to a user on a server in another routing group, Exchange uses these costs (part of the link state information maintained by Exchange) to determine the most efficient route. Exchange always uses the route with the lowest cost unless a connector or server in that route is unavailable. So that every routing group knows what the various costs are for each connector and the status of those connectors, each routing group has a routing group master that updates and coordinates this information with all of the other servers in a routing group.

Understanding Link State Information

Exchange 2003, like Exchange 2000, uses link state information to determine the most effective route for delivering messages. The link state table contains information about the routing topology and whether each connector within the topology is available or unavailable. Additionally, the link state table contains costs associated with each available connector. Exchange uses this information to determine the route with the lowest cost. If a connector along the lowest cost route is unavailable, Exchange determines the best alternate route, based on cost and connector availability.

To understand how link state information and connector costs work, consider the routing topology shown in Figure 5.2, in which four routing groups exist: Seattle, Brussels, London, and Tokyo. The connectors exist between each routing group and are assigned costs based on the network speed and available bandwidth.

If all connections between the routing groups are available, a server in the Seattle routing group always sends a message to the Brussels routing group by sending the message first through the London routing group. This route has a cost of 20, the lowest cost route available. But, if the
bridgehead server in London is unavailable, messages originating in Seattle and destined for Brussels travel over the higher cost route, the one that goes through the Tokyo routing group.

**Understanding Routing Group Masters**

When you create a routing group, the first server in that routing group is assigned the role of *routing group master*. The routing group master keeps track of the link state information and propagates it to the other servers within the routing group, and other servers communicate back any changes in link state. For example, if a member server tries to contact another server over a connector, and this link is unavailable, the member server immediately notifies the routing group master. Likewise, when a non-master receives new link state information, it immediately transfers the link state information to the master, so that other servers can receive the information about the routing change.

Within a routing group, the routing group master and the other Exchange servers communicate link state information over TCP/IP port 691 using SMTP. However, communication of link state information between routing groups is different. If the routing group master is not a bridgehead server for the routing group, the routing group master sends the link state information to the group's bridgehead server over TCP/IP port 691. The bridgehead server then forwards this information (over TCP/IP port 25 using SMTP) to the bridgehead servers of other routing groups.

If you do not want the first server installed in the routing group to be the routing group master (the default setting), you can change the routing group master to another server using the following procedure.

**To change which server is the routing group master**

- In Exchange System Manager, expand the routing group, click *Members*, right-click the server, and then select *Set as Master*.

**Important**

There is no automatic failover for routing group masters. If a routing group master fails, you must manually configure a new routing group master in Exchange System Manager. If a routing group master fails, the other servers in the routing group use the last known link state information until a routing group master becomes available or another routing group master is designated.

**Using Routing Groups in Native and Mixed Modes**

In Exchange 2003 and Exchange 2000, the administrative and routing functions are split into different units:

- Administrative groups define the logical administrative boundary for Exchange servers.
- Routing groups define the physical routes that messages travel over the network.

If your Exchange organization is in native mode, where all servers are running Exchange 2000 or later, this split between administrative groups and routing groups enables you to create routing
groups that span administrative groups, and move servers between routing groups that exist in different administrative groups. This functionality also allows you to separate routing and administrative functions. For example, you can administer servers in two central administrative groups, placing servers from each administrative group in different routing groups, based on your network topology.

However, the functionality of routing groups in mixed mode, where some servers are running Exchange 2003 or Exchange 2000 while others are running Exchange 5.5, is different than in native mode. In mixed mode, you:

- Cannot have a routing group that spans multiple administrative groups.
- Cannot move servers between routing groups that exist in different administrative groups.

This is because the routing topology in Exchange 5.5 is defined by sites—logical combinations of servers connected by a high-bandwidth reliable network. Sites provide the functionality of both the administrative group and routing group in Exchange 2003 and Exchange 2000. This difference in routing topology limits routing groups in mixed mode.

**Note**
For more information about native and mixed mode Exchange organizations, see Chapter 2, "Managing an Exchange Organization."

## Creating Routing Groups

By design, Exchange functions as though all servers are connected by high-speed reliable networks. When your servers do not share this type of network connectivity, you can group servers with reliable network connectivity into routing groups to enable Exchange to maximize message flow efficiency.

By default, all servers in a native-mode Exchange organization are placed in a single routing group, called First Routing Group, and these servers communicate directly with one another. In mixed mode (where some servers are running Exchange 5.5 or earlier), each Exchange 5.5 site becomes a routing group.

**Note**
To understand the difference between routing groups in mixed and native mode, see "Using Routing Groups in Native and Mixed Modes” earlier in this chapter.

After installation, you can create additional routing groups in your Exchange organization. When you install additional Exchange servers into an existing organization, you can then designate the appropriate routing groups where these servers belong. After installation, you can also move servers between routing groups.
When you create a routing group, two containers display beneath the routing group:

- **Connectors** Displays any connectors installed on the servers within the routing group. This list includes any connectors to third-party mail systems, such as the Lotus Notes or Novell GroupWise connector, as well as any routing group connectors, X.400 connectors, and SMTP connectors that you configure.

- **Members** Displays the servers within this routing group. By default, the routing group master is the first server added to a routing group.

**Note**
Before you can create routing groups, you must configure your Exchange organization to display routing groups. In Exchange System Manager, right-click your Exchange organization, click Properties, and then select the Display routing groups check box.

**To create a routing group**

1. In Exchange System Manager, right-click Routing Groups, point to New, and then select Routing Group.

2. On the General tab (see Figure 5.3), in the Name box, enter a name for the routing group, and then click OK.

![Figure 5.3 General tab for routing group](image)
Moving Servers Between Routing Groups

As discussed earlier, you can only add a server to a routing group during installation. However, you can move servers between routing groups at any time. The capability to move servers between routing groups is useful if your network topology changes, and you need to combine servers with reliable connections into different routing groups. You may also need to move servers between routing groups if you are consolidating your physical sites and moving more servers into a central location.

In native mode, you can move servers between routing groups that exist in different administrative groups. In mixed mode, you can only move servers between routing groups within the same administrative group.

Note
You cannot move a server that is configured as the bridgehead server for any connectors. You must first designate a new bridgehead server, or remove the connectors before you can move the server.

To move servers between routing groups

1. In Exchange System Manager, expand the routing group that currently has the server to be moved, and then expand the Members folder within that routing group.

2. Expand the routing group that will be the new location for the server, and then expand the Members folder within that routing group.

3. In the Members folder of the routing group that currently has the server to be moved, do one of the following:
   - Select the server and drag it to the Members folder of the routing group that will be the new location for the server.
   - or —
   - Right-click the server, and then click Cut. In the Members folder of the routing group that will be the new location for the server, right-click, and then click Paste.

Renaming a Routing Group

If necessary, you can rename a routing group after it is created. You may need to rename a routing group if you are consolidating routing groups or expanding a routing group to include more regions, and want to change the name to reflect the new membership.
If any servers in a routing group are bridgehead servers for an X.400 connector, ensure that no messages are in the Exchange message transfer agent (MTA) queue. (Messages are submitted to this queue if they are destined for an X.400 system or an Exchange 5.5 server.) If messages are in the Exchange MTA queue when you rename a routing group, wait 15 minutes for Exchange to apply these changes, and then restart the Microsoft Exchange MTA Stacks service.

You can use Queue Viewer to verify that no messages are in the Exchange MTA queue. Figure 5.4 shows the Exchange MTA queue with no messages.

Note

Messages in other queues are not affected when you rename a routing group.

Figure 5.4 Exchange MTA queue in Queue Viewer

To rename a routing group

- In Exchange System Manager, right-click the routing group, click Rename, and then type a new name for the group.

Deleting a Routing Group

Before you can delete a routing group, you must move all member servers to another routing group. After you remove the servers from the routing group, you can delete the group.

To delete a routing group

- Right-click the routing group, and then click Delete.
Connecting Routing Groups

When you create a routing group, you designate a group of servers that can communicate directly with one another. As discussed earlier, for servers in different routing groups to communicate with each other, you need to connect the routing groups.

It is possible to connect routing groups with an SMTP connector or an X.400 connector. However, using these types of connectors is generally not recommended. The preferred connection method is a routing group connector because this connector is designed and intended specifically for connecting routing groups.

Routing group connectors are one-way routes for outgoing messages, which means messages travel outbound to the connected routing group. For two routing groups to communicate, a routing group connector must exist in each routing group to send messages outbound to the other routing group. When you create a connector to a routing group, Exchange displays a message asking if you want to create a routing group connector in the remote routing group so you can send messages from the remote routing group to the routing group where you are creating the first connector.

Before you create and configure a routing group connector, you should think about the following questions:

- **To which routing group does this connector deliver messages?** This information is critical. Identifying the routing group to which the connector delivers messages establishes the relationship between the sending and receiving routing groups and the rest of your topology. You need to know how the sending and receiving routing groups fit into your topology in order to intelligently assign a cost for the associated connector.

- **What cost should this connector have?** Cost is the variable Exchange uses to determine the most efficient messaging route. Exchange considers the lowest cost route the most efficient. Exchange uses a more expensive route only if a server or connector is unavailable on the route with the lowest cost. You should assign the lowest costs to the routes with the highest available network bandwidth.
- **Which servers in the routing group can act as bridgehead servers?** Only designated bridgehead servers can send messages across the connector to the connected routing group. The default and preferred setting is to have any of the servers in the local routing group send mail using this connector. Use this default option when all servers in the routing group can connect directly over the network to the remote bridgehead server. Connecting directly to the remote bridgehead servers provides more efficient message flow.

   However, you may have better direct network connectivity between specific servers in the local routing group and the designated remote bridgehead server. For example, Server A has a direct connection of 56 kilobits per second (Kbps) to a remote bridgehead server, while Server B and Server C each have a direct connection of 10 megabits per second (Mbps) to the same remote bridgehead server. In this case, you would want to specify the servers that have the better direct network connectivity (that is, Server B and Server C) as the bridgehead servers, and you would add those specific servers to a list of allowable bridgehead servers.

- **Should users access public folders that are not available locally using this connector?** By default, public folder referrals are enabled across connectors connecting routing groups. However, network traffic increases when users access a public folder in a remote routing group. If your routing groups are connected by slow network connectivity or if your network may not be able to handle the additional traffic, disable public folder referrals. For more information about public folder referrals, see "Understanding Public Folder Referrals" in Chapter 7, "Managing Mailbox Stores and Public Folder Stores."

- **What are the remote bridgehead servers to which this connector can send messages?** The remote bridgehead servers are the servers in the connected routing group that receive all messages destined for this routing group. The remote bridgehead servers also send link state information to the bridgehead servers for the connector.

After considering these questions, you answer the first four by setting the configurations options on the **General** tab in the **Routing Group Connector Properties** dialog box. You can answer the last question by specifying remote bridgehead servers on the **Remote Bridgehead** tab.
To configure the options for a routing group connector

1. In Exchange System Manager, expand the routing group, right-click **Connectors**, point to **New**, and then click **Routing Group Connector**.

2. On the **General** tab (see Figure 5.5), select from the following options:
   - For the name of the routing group connector, it is a common practice to use the two routing groups it connects. For example, you could use the name ParisToSeattle to define a connector connecting your Paris routing group to your Seattle routing group.
   - In **Connects this routing group with**, select the routing groups to which you want to connect.
   - In **Cost**, assign a cost for the connector.
   - To have all servers within the local routing group function as bridgehead servers, select **Any local server can send mail over this connector**.
   - To specify which servers within the local routing group can function as bridgehead servers for this connector, select **These servers can send mail over this connector**, and then click **Add** to add the appropriate servers to the list.
   - To prohibit users from accessing public folders that are not available locally using this connector, select **Do not allow public folder referrals**.

![Figure 5.5 General tab of the Routing Group Connector Properties dialog box](image-url)

Figure 5.5  General tab of the Routing Group Connector Properties dialog box
To specify a remote bridgehead server for a routing group connector

1. In the **Routing Group Connector Properties** dialog box, on the **Remote Bridgehead** tab (see Figure 5.6), click **Add**, and then select the remote bridgehead server from the list of servers in the routing group to which you are connecting.

   **Note**
   You must specify a remote bridgehead server. For redundancy, you should specify more than one remote bridgehead server, if possible.

   ![Routing Group Connector Properties dialog box](image)

   **Figure 5.6** Remote Bridgehead tab in the Routing Group Connector Properties dialog box

2. If you are creating a routing group connector between routing groups that includes Exchange 5.5 servers, in **Override connection credentials for Exchange 5.x**, click **Modify**, and then enter the Exchange 5.5 service account credentials for the Exchange 5.5 server to which you are connecting.

3. Click **Apply** to create the connector.
4. When a message appears that asks if you want to create a routing group connector in the remote routing group, click Yes.

After clicking Yes, Exchange creates a routing group connector in the remote routing group. This new routing group connector allows the remote routing group to send messages to the local routing group. When creating this new routing group connector, Exchange does the following:

- Exchange designates the bridgehead servers for the remote routing group connector as those servers listed on the Remote Bridgehead tab of the local routing group connector.

  **Note**  
  When Exchange designates servers in this way, only those servers listed on the Remote Bridgehead tab become bridgehead servers for the new connector. If you would rather have all of the servers in the remote routing group (not just those listed) function as bridgehead servers for the new connector, you must manually select the Any local server can send mail over this connector option on the General tab of the new connector.

- Exchange designates the remote bridgehead servers for the remote routing group connector as those servers listed as bridgehead servers on the General tab of the local routing group.

---

### Connecting to the Internet

Internet connectivity depends on SMTP and Domain Name System (DNS), as well as some other components. As stated earlier, SMTP is the protocol used by Exchange to deliver mail internally and to the Internet. To enable Internet mail delivery in your Exchange organization, you manage the SMTP protocol by configuring SMTP virtual servers and connectors. Additionally, you must ensure that DNS is properly configured because DNS is responsible for locating mail servers outside of the organization, so that SMTP can deliver mail to them.

**Note**  
Before connecting to the Internet, you should configure your Exchange server in accordance with your company's security policy.

After you install Exchange, you can send and receive mail using the default configuration of an SMTP virtual server on an Exchange server if the following conditions exist:

- You have a direct connection to the Internet.

  **Note**  
  Dial-up connectivity requires some additional configuration. For more information, see Configuring SMTP in Exchange 2000 Server ([http://go.microsoft.com/fwlink/?Linkid=15084](http://go.microsoft.com/fwlink/?Linkid=15084)).

- You have DNS configured correctly to resolve Internet names and to send mail to your Exchange server. Specific DNS settings are discussed later in this section.
This section describes how to configure Internet mail delivery. It includes:

- **Understanding SMTP dependencies and how to configure SMTP**  Exchange relies on SMTP to deliver mail internally and externally. Because of this reliance, you need to understand on which components SMTP depends and how to properly configure them to support SMTP. After you have set up these components properly, you need to know how to control the configuration of SMTP.

- **Using a wizard to configure Internet mail delivery**  Internet Mail Wizard is intended primarily for small and medium companies with less complex environments than large or enterprise companies.

- **Manually configuring Internet mail delivery**  In large or enterprise environments, you may need to manually configure Internet mail delivery, in accordance with your organization's policies. When manually configuring Internet mail, there is a separate set of tasks associated with configuring Exchange to send Internet mail and to receive Internet mail.

- **Controlling junk mail using filters**  Exchange supports connection, recipient, and sender filtering. Using these various filtering options helps you control the amount of junk mail your users receive.

**Note**

For detailed information about large or enterprise environments and common deployment scenarios for those environments, see *Configuring SMTP in Exchange 2000 Server*  (http://go.microsoft.com/fwlink/?LinkId=15084).

---

**Defining SMTP Dependencies**

As discussed earlier in this chapter, Exchange relies on SMTP to deliver mail internally and externally. This means that, for Internet mail delivery, Exchange depends on SMTP. However, before configuring Exchange for Internet mail delivery, you need to understand the components on which SMTP depends:

**Internet Information Services (IIS)**

As mentioned earlier, the SMTP service is installed as part of the Windows Server 2003 or Windows 2000 Server operating system. SMTP is a component of IIS and runs under a process called Inetinfo.exe. If you remove IIS from a server running Exchange, mail flow stops working.

IIS provides a framework process for Internet services such as HTTP, SMTP, and Network News Transfer Protocol (NNTP). IIS should not be confused with HTTP because several other services, such as SMTP, depend on IIS to function. After you install Exchange, the management of SMTP virtual servers moves to Exchange System Manager, even though the service itself continues to run within IIS. Because of this integration between Exchange and IIS, both the IIS component and the SMTP service that runs in IIS are required for Exchange and SMTP to function properly.
Active Directory

Exchange Server 2003 is tightly integrated with the Microsoft Active Directory® directory service. Exchange stores all of its configuration information in Active Directory, including information about recipient policies, SMTP virtual server configuration, and user mailboxes. However, SMTP reads its settings from the IIS metabase. Therefore, to supply IIS with the information it needs for SMTP functionality, Exchange System Attendant, using a component called DS2MB (directory service to metabase), replicates the configuration information from Active Directory to the IIS metabase.

DNS

SMTP depends on DNS to determine the Internet protocol (IP) address of its next internal or external destination server. Generally, internal DNS names are not published on the Internet. Therefore, SMTP must be able to contact a DNS server that can resolve external DNS names to send Internet mail, as well as a DNS server that can resolve internal DNS names for delivery within the organization. Additionally, for your Exchange servers to receive Internet mail, your DNS server must contain a mail exchange (MX) resource record that points to the A record with the IP address of the SMTP virtual server on your Exchange server that receives Internet mail for your organization. If you are supporting multiple domains, an MX record must exist for each of these domains for DNS to accept mail for the domain.

Recipient Policies

Recipient policies establish the default e-mail addresses that use a specific protocol (such as SMTP) for a set of users. E-mail addresses define the valid formats for addressing inbound e-mail messages to the Exchange system. The default recipient policy sets the mail domain for which the virtual server accepts incoming e-mail messages. It specifies the default SMTP and X.400 addresses for all Exchange-based mailbox-enabled objects. You can also create additional recipient policies if your organization receives mail for multiple domains, or if your default domain is used strictly for internal purposes and you use a different external mail domain.

Any SMTP domain specified in the recipient policies is replicated into the IIS metabase and set as authoritative local domains. Setting these domains as authoritative local domains means that SMTP accepts inbound mail for these domains and is responsible for sending all non-delivery reports for this domain. The only time an SMTP address is not considered local is when you add the address to the recipient policy because you clear the This Exchange Organization is responsible for all mail delivery to this address check box in the SMTP Address Properties dialog box.

Installing and correctly configuring the previous components ensures that SMTP functions properly with Exchange. With SMTP functioning properly, you can focus on configuring SMTP to meet your organization's needs.
Configuring SMTP

In Exchange, you use SMTP virtual servers and SMTP connectors to control the configuration of SMTP.

SMTP virtual servers

Essentially, an SMTP virtual server is an SMTP stack (a process or server that both receives e-mail messages and acts as a client for sending e-mail). Each SMTP virtual server represents an instance of the SMTP service on a server. Consequently, a single physical server can host many virtual servers.

An SMTP virtual server is defined by a unique combination of an IP address and port number. The IP address is the address on which the SMTP virtual server listens for incoming SMTP connections. The default IP address is All Unassigned, which means that the SMTP virtual server listens on any of the available IP addresses. The port number is the port through which the SMTP virtual server receives communications. The default port number for inbound connections to an SMTP virtual server is port 25.

You use Exchange System Manager to control most of the SMTP settings. The property settings of the SMTP virtual server control inbound mail and, to a lesser degree, outbound mail settings.

SMTP connectors

An SMTP connector designates an isolated route for mail. You can use SMTP connectors to establish a gateway for Internet mail or to connect to a specific domain or mail system. Connectors allow you to define specific options for the designated mail route.

Although you can send and receive Internet mail using an SMTP virtual server, most companies configure an SMTP connector to route Internet mail. Using an SMTP connector is recommended because it provides an isolated route for mail destined to the Internet. Additionally, more configuration options are available on an SMTP connector than on the SMTP virtual server. Because of the benefits of an SMTP connector, the following sections that describe both the Internet Mail Wizard and the manual procedure for configuring Exchange to send Internet mail include information about creating and configuring an SMTP connector to route Internet mail.
Using a Wizard to Configure Internet Mail

Exchange Server 2003 implements a new version of Internet Mail Wizard that helps you configure Internet mail connectivity with Exchange Server 2003 or Exchange 2000 Server. Using Internet Mail Wizard, you can configure an Exchange server to send Internet mail, receive Internet mail, or send and receive Internet mail. Furthermore, using Internet Mail Wizard means that you do not have to configure the SMTP connector and SMTP virtual server manually. Internet Mail Wizard automatically creates the necessary SMTP connector for outgoing Internet mail and configures your SMTP virtual server to accept incoming mail.

**Note**
If you have already set up SMTP connectors, modified the IP address or port number of your default SMTP server, or created additional SMTP virtual servers on your Exchange server, you cannot run Internet Mail Wizard. However, if you reset your server configuration to its default state, you can then run Internet Mail Wizard.

**Important**
Internet Mail Wizard is intended primarily for small and medium companies with less complex environments than large enterprise companies. If you have a complex or enterprise messaging environment, you should manually configure Exchange for Internet mail delivery.

To start Internet Mail Wizard

1. In Exchange System Manager, right-click your Exchange organization, and then click Internet Mail Wizard.

   **Note**
   To run Internet Mail Wizard, you must use the version of Exchange System Manager that comes with Exchange Server 2003.

2. Follow the instructions in the wizard to perform the configuration tasks (see Tables 5.2 and 5.3) necessary to configure Internet mail delivery.
Table 5.2 Using Internet Mail Wizard to configure the sending of mail

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select an Exchange server within your organization that will send Internet mail</td>
<td>As mentioned earlier, you cannot run the wizard on a server on which you have already set up SMTP connectors or created additional SMTP virtual servers. You can only use the wizard to designate Exchange 2000 or later servers.</td>
</tr>
<tr>
<td>Designate a bridgehead server</td>
<td>This is both the Exchange server and the SMTP virtual server on this server. The wizard creates an SMTP connector on the selected SMTP virtual server and Exchange server. The outbound bridgehead server handles all mail sent through this connector.</td>
</tr>
<tr>
<td>Configure an SMTP connector to send Internet mail</td>
<td>Internet Mail Wizard guides you through the process of configuring your SMTP connector.</td>
</tr>
<tr>
<td></td>
<td>• You can allow Internet mail delivery to all external domains, or you can restrict Internet mail delivery to specific domains.</td>
</tr>
<tr>
<td></td>
<td>• You can specify whether the SMTP connector sends outbound mail using DNS to resolve external domain names, or whether it uses a smart host that assumes responsibility for resolving external names and delivering mail.</td>
</tr>
<tr>
<td>Verify that your SMTP virtual server is not open for relaying</td>
<td>With open relaying, external users can use your server to send unsolicited commercial e-mail, which may result in other legitimate servers blocking mail from your Exchange server. If your server is secured for relay, only authenticated users can send mail to the Internet using your server.</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Select an Exchange server within your organization that will receive Internet mail</td>
<td>As mentioned earlier, you cannot run the wizard on a server on which you have already set up SMTP connectors or created additional SMTP virtual servers. You can only use the wizard to designate Exchange 2000 or later servers.</td>
</tr>
<tr>
<td>Configure your SMTP server to receive Internet mail</td>
<td>To receive incoming Internet e-mail messages, the server must have only one SMTP virtual server, and that virtual server must have a default IP address of <strong>All Unassigned</strong> and an assigned TCP port of 25. If more than one SMTP virtual server exists on the Exchange server, or if the IP address or the port assignment is different than the default settings, the wizard will not continue. You can then either restore the Exchange server to its default configuration and rerun the wizard, or you can use Exchange System Manager to configure Exchange manually.</td>
</tr>
<tr>
<td>Verify that your SMTP virtual server allows anonymous access</td>
<td>Other servers on the Internet expect to connect anonymously to your SMTP virtual server. Therefore, anonymous access must be permitted on your SMTP virtual server. If anonymous access is not configured, the wizard guides you through enabling anonymous access.</td>
</tr>
</tbody>
</table>
| Configure your recipient policies with the SMTP domains for which you want to receive inbound mail | The SMTP domains for which you want to receive Internet mail are configured in Exchange System Manager in **Recipient Policies**. You must have a recipient policy configured for every SMTP domain for which you want to accept Internet mail, and Exchange must be authoritative for this domain. If your default recipient policy contains the correct mail domain for your organization, use this policy.  

If you have created multiple recipient policies in Exchange System Manager, you cannot use the wizard to create additional recipient policies. In this case, to add or modify your recipient policies, you must use Exchange System Manager. To configure recipient policies manually, see "Configuring Recipient Policies" later in this chapter.  

You must configure MX records in DNS for all mail domains. If you do not have an MX record for your mail domain, DNS cannot accept messages for your domain. |
Configuring a Dual-Homed Server Using the Wizard

When you use Internet Mail Wizard to configure Internet mail delivery on a dual-homed server (a server configured with two or more network addresses, usually with two network interface cards), the wizard performs the necessary configuration steps described in Tables 5.2 and 5.3.

The wizard also creates an additional SMTP virtual server on the Exchange server. It configures Internet mail delivery in the following ways:

- To configure a server to send Internet mail, the wizard guides you through the process of assigning the intranet IP address to the default SMTP virtual server on which it creates the SMTP connector to send outbound mail. You assign the intranet IP address to this virtual server so that only internal users on your intranet can send outbound mail.

- To configure a server to receive Internet mail, the wizard guides you through the process of assigning the Internet IP address to the Internet SMTP virtual server. You assign an Internet IP address to this virtual server because external servers need to be able to connect to this SMTP virtual server to send Internet mail. Additionally, you must have an MX record on your DNS server that references this server and the IP address of the Internet SMTP virtual server.

  **Important**
  To increase the security on a dual-homed server, use Internet Protocol security (IPSec) policies to filter ports on the Internet network interface card and strictly limit the users that you allow to log on to this server. For more information about IPSec, see your Windows documentation.

Manually Configuring the Sending of Internet Mail

If your messaging environment is large or complex, you cannot use Internet Mail Wizard to configure Exchange to send Internet mail. Instead, you must manually configure Exchange to handle outbound messaging over the Internet.

Configuring Exchange to send Internet mail involves:

- Verifying that your SMTP virtual server uses the standard port for SMTP (port 25).
- Configuring an SMTP connector through which Internet mail is routed.
- Verifying that your DNS server can resolve external names, so that SMTP can deliver messages.

This section explains how to configure these settings on an Exchange server.
Verifying Outbound Settings on SMTP Virtual Servers

As discussed earlier, you configure most of the outbound settings that SMTP uses on the SMTP connector. However, you cannot configure the SMTP connector to control the ports and IP addresses through which Exchange sends outbound mail. To control these ports and IP addresses, you need to configure the SMTP virtual server. SMTP connectors configured on the virtual server inherit these settings.

Two of the SMTP virtual server properties relate directly to configuring Exchange to send Internet mail:

- **The outbound TCP port** You need to ensure that the outbound port is set to port 25 (the default setting). Of the two settings related to sending Internet mail, this is the setting that you must verify.

  **Note**
  Changing the default settings on your default SMTP virtual server can cause mail flow problems.

- **The use of an external DNS server** To send Internet mail, the DNS server Exchange uses must be able to resolve external (Internet) names. Two common methods for configuring DNS to resolve external names include:
  
  - Configuring Exchange to point to an internal DNS server that uses forwarders to an external DNS server (this is the easiest and most common method).
  
  - Configuring Exchange to point to an internal DNS server that does not have a forwarder to an external DNS server, and then configuring an external DNS server on the SMTP virtual server that is responsible for sending external mail.

The following procedures describe how to verify that the outbound TCP port is set to 25, and how to specify an external DNS server.
To verify that the outbound port used to deliver mail is set to 25

1. In Exchange System Manager, expand Servers, expand <server_name>, expand Protocols, expand SMTP, right-click Default SMTP Virtual Server, and then click Properties.

2. On the Delivery tab, click Outbound connections.

3. In the Outbound Connections dialog box (see Figure 5.7), verify that the TCP port is set to 25.

![Outbound Connections dialog box](image)

**Figure 5.7 Outbound Connections dialog box**

**Note**
Remote servers on the Internet expect your server to use TCP port 25. Changing this setting is not recommended because other SMTP servers generally accept connections on port 25 only.
To specify an external DNS server used by the SMTP virtual server

1. In the Default SMTP Virtual Server Properties dialog box, on the Delivery tab, click Advanced.

2. In the Advanced Delivery dialog box, click Configure.

3. In the Configure dialog box (see Figure 5.8), click Add to enter the IP address of an external DNS server. If you are using more than one external DNS server, use the Move Up and Move Down buttons to set the order of preference for the DNS servers.

![Configure dialog box for external DNS servers](image)

Figure 5.8 Configure dialog box for external DNS servers

Configuring an SMTP Connector

The primary uses of an SMTP connector are to connect to the Internet or to other mail systems, and to define additional options on an SMTP Internet gateway. Because an SMTP connector creates an isolated route for Internet mail, it eases administration and troubleshooting if you encounter mail flow problems.

This section focuses on the connector's use as a connection method to deliver Internet mail. To configure an SMTP connector to deliver Internet mail, you first need to consider the following configuration requirements:
How to route mail for outbound delivery?
When you configure a connector, you can either use DNS to route all outgoing mail through the connector, or you can specify a smart host to which the connector routes all mail.

Using DNS to route all outgoing mail through the connector If you use DNS to route outgoing mail, the SMTP connector uses DNS to resolve the IP address of the remote SMTP server, then it delivers the mail.

If you select this routing method, verify the following information:

- Verify that your DNS server can successfully resolve names on the Internet.
- If you use an external DNS server to resolve names, and this server is configured at the SMTP virtual server level (that is, using a different DNS server than the one specified on your network connection), ensure that this external DNS server can resolve names on the Internet.

Specifying a smart host The smart host handles DNS resolution and delivers the mail. Although you can specify a smart host on an SMTP virtual server, you should set the smart host on the connector itself. The smart host setting on the SMTP connector overrides any smart hosts configured on the SMTP virtual server.

If you select this routing method, you specify an IP address or name for the smart host. The IP address and name for the smart host must meet the following requirements:

- **If you specify an IP address for the smart host** Enclose the IP address in brackets (for example, [10.0.0.1]), and ensure that the IP address is not the IP address of the Exchange server.
- **If you specify a name for the smart host** Ensure that the name is a fully qualified domain name (FQDN). (For example, "Server Name" is not an FQDN. However, servername.contoso.com is an FQDN.) Also, ensure that the name is not the FQDN of the Exchange server.

If you do not have a smart host within your network, contact your Internet service provider (ISP) to find out what IP address or FQDN to use for the smart host. After you have the IP address or FQDN, make sure that the IP address or FQDN meets the previous requirements.

Which servers to use as local bridgehead servers?
An SMTP virtual server hosts a connector. When you create a connector, you designate at least one Exchange server and one SMTP virtual server as bridgehead servers. The connector inherits size restrictions and other settings from the SMTP virtual server. However, you can override these settings on the connector. You can also designate multiple bridgehead servers for load balancing, performance, and redundancy.
To send outbound mail, the connector uses the outbound port configured on the SMTP virtual server. If your organization sends a large amount of mail externally, you should designate dedicated Exchange servers and SMTP virtual servers as gateway servers or bridgehead servers receiving Internet mail. Using dedicated servers as gateway servers means that other mailbox servers do not have to assume the additional overhead of a gateway server.

**Which domains should be included in the address space?**

The address space defines the mail addresses or domains for the e-mail messages that you want routed through a connector. For example, an address space of * (asterisk) encompasses all external domains. A connector with this address space is capable of routing all external e-mail messages.

Exchange routes messages through a connector based on the closest match to an address space. If you had a connector with the * address space and then created a second connector with an address space of *.net, Exchange would route all mail sent to a domain with a .net extension through the second connector. This routing difference occurs because Exchange selects the connector that has the most similar address space to the outbound mail.

On connectors with an identical address space, costs work the same way as they do on routing group connectors. For example, you create two SMTP connectors to the Internet, Connector1 and Connector2, and each has the address space of *. Because Connector1 has better network connectivity, you always want to use this connector (unless it becomes unavailable) to send mail to the Internet, and you give Connector1 a cost of 1. Then, you give Connector2 a cost of 2. As long as Connector1 is operating properly, Exchange always sends messages through that connector because it has the lowest cost. If Connector1 becomes unavailable, Exchange uses the connector with the next lowest cost, Connector2.

---

**Important**

Do not list your inbound domains on an SMTP address space for a connector. Your inbound domains are listed in your recipient policies. (For more information, see "Configuring Recipient Policies" later in this chapter.) If you list some or all of your inbound domains in the SMTP address space, you may receive non-delivery reports (NDRs) that indicate a mail loop. (These NDRs may have the diagnostic code 5.3.5.) By specifying domains on the Address Space tab in the connector's Properties dialog box, you can configure these domains as routable domains.

---

**What is appropriate scope for the connector?**

You can select either an entire organization or a routing group for the connector's scope. For example, you have two routing groups and each routing group has a server that has an SMTP connector to send mail to the Internet. For this configuration, you may choose to specify a routing group scope for each of the connectors. Specifying a routing group scope forces the servers in each routing group to use the connector in that routing group. However, a routing group scope also means that, if the group's SMTP connector becomes unavailable, messages queue in the routing group until the connector becomes available again. Given the restrictions imposed by a routing group scope, you would most likely set an SMTP connector to this scope if it is acceptable to have messages queuing when a connector becomes unavailable, or if the network cannot accommodate the extra traffic from one routing group sending Internet mail through an SMTP connector of another routing group.
Otherwise, you must assign the connector an organization-wide scope and allow users in your entire organization to use any acceptable SMTP connector.

Creating an SMTP Connector

After you have thought about the configuration requirements for the SMTP connector and know what your configuration decisions are, you are ready to create and configure an SMTP connector. The first step is to configure the settings on which you have decided. Then you need to enable anonymous access for outbound connections because other servers on the Internet expect your SMTP server to connect anonymously.

After creating and configuring the connector using the following procedures, your SMTP connector is ready to send mail to the Internet. However, these procedures do not cover all the configuration settings for the connector. There are additional configuration settings that control how the connector delivers mail to the Internet. For more information about configuring these additional settings, see "Customizing Mail Delivery" later in this chapter.

To configure a connector for Internet mail delivery

1. In Exchange System Manager, expand the routing group, right-click Connectors, point to New, and then click SMTP Connector.

The Properties dialog box (see Figure 5.9) for the new connector appears.

![Figure 5.9 Properties dialog box for a newly created SMTP connector](image-url)
2. On the **General** tab, select one of the following options:
   - To use the DNS settings configured on the SMTP virtual server that is hosting the connector, select **Use DNS to route to each address space on this connector**.
     The SMTP connector uses DNS to resolve the IP address of the remote SMTP server, and then it delivers the mail.
   - To route mail to a Windows SMTP server or another server in your perimeter network (also known as a DMZ or demilitarized zone, and screened subnet), select **Forward all mail through this connector to the following smart hosts**.
     The SMTP connector then routes mail to the selected server, which handles DNS resolution and delivers the mail.

3. On the **General** tab, click Add, and add at least one bridgehead server and one SMTP virtual server.
   The servers that you add appear in the **Local bridgeheads** list on the **General** tab.

4. Click the **Address Space** tab.

5. On the **Address Space** tab, click Add.

6. In the **Add Address Space** dialog box (see Figure 5.10), in the **Select an address type** list, click SMTP, and then click OK.

   ![Figure 5.10 Add Address Space dialog box](image-url)
7. In the **Internet Address Space Properties** dialog box (see Figure 5.11), select the following options:

- In the **E-mail domain** box, type an e-mail domain for the connector.

  **Important**  
  In the **E-mail domain** box, there is a default value of * that represents all addresses. At least one connector in your organization should have this address space to ensure that all external domains are routed to the Internet.

- In the **Cost** box, assign an appropriate cost. By default, the cost is 1.

![Internet Address Space Properties dialog box](image-url)  

**Figure 5.11** Internet Address Space Properties dialog box
8. Click **OK** to return to the **Address Space** tab (see Figure 5.12).
9. On the **Address Space** tab, under **Connector scope**, select one of the following options:
   - To allow all servers in your Exchange organization to use this connector, select **Entire organization**.
   - To allow only servers in the routing group to use this connector to send Internet mail, select **Routing group**.

   **Note**
   If you select **Routing group**, ensure that you have another way for servers in different routing groups to send Internet mail.

**To enable anonymous access**

1. In the **Properties** dialog box for your SMTP connector, on the **Advanced** tab, click **Outbound Security**.

2. In the **Outbound Security** dialog box (see Figure 5.13), select **Anonymous access**.

![Outbound Security dialog box](image)

**Figure 5.13** Outbound Security dialog box
Customizing Mail Delivery

As discussed earlier in this chapter, one advantage to using an SMTP connector for outbound mail, rather than using an SMTP virtual server, is that you can specify additional configuration settings to affect how mail is delivered (see Table 5.4). Whether you need to adjust the default values for these settings depends on how you want your SMTP connector to deliver mail.

Table 5.4  Additional configuration settings for an SMTP connector

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery restrictions</td>
<td>Restricts who can send mail through a connector. By default, the connector accepts mail from everyone.</td>
</tr>
<tr>
<td></td>
<td>You configure these settings on the Delivery Restrictions tab of the SMTP connector's Properties dialog box.</td>
</tr>
<tr>
<td>Content restrictions</td>
<td>Specifies what types of messages are delivered through a connector.</td>
</tr>
<tr>
<td></td>
<td>You configure these settings on the Content Restrictions tab of the SMTP connector's Properties dialog box.</td>
</tr>
<tr>
<td>Delivery options</td>
<td>If you connect to a network service provider to retrieve your mail, configure a connector to run on a specified schedule, and implement advanced queuing and dequeuing features.</td>
</tr>
<tr>
<td></td>
<td>You configure these settings on the Delivery Options tab of the SMTP connector's Properties dialog box.</td>
</tr>
<tr>
<td>SMTP communication</td>
<td>Controls how the connector uses SMTP to communicate with other SMTP servers. Specifically, you can specify whether the connector uses SMTP or Extended Simple Mail Transfer Protocol (ESMTP) commands to initiate a conversation with another server and control the use of the ERTN and TURN commands. (These commands request that another SMTP server sends the e-mail messages that it has.)</td>
</tr>
<tr>
<td></td>
<td>You configure these settings on the Advanced tab of the SMTP connector's Properties dialog box.</td>
</tr>
<tr>
<td>Outbound security</td>
<td>Ensures that any mail flowing through the connector is authenticated. This setting is useful if you want to establish a more secure route for communicating with a partner company. With this setting, you can establish an authentication method and require Transport Layer Security (TLS) encryption.</td>
</tr>
<tr>
<td></td>
<td>You configure these settings on the Advanced tab of the SMTP connector's Properties dialog box.</td>
</tr>
</tbody>
</table>
Verifying DNS Setup for Outbound Mail

To send Internet mail using DNS rather than forwarding mail to a smart host, the Exchange server resolves the receiving domain and IP address of the recipient's SMTP server. The server then uses SMTP over TCP port 25 to establish a conversation with the recipient's SMTP server, and deliver the mail.

When you use DNS, the most important thing to remember is that all DNS servers that an Exchange server uses must be able to resolve external domains (also referred to as Internet domains).

There are two methods that you can use to configure DNS for outbound mail:

- **Method 1** You can configure Exchange to rely on your internal DNS servers. These servers resolve external names on their own or use a forwarder to an external DNS server.

- **Method 2** You can configure Exchange to use a dedicated external DNS server. (For more information about external DNS servers, see "To specify an external DNS server used by the SMTP virtual server" in the section "Verifying Outbound Settings on SMTP Virtual Servers" earlier in this chapter.)

For more information about how to configure and verify your DNS configuration, see Configuring SMTP in Exchange 2000 Server (http://go.microsoft.com/fwlink/?LinkId=15084) and your Windows documentation.

Manually Configuring the Receipt of Internet Mail

Manually configuring Exchange to receive Internet mail involves:

- Creating the proper recipient policies, so that your Exchange server receives mail for all e-mail domains that are used by your company.

- Configuring inbound SMTP virtual server settings to allow anonymous access, so that other SMTP servers can connect and send mail to your SMTP virtual server.

- Verifying that the correct MX records exist in DNS, so that other servers on the Internet can locate your server to deliver mail.

This section explains how to configure these settings on your Exchange server.
Configuring Recipient Policies

Exchange uses recipient policies to determine which messages should be accepted and internally routed to mailboxes in your organization. Recipient policies that are configured improperly can disrupt message flow for some or all recipients in your messaging system. Recipient policies are configured in Exchange System Manager under the Recipients container in Recipient Policies.

To ensure that your recipient policies are configured properly, verify the following:

- That recipient policies do not contain an SMTP address that matches the fully qualified domain name (FQDN) of any Exchange server in your organization. For example, if you have an Exchange server with an FQDN of server01.contoso.com and you also have this same FQDN (@server01.contoso.com) listed as an SMTP address and as a domain name on any recipient policy, this entry prevents mail from routing to other servers in the routing group.

- That the domain for which you want to receive SMTP mail is listed on a recipient policy—either on the default policy or another recipient policy. By verifying this information, you ensure that your users can receive mail from other SMTP domains.

- That you configured the necessary SMTP e-mail addresses to receive e-mail messages for additional domains. If you are not receiving e-mail messages for all of your SMTP domains, you may need to configure additional SMTP addresses for your recipients. For example, some of your users may currently receive e-mail messages addressed to contoso.com, but you also want them to receive e-mail messages addressed to adatum.com. In this situation, the SMTP address of @adatum.com and the SMTP address of @contoso.com must exist on a recipient policy for your Exchange organization.

For more information about recipient policies, see Chapter 4, "Managing Recipients and Recipient Policies."

Configuring Inbound SMTP Virtual Server Settings

To configure your SMTP virtual server to receive Internet mail, you must perform the following tasks:

- **Configure the inbound port as 25 and specify the IP address** Other servers on the Internet expect to connect to your SMTP virtual server on port 25. By default, all SMTP virtual servers use this port.
• **Verify that your SMTP virtual server allows anonymous access**  To receive Internet mail, your SMTP virtual server must permit anonymous access. Other servers on the Internet expect to communicate anonymously with your SMTP virtual server to send Internet mail to your users.

• **Verify that default relay restrictions are configured on your SMTP virtual server**  By default, the SMTP virtual server allows only authenticated users to relay e-mail messages. This setting prevents unauthorized users from using your Exchange server to send e-mail messages to external domains.

The following procedures describe how to perform each of these tasks.

**To configure or verify the inbound port and IP address**

- In Exchange System Manager, in the Properties dialog box of the SMTP virtual server, on the General tab, click **Advanced**.

  The **Advanced** dialog box appears (see Figure 5.14). By default, your SMTP virtual server uses an IP address of **All Unassigned**, which means that the virtual server listens for requests on all available IP addresses. You can keep the default IP address, or click **Edit** to change the address. By default, your SMTP virtual server uses TCP port 25. It is recommended that you do not modify the default port assignment.

![Advanced dialog box](image)

*Figure 5.14  Advanced dialog box*
To verify that your SMTP virtual server is configured to allow anonymous access

1. In Exchange System Manager, in the Properties dialog box of the SMTP virtual server, on the Access tab, click Authentication.

2. In the Authentication dialog box (see Figure 5.15), select the Anonymous access check box (if it is not already selected).

![Authentication dialog box](image)

Figure 5.15 Authentication dialog box
To verify that your SMTP virtual server is not set to open relay

1. In Exchange System Manager, in the Properties dialog box of the SMTP virtual server, on the Access tab, click Relay.

2. In the Relay Restrictions dialog box (see Figure 5.16), select Only the list below (if it is not already selected), click Add, and follow the instructions to add only those hosts that you want to allow to relay mail to the list.

   **Note**
   If you select All except the list below, your server may be used by unauthorized users to distribute unsolicited e-mail messages on the Internet.

   ![Figure 5.16 Relay Restrictions dialog box](image)

3. Select Allow all computers which successfully authenticate to relay, regardless of the list above (if it is not already selected).

   This setting allows you to deny relay permissions to all users who do not authenticate. Any remote Internet Message Access Protocol version 4 (IMAP4) and Post Office Protocol version 3 (POP3) users who access this server will authenticate to send mail. If you do not have users who access this server through IMAP4 or POP3, you can clear this check box to prevent relaying entirely, thereby increasing security. You can also designate a specific server for IMAP4 and POP3 users, and then clear this check box on all other Internet gateway servers.
Verifying DNS Setup for Inbound Mail

To receive Internet mail, the following DNS settings are necessary:

- Your DNS server must be configured correctly.
- Your external DNS servers must have an MX record pointing to an A record with the IP address of your mail server. The IP address must match the IP address configured on your SMTP virtual server that receives Internet mail.
- For external DNS servers to resolve your mail server's MX record and contact your mail server, your mail server must be accessible from the Internet.
- Your Exchange server must be configured to use a DNS server that can resolve external DNS names.

To ensure that your MX records are configured correctly, you can use the Nslookup utility. To verify that your server is accessible on port 25 to other servers on the Internet, you can use Telnet.

Note
For more information about how to configure and verify your DNS configuration, see Configuring SMTP in Exchange 2000 Server (http://go.microsoft.com/fwlink/?LinkId=15084) and your Windows documentation.

Enabling Filtering to Control Junk E-Mail Messages

Exchange Server 2003 supports three types of filters: connection filtering, recipient filtering, and sender filtering. These filters are useful in reducing the amount of junk e-mail messages your users receive.
You configure filtering in **Message Delivery Properties** under **Global Settings**. However, you must enable these filters on each SMTP virtual server to which you want to apply the filters. Generally, you should enable filtering on your Internet gateway servers because filtering is applied only to mail submitted from external users. On Exchange servers designated for internal mail, you do not need to enable filtering.

**To enable filtering**

1. On the **General** tab of the SMTP virtual **Properties** dialog box, click **Advanced**.
2. Select an IP address, and then click **Edit**.
3. In the **Identification** dialog box (see Figure 5.17), enable the filters that you want applied on this virtual server.

Figure 5.17 shows a virtual server with sender, recipient, and connection filtering enabled.

![Identification dialog box](image-url)
Connecting to Exchange 5.5 Servers and Other X.400 Systems

This section focuses on using the X.400 protocol and X.400 connectors to connect to Exchange 5.5 servers or other third-party X.400 mail systems. The X.400 connector relies on the X.400 protocol and its accompanying transport stack to provide the underlying transport functionality.

Three components control the behavior of the X.400 protocol on an Exchange server:

- **X.400 protocol**  An X.400 node appears under the Protocols container in Exchange System Manager on an Exchange server. Properties that are configured on the X.400 protocol determine how the protocol works on an individual server.

- **X.400 transport stacks**  An X.400 transport stack contains configuration information about network software, such as TCP/IP network services, and information about hardware, such as an X.25 port adapter or dial-up connection on the computer running Exchange. Each X.400 connector requires a transport stack on which to run and communicates using the configuration information within that stack. You can create either an X.400 TCP transport stack or an X.400 X.25 transport stack.

- **X.400 connectors**  X.400 connectors provide a mechanism for connecting Exchange servers with other X.400 systems or Exchange 5.5 servers outside of the Exchange organization. An Exchange 2003 server can then send messages using the X.400 protocol over this connector.

  **Important**  
  X.400 connectors are only available in Exchange Server 2003 Enterprise Edition.
Customizing the X.400 Protocol

The X.400 protocol provides the underlying functionality used by X.400 connectors and protocol stacks. The X.400 service message transfer agent (MTA) stack, located in the Protocols container under your Exchange server in Exchange System Manager, provides addressing and routing information for sending messages from one server to another. Use the X.400 Properties dialog box (see Figure 5.18) to configure basic settings and messaging defaults used by the X.400 protocol on your server. Any X.400 transport stacks and X.400 connectors that you create on this server inherit these settings by default, although you can override this configuration on individual connectors.

Figure 5.18 The General tab on the X.400 Properties dialog box
The following general properties can be set on the X.400 protocol.

- The entry in the **LocalX.400 name** box identifies the X.400 account that Exchange uses when it connects to the remote system. This name identifies the MTA to other mail systems. By default, this name is the name of the server where the X.400 service is installed. You can change the local X.400 name by using the **Modify** button. You can also set a local X.400 password. Third-party systems use this password when connecting to the X.400 service.

- The **Expand remote distribution lists locally** option makes a remote distribution list available to users in your organization. When this option is selected and a user sends a message to a remote distribution list, the distribution list expands locally (on the server to which the user is currently connected). Exchange finds the best routing for the message, based on the location of recipients in the list. This method ensures the most efficient message handling. However, note that processing large distribution lists can affect server performance.

- The **Convert incoming messages to Exchange contents** option changes the address and contents of incoming messages to a format compatible with MAPI clients, such as Microsoft Outlook® and Exchange. Do not select this option if your users do not use a MAPI client.

- The **Modify** button in **Message queue directory** allows you to change the location of the X.400 message queue directory.

  **Note**
  When you modify the location of the queue directory, you are modifying only the MTA database path and moving only the database (.dat) files. You are not moving any of the run files or the run directory. The database files are the core files that are required for starting the MTA, queue files, and message files.

### Understanding X.400 Connectors

Generally, you use X.400 connectors in the following situations:

- If your environment has an existing X.25 network.
- If you are connecting to an X.400 system or an Exchange 5.5 server outside of your organization.

  **Note**
  Although you can use X.400 connectors to connect routing groups within Exchange, the routing group connector is recommended.

To configure an X.400 connector, you perform the following steps:

1. Create an X.400 protocol stack.
2. Create an X.400 connector.

The following sections detail these steps.

**Creating an X.400 Protocol Stack**

Before you create an X.400 connector, you must create a protocol stack on the Exchange server that will host the connector. The protocol (or transport) stack is created on individual Exchange servers and provides the underlying functionality for the connector to transport messages. The server on which you create the protocol stack processes all messages that are sent by connectors that use this stack.

You create a transport stack using TCP or X.25, based on your network and the system to which you are connecting. Creating a transport stack involves the same steps for either protocol.

**To create a transport stack**

1. In Exchange System Manager, expand Protocols, right-click X.400, point to New, and then select either TCP/IP X.400 Service Transport Stack or X.25 X.400 Service Transport Stack.
2. On the General tab, type a name for this transport stack.

   The following names are the default names:

   - X.25 <server name>
   - TCP <server name>
3. (Optional) Under **OSI address information**, select the character set and the selector information if other applications use this transport stack.

Figure 5.19 shows the **General** tab of the Properties dialog box for a TCP/IP X.400 transport stack. On this tab, you can configure the transport stack. Any connectors that you configure to use this transport stack appear on the **Connectors** tab.

**Note**
When you first create the connector, the **Connectors** tab does not list any connectors.

![Figure 5.19](image)

**Figure 5.19** General tab of the Properties dialog box for a TCP/IP X.400 transport stack
4. (Optional) On the **General** tab of an X.25 transport stack (see Figure 5.20), set the following X.25-specific configuration options:

- Based on the information supplied by your X.400 service provider, type in the appropriate values for **Call user data**, **Facilities data**, and the **X.121 address** of the remote X.25 provider.

- For **I/O port**, type in the port number used by the X.25 adaptor. (If you have multiple X.25 X.400 transport stacks on a single server, each stack must use a different port number.)

![Figure 5.20   General tab of the Properties dialog box for an X.25 protocol stack](image)

Figure 5.20   General tab of the Properties dialog box for an X.25 protocol stack
Creating an X.400 Connector

After you create a TCP X.400 or X.25 X.400 transport stack, you can create an X.400 connector to connect to another X.400 system. Remember that connectors send mail in only one direction, so the X.400 connector enables mail to flow from your system to the remote system or routing group. If you are connecting to a remote system, the administrator of that system must also create a connector to send mail to your organization.

Table 5.5 lists the configuration settings that are available for an X.400 connector. These settings are available in the Properties dialog box for an X.400 connector (see Figure 5.21).

Table 5.5  Configuration settings for an X.400 connector

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote X.400 name</td>
<td>When you configure an X.400 connector, you need to specify a valid account and password for the remote X.400 system to which you are connecting. You configure these settings on the General tab of the X.400 connector's Properties dialog box.</td>
</tr>
<tr>
<td>Address space</td>
<td>The address space defines the mail addresses or domains for the e-mail messages that you want routed through a connector. You can specify the X.400 address of a third-party X.400 system or an Exchange 5.5 server to which you are connecting, so that all mail destined to the specified X.400 system is routed through this connector. You configure these settings on the Address Space tab of the X.400 connector's Properties dialog box.</td>
</tr>
<tr>
<td>Transport address information for the remote system</td>
<td>You must specify transport address information for the remote X.400 system to which you are connecting. You configure these settings on the Stack tab of the X.400 connector's Properties dialog box.</td>
</tr>
<tr>
<td>Settings</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Content restrictions</td>
<td>You can specify what types of messages are delivered through a connector. You configure these settings on the <strong>Content Restrictions</strong> tab of the X.400 connector's <strong>Properties</strong> dialog box.</td>
</tr>
<tr>
<td>Scope</td>
<td>You can select either an entire organization or a routing group for the connector's scope. For example, if you create an X.400 connector to send mail to an X.400 system on a server in one routing group, and an X.400 connector exists on a server in another routing group, you may choose to specify a routing group scope for these connectors so that servers in each routing group are forced to use the connector. If an X.400 connector that is set to a routing group scope becomes unavailable, messages queue in the routing group until the connector becomes available. If your user requirements permit this, you could implement the connectors with a routing group scope. You configure these settings on the <strong>Address Space</strong> tab of the X.400 connector's <strong>Properties</strong> dialog box.</td>
</tr>
<tr>
<td>Override options</td>
<td>By default, the X.400 connector inherits the settings that are configured on the X.400 protocol. To override these settings, you use the <strong>Override</strong> tab of the X.400 connector's <strong>Properties</strong> dialog box.</td>
</tr>
<tr>
<td>Delivery restrictions</td>
<td>You can restrict who can send mail through a connector. By default, mail is accepted from everyone. You configure these settings on the <strong>Delivery Restrictions</strong> tab of the X.400 connector's <strong>Properties</strong> dialog box.</td>
</tr>
</tbody>
</table>
To create an X.400 connector

1. In Exchange System Manager, right-click Connectors, point to New, and then click X.25 X.400 Connector or TCP X.400 Connector.

2. On the General tab (see Figure 5.21), in the Name box, type the connector name.

![Figure 5.21  General tab of the Properties dialog box for an X.400 connector](image)

3. On the General tab, under Remote X.400 name, click Modify.

4. In Remote Connection Credentials, in Remote X.400 name, type the name of the remote X.400 connector on the remote server. (The remote connector name defaults to the remote server name.) In the Password box, type the password for the remote X.400 connector. In the Confirm password box, type the password again.
5. Select one of the following options:
   - On the **Address Space** tab, click **Add**, select an address type, and then, in the **Address Properties** box, type all necessary information, including cost.
   - On the **Connected Routing Groups** tab, click **New**. On the **General** tab, in the **Organization** box, type the name of the organization that contains the routing group to which you want to connect, and then in the **Routing Group** box, type the name of the routing group to which you want to connect.

   **Note**
   The organization must exist on an Exchange server so that the naming conventions are known. Optionally, you can type address space information and cost on the **Routing Address** tab. By default, the address space is created from the organization and routing group names, and the cost is 1.

6. If the remote system is not an Exchange server, on the **Advanced** tab, clear the **Allow Exchange contents** check box.
   If you do not clear the check box, addresses on messages are in domain name form and not in X.400 form, and replies are not possible.

7. On the **Stack** tab for an X.25 X.400 connector, in the **X.121 address** box, type the X.121 address of the remote server as specified in the X.25 network service setup.
   —or—
   On the **Stack** tab for a TCP X.400 connector, choose one of the following options:
   - Select **Remote host name**, and then, in the **Address** box, type the fully qualified domain name (FQDN).
   - Select **IP Address**, and then, in the **Address** box, type the remote server's IP address.

**Configuring Additional Options on the X.400 Connector**

You can also use the **General** tab of the X.400 connector (see Figure 5.21) to configure public folder referrals and specify how messages are delivered by this connector. These additional options include:

- The **Message text word-wrap** option controls whether or not text wraps at a specific column in a message.
- The **Remote clients support MAPI** option results in Exchange sending messages through the connector in rich text format. Do not select this option if clients do not support MAPI because it can cause problems with message formatting on non-MAPI clients.
- The **Do not allow public folder referrals** option prevents public folder referrals when you connect to another routing group. Public folder referrals enable users in a connected routing group or a remote system to access public folders through this connector.
Overriding X.400 Properties

By default, each X.400 connector inherits the settings that are configured on the X.400 protocol. You can use the **Override** tab (see Figure 5.22) on the X.400 connector to override the options that are set on the X.400 protocol.

![X.400 Connector Properties](image)

**Figure 5.22  Override tab**

The configuration options that are available on the **Override** tab are as follows:

- The name entered in the **Local X.400 Service name** box overrides the local X.400 name of the X.400 transport stack. Some X.400 systems do not support certain characters. If your local X.400 name contains characters that are not supported by the remote system to which you are connecting, use this option to connect to the remote X.400 service using a name that it can support.

- The **Maximum open retries** option sets the maximum number of times that the system tries to open a connection before it sends a non-delivery report (NDR). The default is 144.

- The **Maximum transfer retries** option sets the maximum number of times that the system tries to transfer a message across an open connection. The default is 2.
• The **Open interval (sec)** option sets the number of seconds that the system waits after a message transfer fails. The default is 600.

• The **Transfer interval (sec)** option sets the number of seconds the system waits after a message transfer fails before resending a message across an open connection. The default is 120.

**Tip**
To restore Exchange default values, click **Reset Default Value**.

To set additional override values, you use the **Additional Values** dialog box (see Figure 5.23). To open this dialog box, click the **Additional Values** button on the **Override** tab in the X.400 connector's **Properties** dialog box.

![Additional Values dialog box](image)

**Figure 5.23** Additional Values dialog box
In the **Additional Values** dialog box, you can set these options:

- **The options under **RTS values** set the Reliable Transfers Service (RTS) values. RTS values determine message reliability parameters, such as the checkpoints to include in data and the amount of unacknowledged data that can be sent. You can use the options on an X.400 connectors’ **Override** tab to override the default X.400 service attributes, such as RTS values.**

- **The options under **Association parameters** determine the number and duration of connections to the remote system. Each X.400 connector uses the association parameters that are configured on the X.400 protocol, but you can configure association parameters on each individual connector to override the settings.**

- **The options under **Transfer timeouts** determine how long the X.400 connector waits before sending an NDR for urgent, normal, and not urgent messages. Each X.400 connector uses the transfer timeout values that are configured on the X.400 MTA, but you can configure specific transfer timeout values on each individual connector that override these settings.**

---

**Disabling or Removing Connectors**

If necessary, you can disable or remove existing connectors in your organization.

You can disable a connector that you do not want Exchange to use by setting the connection schedule to **Never**. Disabling a connector rather than deleting it allows you to retain the configuration settings if you want to enable it again in the future.

**To disable a connector**

1. In Exchange System Manager, right-click a connector, and then click **Properties**.
2. Select one of the following options:
   - For an X.400 connector, click the **Schedule** tab, and then click **Never**.
   - For an SMTP connector or a routing group connector, click the **Delivery Options** tab. Under **Specify when messages are sent through this connector**, in **Connection time**, select **Never run** from the drop-down list.

You can remove a connector that you no longer use by deleting it. You can remove a connector at any time. When you remove a connector, you are not warned of the connections you are breaking. (For example, you may be breaking an established connection between two routing groups.) However, you are prompted to verify that you want to remove the connector.

**To remove a connector**

- In Exchange System Manager, right-click the connector that you want to remove, and then click **Delete**.
Using Queue Viewer to Manage Messages

Queue Viewer is a feature in Exchange System Manager that allows you to monitor your organization's messaging queues, as well as the messages that are contained within those queues. Queue Viewer works at a server level. In Exchange System Manager, you expand the server and then click **Queues** to open Queue Viewer and display the messaging queues associated with the server (see Figure 5.24).

In Exchange Server 2003, Queue Viewer is enhanced to improve the monitoring of message queues. In Exchange 2003, you can view all of the messaging queues for a specific server from the **Queues** node under each server. This is an improvement over Exchange 2000, where each protocol virtual server has its own **Queues** node, and you cannot view all queues on a server from a central location. For example, using Exchange 2003, you can now use Queue Viewer to view both the X.400 and SMTP queues on a server (as in Figure 5.24), rather than having to view each of these queues separately in each of their respective protocol nodes.
Other enhancements to Queue Viewer in Exchange 2003 include:

- **Disabling outbound mail** You can use a new option called **Disable Outbound Mail** to disable outbound mail from all SMTP queues.

- **Setting the refresh rate** You can use the **Settings** option to set the refresh rate of Queue Viewer.

- **Finding messages** You can use **Find Messages** to search for messages based on the sender, recipient, and message state. This option is similar to enumerating messages in Queue Viewer in Exchange 2000.

- **Viewing additional information** You can click a specific queue to view additional information about that queue.

- **Viewing previously hidden queues** Queue Viewer in Exchange 2003 exposes three queues that were not visible in Exchange 2000: **DSN messages pending submission**, **Failed message retry queue**, and **Messages queued for deferred delivery**. (For descriptions of these queues, see Table 5.9.)

The remainder of this section highlights two of these new enhancements, disabling outbound mail and finding messages, as well as provides guidelines for how to use the SMTP and X.400 queues shown in Queue Viewer to troubleshoot message flow.

---

**Disabling Outbound Mail**

Using the **Disable Outbound Mail** option, you can disable outbound mail from all SMTP queues. For example, disabling outbound mail can be useful if a virus is active in your organization.

**To disable outbound mail**

- In Queue Viewer, click **Disable Outbound Mail**.

  **Note**

  The **Disable Outbound Mail** option does not disable the MTA or system queues. System queues are default queues for each protocol that hold messages only while certain essential routing tasks are performed, such as content conversion and address resolution. If you find messages in your system queues for extended periods, it means that one or more basic routing functions are failing somewhere in your Exchange organization. For more information about working with message accumulation in queues, see the sections "Using SMTP Queues to Troubleshoot Message Flow" and "Using X.400 (MTA) Queues to Troubleshoot Message Flow" later in this chapter.

  If you want to prevent outbound mail from a particular remote queue, instead of disabling all SMTP queues, you can freeze the messages in that particular queue.
To freeze all of the messages in a particular queue

- In Queue Viewer, right-click the queue, and then click Freeze.

To unfreeze a queue

- In Queue Viewer, right-click the queue, and then click Unfreeze.

Finding Messages

You can use the Find Messages option to search for messages by specifying search criteria (such as the sender or recipient) or the message state (such as frozen). You can also specify the number of messages that you want your search to return. Using Find Messages in Exchange Server 2003 is similar to the Enumerate messages option in Exchange 2000.

To search for messages by a particular sender (or recipient)

- In Queue Viewer, click Find Messages, click Sender (or Recipient), and then search by typing the name or using the search criteria.

To specify the number of messages that you want returned by a search

- In Queue Viewer, click Find Messages, click the Number of messages to be listed in the search list, and select the number of messages (for example, 500) that you want listed in the search.

To search for messages in a particular state

1. In Queue Viewer, click Find Messages, click the Show messages whose state is list, and select from the following options:
   - All Messages This option shows all of the messages in the list regardless of the state that they are in.
   - Frozen This option shows the messages that are in a frozen state. Besides freezing all messages in a specific queue, a single message can also be frozen. If a single message or a few messages in a queue are frozen, other messages can still flow into or out of this queue. The entire queue is not frozen.
   - Retry This option shows the messages that are awaiting another delivery attempt. Messages in the retry state have failed one or more delivery attempts.

2. After you have specified your search criteria, click Find Now to begin the search.
   The results of the search appear under Search Results.
Using SMTP Queues to Troubleshoot Message Flow

During message categorization and delivery, all mail is sent through the SMTP queues of an SMTP virtual server. If there is a problem delivering the message at any point in the process, the message remains in the queue where the problem occurred until the problem is remedied.

Use the SMTP queues to isolate possible causes of mail flow issues. If a queue is in a Retry status, in Queue Viewer, select the queue and check the properties of the queue to determine the cause. For example, if the queue properties display a message similar to "An SMTP error has occurred," you should review your server's event logs to locate any SMTP errors. If there are no events in the log, you should increase the SMTP logging level, by right-clicking the Exchange server, clicking Properties, clicking the Diagnostics Logging tab, and then selecting MSExchangeTransport.

Table 5.6 lists the SMTP queues, their descriptions, and troubleshooting information for message accumulation in each queue.

Table 5.6  SMTP queues

<table>
<thead>
<tr>
<th>Queue name</th>
<th>Description</th>
<th>Causes of message accumulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSN messages pending submission</td>
<td>Contains delivery status notifications, also known as non-delivery reports (NDRs), that are ready to be delivered by Exchange.</td>
<td>Messages can accumulate in this queue if the store service is unavailable or not running, or if problems exist with the IMAIL Exchange store component, which is the store component that performs message conversion. Check the event log for possible errors with the store service.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The following operations are unavailable for this queue: Delete All Messages (no NDR) and Delete All Messages (NDR).</td>
<td></td>
</tr>
<tr>
<td>Failed message retry queue</td>
<td>Contains messages that Exchange has failed to deliver, but that the server will attempt to send again.</td>
<td>Messages can accumulate in this queue if a problem exists with DNS or SMTP. Check the event log to determine whether an SMTP problem exists. Verify your DNS configuration using NSlookup or another utility. On rare occasions, a corrupted message can remain in this queue. To determine whether a message is corrupted, try to look at its properties. If some properties are not accessible, this can indicate message corruption.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The following operations are unavailable for this queue: Delete All Messages (no NDR) and Delete All Messages (NDR).</td>
<td></td>
</tr>
<tr>
<td>Queue name</td>
<td>Description</td>
<td>Causes of message accumulation</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Messages queued for deferred delivery | Contains messages queued for delivery at a later time, including messages sent by earlier versions of Outlook clients. (You can set this option in Outlook clients.) Messages sent by earlier versions of Outlook treat deferred delivery slightly differently. Previous versions of Outlook depend on the MTA for message delivery because SMTP, not the MTA, now handles message delivery. These messages remain in this queue until their scheduled delivery time. | Possible causes of message accumulation include:  
• Messages are sent to a user's mailbox while the mailbox is being moved.  
• The user does not yet have a mailbox created, and no master account security identifier (SID) exists for the user. For more information, see Microsoft Knowledge Base Article 316047, "XADM: Addressing Problems That Are Created When You Enable ADC-Generated Accounts" (http://support.microsoft.com/?kbid=316047).  
• The message may be corrupted, or the recipient may not be valid. To determine if a message is corrupted, check its properties. If some properties are not accessible, this can indicate a corrupted message. Also check that the recipient is valid. |
| Local delivery                     | Contains messages that are queued on the Exchange server for local delivery to an Exchange mailbox. | Messages can accumulate in this queue if the Exchange server is not accepting messages for local delivery. Slow or sporadic message delivery can indicate a looping message or a performance problem.  
This queue is affected by the Exchange store. Increase diagnostic logging for the Exchange store as described in "Configuring Diagnostic Logging for SMTP" later in this chapter. |
<table>
<thead>
<tr>
<th>Queue name</th>
<th>Description</th>
<th>Causes of message accumulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages awaiting directory lookup</td>
<td>Contains messages addressed to recipients who have not yet been resolved against Active Directory. Messages are also held here while distribution lists are expanded.</td>
<td>Generally, messages accumulate in this queue because the advanced queuing engine is unable to categorize the message. The advanced queuing engine may not be able to access the global catalog servers and access recipient information, or the global catalog servers are unreachable or performing slowly. The categorizer affects this queue. Increase diagnostic logging for the categorizer as described in &quot;Configuring Diagnostic Logging for SMTP&quot; later in this chapter.</td>
</tr>
<tr>
<td>Messages waiting to be routed</td>
<td>Holds messages until their next-destination server is determined, and then moves them to their respective link queues.</td>
<td>Messages accumulate in this queue if Exchange routing problems exist. Message routing may be experiencing problems. Increase diagnostic logging for routing as described in &quot;Configuring Diagnostic Logging for SMTP&quot; later in this chapter.</td>
</tr>
<tr>
<td>[Connector name</td>
<td>Server name</td>
<td>Remote domain]</td>
</tr>
<tr>
<td>Queue name</td>
<td>Description</td>
<td>Causes of message accumulation</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Final destination currently unreachable</td>
<td>Contains messages for which the final destination server cannot be reached. For example, Exchange cannot determine a network path to the final destination.</td>
<td>Messages can accumulate in this queue if no route exists for delivery. Additionally, any time a connector or a remote delivery queue is unavailable or in Retry for a period of time, and no alternate route exists to the connector or remote destination, new messages queue here. Messages can remain in this queue until an administrator fixes the problem or defines an alternate route. To get new messages to flow to their remote destination queue, allowing you to force a connection and get a Network Monitor (NetMon) trace, restart the SMTP virtual server.</td>
</tr>
<tr>
<td>Pre-submission</td>
<td>Holds messages that have been acknowledged and accepted by the SMTP service. The processing of these messages has not begun.</td>
<td>Messages that are accumulating constantly may indicate a performance problem. Occasional peaks in performance can cause messages to appear in this queue intermittently. Message accumulation in this queue can also indicate problems with a custom event sink or a third-party event sink.</td>
</tr>
</tbody>
</table>
Using X.400 (MTA) Queues to Troubleshoot Message Flow

Exchange Server 2003 uses the X.400 queues to submit mail to and receive mail from Exchange 5.5 servers and to send mail through connectors to other mail servers. If you experience mail flow problems when you are sending mail to an Exchange 5.5 or earlier server, or to another mail system to which you are connecting using X.400, check the X.400 queues on the Exchange server. If you experience mail flow problems when sending mail to servers that are running Exchange 5.5 or earlier, you should also check the MTA queues on those servers.

Table 5.7 lists the X.400 queues, their descriptions, and troubleshooting information for message accumulation in each queue.

Table 5.7 X.400 queues

<table>
<thead>
<tr>
<th>Queue name</th>
<th>Description</th>
<th>Causes of message accumulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>PendingRerouteQ</td>
<td>Contains messages that are waiting to be rerouted after a temporary link outage.</td>
<td>Messages can accumulate in this queue if a route to a connector, to a different mail system, or to an Exchange 5.5 server is unavailable.</td>
</tr>
<tr>
<td>Next hop MTA</td>
<td>Contains messages destined to one of the following:</td>
<td>Messages can accumulate in this queue when Exchange 2003 experiences problems sending to another mail system, to an Exchange 5.5 server, or through an X.400 link. Increase diagnostic logging for the X.400 service as described in &quot;Configuring Diagnostic Logging for the X.400 Service (MSEXchangeMTA)&quot; later in this chapter.</td>
</tr>
<tr>
<td></td>
<td>• Another gateway, such as a connector for Lotus Notes or Novell GroupWise.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• An X.400 link to an Exchange 5.5 site or a destination outside of the organization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• An Exchange MTA over the LAN—for example, destined to an Exchange 5.5 server in a mixed-mode environment.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Diagnostic Logging for SMTP

To help you determine the cause of a transport issue, you can view events that relate to MSExchangeTransport. If you experience problems with Exchange message flow, immediately increase the logging levels relating to MSExchangeTransport. Logging levels control the amount of data that is logged in the application log. The more events that are logged, the more transport-related events that you can view in the application log. Therefore, you have a better chance of determining the cause of the message flow problem. The SMTP log file is located in the Exchsrvr\Server_name.log folder.

As discussed in "Using SMTP Queues to Troubleshoot Message Flow" and "Using X.400 (MTA) Queues to Troubleshoot Message Flow" earlier in this chapter, issues with specific routing and transport components can cause messages to accumulate in a queue. If you are having problems with a specific queue, increase the logging level for the component that is affecting the queue.

Modifying Logging Settings

The following procedure explains how to modify diagnostic logging related to MSExchangeTransport.

To modify logging settings for MSExchangeTransport

1. In the console tree, expand Servers, right-click <server name>, and then click Properties.
2. Click the Diagnostics Logging tab.
3. Under Services, click MSExchangeTransport.
4. Under Categories, click the category for which you want to configure the logging level:
   - To troubleshoot routing issues, select Routing Engine/Service. Increase the logging level for this component if messages are accumulating in the Messages waiting to be routed SMTP queue.
   - To troubleshoot problems with address resolution in Active Directory, distribution list expansion, and other categorizer issues, select Categorizer. Increase the logging level for this component if messages are accumulating in the Messages waiting to be routed SMTP queue.
   - To troubleshoot issues with dial-up and virtual private network connectivity through Connection Manager, select Connection Manager.
• To troubleshoot problems with the queuing engine, select Queuing Engine. Increase the logging level for this component if you are experiencing mail flow problems, and mail is not accumulating in any of the queues.

• To troubleshoot issues with the Exchange store driver, select Exchange Store Driver. Increase the logging level for this component if messages are accumulating in the local delivery SMTP queue, the X.400 queues, or if you have problems receiving mail from Exchange 5.x servers or other mail systems.

• To troubleshoot general SMTP issues, select SMTP Protocol. Increase the logging level for this component if messages are accumulating in the Remote delivery SMTP queue to determine if SMTP errors are causing the bottleneck.

• To troubleshoot issues with the NTFS store driver, select NTFS Store Driver. Increase the logging level for this category if messages are accumulating in the local delivery SMTP queue.

5. Under Logging level, click None, Minimum, Medium, or Maximum. Click Maximum for troubleshooting purposes.

<table>
<thead>
<tr>
<th>Caution</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you increase the logging levels for Exchange services, you will experience some performance degradation. It is recommended that you increase the size of the application log to contain all of the data produced. If you do not increase the size of the application log, you will receive frequent reminders that the application log is full.</td>
</tr>
</tbody>
</table>

### Enabling Debugging Level Logging

If you are experiencing mail flow issues and want to view all events, you can modify a registry key to set logging to the debugging level, which is the highest level (level 7).

<table>
<thead>
<tr>
<th>Caution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.</td>
</tr>
</tbody>
</table>

#### To enable logging at the debugging level

1. Start Registry Editor.

2. In Registry Editor, locate and click the following registry key:
   
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeTransport\Diagnostics\SMTP Protocol

3. Set the value to 7, and then click OK.
Configuring Diagnostic Logging for the X.400 Service (MSExchangeMTA)

This section explains how to configure diagnostic logging for the X.400 service (MSExchangeMTA) on Exchange Server 2003. If you have to troubleshoot mail flow problems for servers running Exchange 5.5 and earlier, for other mail systems, or for X.400 connectors, it is useful to increase the logging level for MSExchangeMTA.

To configure logging for MSExchangeMTA

1. In the console tree, expand Servers, right-click <server name>, and then click Properties.
2. Click the Diagnostics Logging tab.
3. Under Services, click MSExchangeMTA.
4. Under Categories, click X.400 Service to troubleshoot delivery problems to servers running Exchange 5.5 and earlier, and other systems.
5. Under Logging level, click None, Minimum, Medium, or Maximum. Click Maximum for troubleshooting purposes.
This chapter reviews basic client access concepts, and how you manage the protocols used by the individual clients that access Exchange and the front-end and back-end server architecture.

This chapter also explains how to administer Microsoft® Exchange Server 2003 for client access in the context of a front-end/back-end server architecture. If you use more than one server, it is recommended that you use the front-end and back-end server architecture to handle the various messaging needs for the clients that you support.

The first part of this chapter provides an overview of the front-end and back-end server architecture. The second part of this chapter explains the configuration settings for the individual clients for Exchange. Use this chapter to configure your Exchange server for client access.

**Note**
To properly manage client access to Exchange Server 2003, you must first understand how Microsoft Windows® technologies, such as Internet Information Services (IIS) and the Microsoft Active Directory® directory service, interact with Exchange. You must also understand protocols such as HTTP and MAPI, and how client applications such as Exchange ActiveSync® and Microsoft Office Outlook® 2003 use these respective protocols to interact with Exchange.
Preparing to Manage Client Access

Before you configure the settings on your Exchange server for the protocols and clients that you will support, make sure that you have properly configured Exchange for your particular client access needs.

In general, to configure Exchange for client access, you must complete the following steps:

1. Choose your topology.
2. Secure your messaging infrastructure.
3. Choose your client access model and protocols.
4. Enable protocols that you will support. (optional)
5. Configure clients and devices.

The following sections briefly discuss each of these steps, giving you an overview of what each step involves and what to consider in making decisions related to that step. For more detailed information regarding the first three steps—topology, messaging infrastructure, and client access model, refer to the cross-references located in each of the following overview sections. For more detailed information about enabling protocols and configuring clients, see the appropriate sections later in this chapter.
Choosing a Topology

If you have more than one Exchange server, and if you plan to allow external access to Exchange from the Internet, you must understand the recommended Exchange front-end and back-end server architecture. This server architecture simplifies the client access model for organizations with multiple Exchange servers by using a single Exchange server to handle all requests from clients. The front-end server is responsible for proxying requests from clients and passing these requests to the Exchange back-end servers that have mailboxes on them. Front-end and back-end server architectures vary from simple to complex. Figure 6.1 shows the recommended front-end and back-end server architecture with the various clients that Exchange supports.

![Figure 6.1 The recommended Exchange front-end and back-end server architecture](image)
Understanding this server architecture helps you to better manage the types of clients that you plan to support in your messaging infrastructure. For more information about the front-end and back-end server architecture and choosing a topology for your Exchange deployment, see the book *Planning an Exchange Server 2003 Messaging System* ([http://www.microsoft.com/exchange/library](http://www.microsoft.com/exchange/library)). For the complete steps related to configuring the Exchange front-end and back-end server architecture, see "Post Installation Procedures," in the book *Exchange Server 2003 Deployment Guide* ([http://www.microsoft.com/exchange/library](http://www.microsoft.com/exchange/library)).

**Note**
You are no longer required to use Enterprise Server 2003 Enterprise Edition as your front-end server.

---

**Configuring Security for Client Access**

Before you deploy Exchange, prepare your organization for the client access methods that you will support by securing your messaging infrastructure. This involves the following steps:

1. Updating your server software.
2. Securing the Exchange messaging environment.


---

**Choosing Client Access Model and Protocols**

Although Simple Mail Transfer Protocol (SMTP) is the primary messaging protocol of Exchange, clients that communicate with Exchange often use protocols other than SMTP. Clients communicate using Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4 (IMAP4), HTTP, or Network News Transfer Protocol (NNTP). Some clients support all of these protocols; others do not. To accommodate these differences in protocol usage, Exchange supports all of these protocols. This comprehensive support means that you do not have to limit yourself when choosing a client access model. You decide what client access model best fits your users' needs, and then you select the protocols in Exchange that support this model.

**Note**
These services, as well as SMTP, are part of the Microsoft Windows Server™ 2003 operating system and run in IIS under the Inetinfo.exe process.

For more information about choosing a client access model and protocols, see the book *Planning an Exchange Server 2003 Messaging System* ([http://www.microsoft.com/exchange/library](http://www.microsoft.com/exchange/library)). After you select your client access model and supported protocols, you then enable and manage those protocols as described in "Managing Protocols" later in this chapter.
Chapter 6: Managing Client Access to Exchange

Configuring Clients and Devices

Part of planning an Exchange deployment involves determining which clients are necessary for the users in your organization. Exchange 2003 provides support for clients that use MAPI, IMAP4, POP3, HTTP, SMTP, and NNTP.

Clients often are able to support multiple protocols. For instance, client applications, such as Outlook 2003, can use MAPI, IMAP4, POP3, and SMTP. However, Microsoft Outlook Web Access, Outlook Mobile Access, and Exchange ActiveSync clients use HTTP.

**Note**

Depending on the clients that you choose to support, you use Exchange System Manager or the IIS Microsoft Management Console (MMC) snap-in to manage the protocols used by the client applications.

If your users use any of the client applications that are included with Exchange—Outlook Web Access, Outlook Mobile Access, and Exchange ActiveSync—there are specific requirements related to each of these clients:

- Outlook Mobile Access requires a compatible mobile device such as a cHTML (Compact HTML) device.
- Exchange ActiveSync requires a Microsoft Windows Mobile™-based device.

After you select your clients and configure Exchange for client access, Exchange provides a high level of flexibility for how you administer access to your messaging infrastructure. Later in this chapter are sections that describe the client applications that Microsoft supports for client access, and how to manage these applications. Read these sections to learn how to administer the clients that you use with Exchange.

Managing Protocols

In your Exchange messaging deployment configuration, you use Exchange System Manager to manage the protocols that you have decided to support. When you use Exchange System Manager to manage protocols, you manipulate settings on the individual virtual servers for the protocol that is to be configured. The virtual servers that are associated with the various protocols, such as the Exchange Virtual Server and the IMAP4 virtual server, contain settings based on the capabilities and use of the specific protocol. For example, the Exchange Virtual Server, which manages HTTP access to Exchange, provides settings for Outlook Web Access, such as gzip compression support.
For the most part, managing the virtual server for one protocol is identical to managing a virtual server for a different protocol. The common management tasks include enabling a virtual server, assigning ports, setting connection limits, starting or stopping a virtual server, and terminating connected users. However, there are some server-specific management tasks. The following sections describe both the common tasks for all virtual servers associated with protocols and the server-specific tasks for the Exchange Virtual Server, IMAP4 virtual server, and the NNTP virtual server.

**Note**
To manage individual Exchange client access settings, use Active Directory Users and Computers.

### Enabling a Virtual Server

When you install Exchange, the services that are necessary to support clients such as Outlook 2003, Outlook Web Access, and Exchange ActiveSync are enabled by default. For example, Exchange enables the SMTP service because it is the underlying protocol used to route messages both internally within an Exchange organization and externally to messaging systems outside of an Exchange organization. Similarly, Exchange enables HTTP because it is the underlying protocol for all Internet communication.

**Note**
Although Outlook Mobile Access uses the HTTP protocol, Outlook Mobile Access is disabled by default and must be enabled using Exchange System Manager.

However, Exchange installs, but does not enable services for POP3, IMAP4, and NNTP. If your client access model relies on communications that use POP3, IMAP4, or NTTP, then you must manually enable them.

To enable either the POP3 or IMAP4 service, you use the Services snap-in to set the service to automatically start. Then, you start the service using Exchange System Manager. To enable NNTP, you first use the Services snap-in to set the Network News Transfer Protocol service to start automatically, and then use Exchange System Manager to start the service.

**To enable a POP3 or IMAP4 virtual server to start automatically**

1. In the Services snap-in, in the console tree, click Services (Local).
2. In the details pane, right-click Microsoft Exchange POP3 or Microsoft Exchange IMAP4, and then click Properties.
3. On the General tab, under Startup type, select Automatic, and then click Apply.
4. Under Service status, click Start, and then click OK.
5. Repeat this procedure on all nodes that will be running the POP3 or IMAP4 virtual server.
To enable an NNTP virtual server

1. In the Services snap-in, in the console tree, click Services (Local).
2. In the details pane, right-click Network News Transfer Protocol (NNTP), and then click Properties.
3. On the General tab in Startup type, select Automatic. Click OK.

To start a POP3, IMAP4, or NTTP virtual server

- In Exchange System Manager, expand Protocols, expand the appropriate protocol (POP3, IMAP4, or NNTP), right-click the appropriate default virtual server (Default POP3 Virtual Server, and Default NTTP Virtual Server) and then click Start.

Assigning Ports and an IP Address to a Virtual Server

When you create a virtual server for a protocol, you have the option of using the default port assignments and Internet Protocol (IP) address for the server. Table 6.1 shows the default port assignments associated with the various protocols. The default IP address is (All Unassigned), which means that a specific IP address has not been assigned and the virtual server will use the IP address of the Exchange server that is currently hosting the virtual server. These default values provide a virtual server with automatic discovery—the server is able to immediately receive incoming connections using the default IP address and ports.

<table>
<thead>
<tr>
<th>Protocols</th>
<th>TCP port</th>
<th>Secure Sockets Layer (SSL) port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>25</td>
<td>Not available</td>
</tr>
<tr>
<td>IMAP4</td>
<td>143</td>
<td>993</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td>995</td>
</tr>
<tr>
<td>NNTP</td>
<td>119</td>
<td>563</td>
</tr>
</tbody>
</table>

**Important**

If you do not use the recommended port assignments, some clients may be unable to connect. You may also have to reconfigure your client software manually to connect to the new port assignments.

**Note**

Although it is highly recommended that you use the default port assignments, you do not have to use the default IP address. You can use the IP address from any available network card as the IP address for the virtual server.

If you plan to create multiple virtual servers, each virtual server must have a unique combination of ports and IP address. Because the port settings are standard and should not be changed, you will need to provide each virtual server with its own unique IP address.

Besides creating a unique combination of ports and IP address for each virtual server, you can also configure multiple identities for your virtual server. Multiple identities enable you to associate multiple host or domain names with a single virtual server.

Use the following procedure to either assign a unique IP address to a virtual server or to assign multiple identities to a virtual server.

**To assign an IP address or an identity to a virtual server**

1. On your Exchange server on which the virtual server is running, log on with the Exchange administrator account that has local administrative rights and Exchange full administrator permissions.
2. In Exchange System Manager, expand **Protocols**, right-click the protocol that is to be assigned a new IP address or to which you want to add a new identity, and then click **Properties**.
3. On the **General** tab, click **Advanced**.
4. In the **Advanced** dialog box, click **Edit** to change the IP address to a unique value, or click **Add** to add a new identity (that is, a new IP address and port combination).

---

**Setting Connection Limits**

A virtual server can accept an unlimited number of inbound connections and is limited only by the resources of the computer on which the virtual server is running. To prevent a computer from becoming overloaded, you can limit the number of connections that can be made to the virtual server at one time. By default, Exchange does not limit the number of incoming connections.

After users are connected, you can also limit the length of time that idle connections remain logged on to the server. By default, Exchange disconnects idle sessions after 10 minutes.

In topologies that contain Exchange front-end and back-end servers, the connection time-out setting varies based on server role. On back-end servers, the connection time-out setting limits the length of time clients can be connected to the server without performing any activity. However, on front-end servers, the connection time-out setting limits the total length of the client session, regardless of client activity. Therefore, in front-end and back-end server environments, you should configure the time-out value on your front-end servers high enough so that users can download the maximum message size that is permitted over the slowest connection speed that you want to support. Setting this value high enough ensures that clients are not disconnected.
while they are downloading messages. For details about configuring your Exchange front-end and back-end server architecture, see the book *Exchange Server 2003 Deployment Guide* (http://www.microsoft.com/exchange/library).

**Warning**

Setting the connection time-out setting too low can cause clients to be unexpectedly disconnected from the server and possibly receive error messages. Thirty minutes is the lowest recommended connection time-out setting.

To set connection limits

1. On your Exchange server that is running the virtual server, log on with the Exchange administrator account that has local administrative rights and Exchange full administrator permissions.
2. In Exchange System Manager, expand Protocols, right-click the protocol for which you want to change connection limits, and then click Properties.
3. On the General tab, set the appropriate connection limits.

---

**Starting, Stopping, or Pausing a Virtual Server**

Managing virtual servers often requires you to start, stop, or pause Exchange services. You manage Exchange services through the Computer Management console and Exchange System Manager.

**To start, stop, or pause a virtual server**

- In Exchange System Manager, right-click the virtual directory that you want to manage, and do one of the following:
  - To start the service, click Start.
  - To either change the server status to paused, or to restart a server that has previously been paused, click Pause.

  **Note**
  
  When a server is paused, an icon indicating that the server is paused appears next to the server name in the console tree.

- To change the server status to stopped, click Stop.

  **Note**
  
  When a server is stopped, an icon indicating that the server is stopped appears next to the server name in the console tree.
Terminating Connected Users

You can immediately disconnect a single user or all users if they are accessing the virtual server without permission.

To terminate connected users

1. In Exchange System Manager, expand SMTP, IMAP4, or POP3, and then double-click the virtual server on which you want to terminate connected users.
2. To terminate users from the Current Sessions node under the virtual server, do one of the following:
   • To disconnect a single user, click Terminate.
   • To disconnect all users, click Terminate all.

Managing Calendaring Options for the POP3 and IMAP4 Virtual Servers

You can configure a URL for access to calendaring information for your POP3 and IMAP4 messaging clients. This functionality allows you to use a POP3 or IMAP4 messaging client and Outlook Web Access to manage your calendar. The options that you select for this feature control the format of the URL.

Note
In topologies that contain Exchange front-end and back-end servers, you configure the URL that is used to access calendaring information on the back-end server. Exchange does not recognize any URL settings that you configure on the front-end servers.

When downloading meeting requests through POP3 and IMAP4, a URL to the meeting request in Outlook Web Access is added to the plain text/HTML portion of the message. Users click the URL to access the meeting request, and then accept or decline the request. (Some IMAP4 and POP3 messaging clients include a graphical user interface that allows those clients to accept or decline meetings without having to click the URL.) If users accept the request, Exchange automatically adds it to their calendar.

Note
The URL to the meeting request does not work for POP3 clients that are configured to download messages from the server. This situation occurs because the message is downloaded to the client. As a result, the URL points to a message that is no longer on the server.
To configure the calendaring options for a POP3 or IMAP4 virtual server

1. In Exchange System Manager, expand the First Administrative Group, expand the Servers node, and then expand the Exchange server for which you want to manage POP3 or IMAP4 calendaring options.

2. Expand the Protocols node, and then right-click the POP3 or IMAP4 protocol and select Properties.

3. On the Calendaring tab, select the server from which recipients download meeting requests:
   - To designate the recipient's home server as the server from which the recipient download meeting requests, select Use recipient's server.
     This is the default setting. If you select this option, the URL has the following format:
     ```
     http://<HomeServerName>/Exchange/Username/Inbox/Team%20Meeting.eml
     ```
   - To designate a front-end server as the server from which recipients download meeting requests, select Use front-end server.
     This option is useful if you have configured your Outlook Web Access users to access their mailboxes through a front-end server. If you select this option, the URL has the following format:
     ```
     http://<FQDomainName>/Exchange/Username/Inbox/Team%20Meeting.eml
     ```

4. To use SSL to connect to the Exchange servers, select Use SSL connections.
   
   Note
   If you select this option, the URL syntax includes https:// instead of http://.

5. Click OK to save your settings.

Managing the HTTP Virtual Server

Outlook Web Access, Outlook Mobile Access, and Exchange ActiveSync rely on the HTTP protocol to access Exchange information. These clients also use the WebDAV protocol, a set of rules that enable computers to exchange information, to execute instructions through the Exchange front-end server, as well as retrieve and manipulate information in the Exchange store. By supporting both HTTP and WebDAV, Exchange 2003 is able to provide more data access functionality to users. For example, users of Outlook Web Access are able to perform calendar request operations and can store Microsoft Office files, such as Word Documents, in the Exchange store.

Exchange provides support for both HTTP and WebDAV through the HTTP virtual server. When you install Exchange, Exchange automatically installs and configures an HTTP virtual server. You administer this default server only from IIS.
However, to provide for a number of different collaboration scenarios and to supplement the access to folders that is provided by the default Web site in IIS, you can create new HTTP virtual servers in Exchange System Manager. As with any virtual server, each new HTTP virtual server that you create requires a unique combination of IP address, TCP port, SSL port, and host name. Furthermore, for each virtual server that you create, you must define one virtual directory as the root directory of the server for publishing content.

**Note**
The folder contents displayed by the HTTP virtual server are converted to Web pages and sent to a user's browser by IIS.

**To create a new HTTP virtual server**

1. In Exchange System Manager, expand the **First Administrative Group**, expand the **Servers** node, and then expand the Exchange server on which you want to create a new HTTP virtual directory.

2. Expand the **Protocols** node, and then right-click the HTTP protocol and select **New HTTP Virtual Server**.

3. In the **Properties** dialog box for the new HTTP virtual server, configure the settings for your new Exchange virtual directory.

**Managing the Exchange Virtual Server**

The Exchange Virtual Server contains the virtual directories that provide access to Exchange for the various HTTP clients that Exchange supports, such as Outlook Web Access, Outlook Mobile Access, and Exchange ActiveSync. Although you enable settings for Outlook Web Access, including forms-based authentication and gzip compression, using the Exchange Virtual Server, you manage most settings for the Exchange virtual directories in the IIS snap-in.

Specifically, in Exchange 2003, if you need to configure authentication settings to your Exchange virtual directories, use the IIS snap-in. If you need to configure access control for the \Exchange, \Public, and \Exadmin virtual directories, use Exchange System Manager instead.
Working with IMAP4-Specific Settings

The IMAP4 virtual server has two protocol-specific settings:

- **Include all public folders when a folder is requested**  
  Unlike POP3, which allows clients to access only mail messages, IMAP4 clients have access to folders other than the Inbox folder. However, this ability to access other folders needs to be enabled on the virtual server.

- **Enable fast message retrieval**  
  Fast message retrieval improves performance by approximating message size, as opposed to actually calculating the message size. Performance improves because less processor work is needed.

You select these settings on the **General** tab for the **Default IMAP4 Virtual Server Properties** dialog box (see Figure 6.2).

![Figure 6.2 General tab in the Default IMAP Virtual Server Properties dialog box](image)
Configuring NNTP Posting Limits and Moderation Settings

Exchange Server 2003 uses NNTP to enable users to participate in newsgroup discussions. Exchange also enables users who are running client applications that support NNTP to access newsgroup public folders on computers running Exchange. Users can read and post items, such as messages and documents, to NNTP newsgroups that are represented in Exchange as public folders. For example, users can share information by posting messages to a newsgroup public folder in their area of interest. Other users can read and respond to items in the newsgroup. Items in newsgroups can be replicated to Usenet host computers through newsfeeds.

A newsfeed is the flow of items from one Usenet site to another. Newsfeeds enable users of different news sites to read and post articles to newsgroups as though they are using one news site. A news site is a collection of related newsgroups. An article posted to one news site is sent to other news sites where it can be read. You need to create a newsfeed to each remote server to which you want to distribute news articles.

Because the reason for using newsgroups is to post and share information, you will likely need to manage the size of these postings in relation to the resources available on the NNTP virtual server. Accepting articles that are too large or accepting too much data during one connection can cause increased traffic, overload your network, and quickly fill your hard disk. Be sure to set a size limit that matches your server's capabilities.

To configure posting limits and moderation settings for an NNTP virtual server

1. On your Exchange server that is running the virtual server, log on with the Exchange administrator account that has local administrative rights and Exchange full administrator permissions.

2. In Exchange System Manager, expand Protocols, right-click the protocol for which you want to change connection limits, and then click Properties.
3. On the **Settings** tab (see Figure 6.3), select from the following options:

- To allow clients to post articles to newsgroups on this NNTP virtual server, select **Allow client posting**. This option permits users to post and read articles in newsgroups that they can access, unless the newsgroup is set to read-only. You can also limit the size of the article that clients post as well as the size of the connection.

- To allow clients to post articles to newsfeeds on the NNTP virtual server, select **Allow feed posting**. You can limit the size of articles that are posted by using the **Limit post size** check box. You can limit the amount of data that is sent to a newsfeed during a single connection by using the **Limit connection size** check box.

![Figure 6.3 Settings tab of the Default NNTP Virtual Server Properties dialog box](image)

**Note**

For more information about configuring NNTP, see the Exchange Server 2003 Help.
Managing Outlook 2003

Exchange Server 2003 and Outlook 2003 build on previous versions of Exchange and Outlook and include several improvements for client messaging:

- Exchange and Outlook now require less information to be passed from the client to the server, resulting in increased performance and a better end-user experience on slow networks.


- Exchange and Outlook now include the Cached Exchange Mode feature, allowing for true offline access using Outlook.

Note

Of all the new features in Outlook 2003, Cached Exchange Mode is one of great interest to many organizations, and it is discussed in detail in this section.

Configuring Cached Exchange Mode

Cached Exchange Mode makes it possible for users to use a local copy of their mailbox on their computer to allow for a true offline experience with Outlook 2003. This means that, if network connectivity is lost between the Outlook 2003 client and Exchange 2003, users are able to continue working with the cached information and do not see a pop-up message stating that Outlook is requesting information from the Exchange server.

By default, new installations of Outlook 2003 use Cached Exchange Mode. If you are upgrading from previous versions of Outlook to Outlook 2003 and you want your users to be able to use Cached Exchange Mode, you must manually configure the Outlook client to use Cached Exchange Mode. To do this, you modify a user's profile to use the local copy of the user's Exchange mailbox.
To manually enable Cached Exchange Mode for Outlook 2003 upgrades

1. In Control Panel on the computer running Outlook 2003, perform one of the following tasks:
   - If you are using Category View, in the left pane, under See Also, click Other Control Panel Options, and then click Mail.
   - If you are using Classic View, double-click Mail.

2. In Mail Setup, click E-mail Accounts.

3. In the E-mail Accounts Wizard, click View or change existing e-mail accounts, and then click Next.

4. On the E-mail Accounts page, highlight the account that you want to modify, and then click Change.

5. On the Exchange Server Settings page, select the Use Cached Exchange Mode check box.

6. Click Next, and then click Finish to save the changes to your local profile.

Managing Outlook Web Access


When it comes to managing Outlook Web Access, you use both Exchange System Manager and the IIS snap-in. Use:

- Exchange System Manager to modify settings for access control to Outlook Web Access.
- The IIS snap-in to control the Authentication settings for the virtual directories for Outlook Web Access, including \Exchange, \Exchweb, and \Public.

The following sections show how to use Exchange System Manager and the IIS snap-in to perform a variety of management tasks associated with Outlook Web Access.
Enabling and Disabling Outlook Web Access for Internal Clients Only

You can enable users within your corporate network to access Outlook Web Access, while at the same time denying access to external clients. The key to this approach is a combination of a recipient policy and a special HTTP virtual server. The steps for this approach are as follows:

1. Create a recipient policy with an SMTP domain name. Users who are connecting to an HTTP virtual server must have an e-mail address with the same SMTP domain as the virtual server. Creation of a recipient policy is an efficient way to apply the same SMTP domain to multiple users.

   **Note**
   Outlook Web Access users do not need to know the name of the SMTP domain.

2. Apply the recipient policy to the user accounts for which you want to enable access.

3. Then, on the front-end server, create a new HTTP virtual server that specifies the domain that is used in the recipient policy.

After you have completed these steps, users whose e-mail addresses do not have the same SMTP domain as the HTTP virtual server will not be able to log on and access Outlook Web Access. Also, as long as you do not use the SMTP domain as the default domain, external users cannot determine what the SMTP domain is because the domain does not appear in the *From* field when users send e-mail messages outside the organization.

   **Note**
   For more information about users with mailboxes that have an SMTP address that is not related to the address specified in the default recipient policy, see Microsoft Knowledge Base Article 257891, "XWEB: 'The Page Could Not Be Found' Error Message When You Use OWA" ([http://support.microsoft.com/?kbid=257891](http://support.microsoft.com/?kbid=257891)).

Besides enabling Outlook Web Access for users within your corporate network, you can also prevent specific internal users from accessing Outlook Web Access. You do this by disabling the HTTP and NNTP protocols for those users.

**To prevent an internal user from accessing Outlook Web Access**

1. In Active Directory Users and Computers, open the user's *Properties* dialog box.

2. On the *Exchange Features* tab, clear the settings for HTTP and NNTP.
Using Browser Language

When using Microsoft Internet Explorer 5 or later to access Outlook Web Access, new installations of and upgrades to Exchange 2003 use the browser's language settings to determine the character set to use to encode information, such as e-mail messages and meeting requests.

If you upgrade a server running Exchange 2000 Server that was modified to use a browser's language setting, Exchange 2003 continues to function in the same manner. Table 6.2 lists the language groups and respective character sets.

**Table 6.2  Outlook Web Access language group and character sets**

<table>
<thead>
<tr>
<th>Language group</th>
<th>Character set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arabic</td>
<td>Windows 1256</td>
</tr>
<tr>
<td>Baltic</td>
<td>iso-8859-4</td>
</tr>
<tr>
<td>Chinese (Simplified)</td>
<td>Gb2131</td>
</tr>
<tr>
<td>Chinese (Traditional)</td>
<td>Big5</td>
</tr>
<tr>
<td>Cyrillic</td>
<td>koi8-r</td>
</tr>
<tr>
<td>Eastern European</td>
<td>iso-8859-2</td>
</tr>
<tr>
<td>Greek</td>
<td>iso-8859-7</td>
</tr>
<tr>
<td>Hebrew</td>
<td>windows-1255</td>
</tr>
<tr>
<td>Japanese</td>
<td>iso-2022-jp</td>
</tr>
<tr>
<td>Korean</td>
<td>ks_c_5601-1987</td>
</tr>
<tr>
<td>Thai</td>
<td>windows-874</td>
</tr>
<tr>
<td>Turkish</td>
<td>iso-8859-9</td>
</tr>
<tr>
<td>Vietnamese</td>
<td>windows-1258</td>
</tr>
<tr>
<td>Western European</td>
<td>iso-8859-1</td>
</tr>
</tbody>
</table>
If you expect Outlook Web Access users in your organization to send mail frequently, you can modify registry settings so that users who are running Internet Explorer 5 or later can use UTF-8 encoded Unicode characters to send mail.

**Warning**
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

**To modify the default language setting for Outlook Web Access**

1. On the Exchange server, log on with the Exchange administrator account, and start Registry Editor (`regedit`).
2. In Registry Editor, locate the following registry key:
   ```plaintext
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWEB\OWA\UseRegionalCharset
   ```
3. Create a DWORD value called `UseRegionalCharset`.
4. Right-click the `UseRegionalCharset` DWORD value, and then click **Modify**.
5. In **Edit DWORD Value**, in the **Value data** box, type `1`, and then click **OK**.
6. Close Registry Editor to save your changes.

**Setting Up a Logon Page**

You can enable a new logon page for Outlook Web Access that stores the user's name and password in a cookie instead of in the browser. When a user closes a browser, the cookie is cleared. Additionally, after a period of inactivity, the cookie is cleared automatically. The new logon page requires the user to enter a domain, user name, and password, or a full user principal name (UPN) e-mail address and password, to access e-mail.

To enable this logon page, you must first enable forms-based authentication on the server, and then secure the logon page by setting the cookie time-out period and adjusting client-side security settings.
Enabling Forms-based Authentication

To enable the Outlook Web Access logon page, you must enable forms-based authentication on the server.

To enable forms-based authentication

1. On the Exchange server, log on with the Exchange administrator account, and then start Exchange System Manager.
2. In the console tree, expand Servers.
3. Expand the server for which you want to enable forms-based authentication, and then expand Protocols.
4. Expand HTTP, right-click Exchange Virtual Server, and then click Properties.
5. In the Exchange Virtual Server Properties dialog box, on the Settings tab, in the Outlook Web Access pane, select the Enable Forms Based Authentication option.
6. Click Apply, and then click OK.

Setting the Cookie Authentication Time-out

In Exchange 2003, Outlook Web Access user credentials are stored in a cookie. When the user logs off from Outlook Web Access, the cookie is cleared and it is no longer valid for authentication. Additionally, by default, if your user is using a public computer, and selects the Public or shared computer option on the Outlook Web Access logon screen, the cookie on this computer expires automatically after 15 minutes of user inactivity.

The automatic time-out is valuable because it helps to protect a user's account from unauthorized access. However, although the automatic time-out greatly reduces the risk of unauthorized access, it does not completely eliminate the possibility that an unauthorized user could access an Outlook Web Access account if a session is left running on a public computer. Therefore, it is important that you educate users about precautions to take to avoid risks.

To match the security needs of your organization, an administrator can configure the inactivity time-out values on the Exchange front-end server. To configure the time-out value, you must modify the registry settings on the server.

Warning

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.
To set the Outlook Web Access forms-based authentication public computer cookie time-out value

1. On the Exchange front-end server, log on with the Exchange administrator account, and then start Registry Editor (regedit).
2. In Registry Editor, locate the following registry key:
   
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA

3. From the Edit menu, point to New, and then click DWORD Value.
4. In the details pane, name the new value PublicClientTimeout.
5. Right-click the PublicClientTimeout DWORD value, and then click Modify.
6. In Edit DWORD Value, under Base, click Decimal.
7. In the Value Data box, type a value (in minutes) between 1 and 432000.
8. Click OK.

To set the Outlook Web Access forms-based authentication trusted computer cookie time-out value

1. On the Exchange front-end server, log on with the Exchange administrator account, and then start Registry Editor (regedit).
2. In Registry Editor, locate the following registry key:
   
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA

3. From the Edit menu, point to New, and then click DWORD Value.
4. In the details pane, name the new value TrustedClientTimeout.
5. Right-click the TrustedClientTimeout DWORD value, and then click Modify.
6. In Edit DWORD Value, under Base, click Decimal.
7. In the Value Data box, type a value (in minutes) between 1 and 432000.
8. Click OK.
Adjusting Client Security Options for Users

For your Outlook Web Access logon page, you can allow two types of security options for authentication. Depending on their needs, users can select either of these security options on the Outlook Web Access logon page:

- **Public or shared computer**  Inform your users to select this option when they access Outlook Web Access from a computer that does not conform to the security setting for your organization (for example, an Internet kiosk computer). This is the default option and provides a short default time-out option of 15 minutes.

- **Private computer**  Inform your users to select this option when they are the sole operator of the computer, and the computer adheres to the security settings for your organization. When selected, this option allows for a much longer period of inactivity before automatically ending the session—its internal default value is 24 hours. This option is intended to benefit Outlook Web Access users who are using personal computers in their office or home.

Enabling Outlook Web Access Compression

Outlook Web Access supports data compression, which is optimal for slow network connections. Depending on the compression setting that you use, Outlook Web Access compression works by compressing static or dynamic Web pages.

Table 6.3 lists the available compression settings in Exchange Server 2003 for Outlook Web Access.

<table>
<thead>
<tr>
<th>Compression setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Compresses both static and dynamic pages.</td>
</tr>
<tr>
<td>Low</td>
<td>Compresses only static pages.</td>
</tr>
<tr>
<td>None</td>
<td>No compression is used.</td>
</tr>
</tbody>
</table>

Using data compression, users can experience performance increases of up to 50 percent when they are using slower network connections, such as traditional dial-up access.
To use data compression for Outlook Web Access in Exchange 2003, the following prerequisites must be fulfilled:

- The Exchange server that users authenticate against for Outlook Web Access is running Windows Server 2003.
- Your users' mailboxes are on Exchange 2003 servers. (If you have a mixed deployment of Exchange mailboxes, you can create a separate virtual server on your Exchange server just for Exchange 2003 users and enable compression on it.)
- Client computers are running Internet Explorer version 6.0 or later. The computers must also be running Windows XP or Windows 2000, with the security update discussed in Microsoft Knowledge Base Article 328970, "Cumulative Patch for Internet Explorer" (http://support.microsoft.com/?kbid=328970), installed.

Note
If a user does not have a supported browser for compression, the client will still perform normally.

In addition to the previous prerequisites, you may also need to enable HTTP 1.1 support through proxy servers for some dial-up connections. (HTTP 1.1 support is required for compression to function properly.)

**To enable data compression**

1. On the Exchange server, log on with the Exchange administrator account, and then start Exchange System Manager.
2. In the details pane, expand Servers, expand the server on which you want to enable data compression, and then expand Protocols.
3. Expand HTTP, right-click Exchange Virtual Server, and then click Properties.
4. In Exchange Virtual Server Properties, on the Settings tab, under Outlook Web Access, use the Compression list to select the compression level that you want (None, Low, or High).
5. Click Apply, and then click OK.

**Blocking Web Beacons**

In Exchange 2003, Outlook Web Access makes it more difficult for people who send junk e-mail messages to use beacons to retrieve e-mail addresses. Beacons often come in the form of images that are downloaded onto a user's computer when the user opens a junk e-mail item. After the images download, a beacon notification is sent to the sender of the junk e-mail informing the sender that the e-mail address of your user is valid. The end result is that the user will receive junk e-mail more frequently because the junk e-mail sender now knows that the e-mail address is valid.
In Outlook Web Access, an incoming message with any content that could be used as a beacon, regardless of whether the message actually contains a beacon, prompts Outlook Web Access to display the following warning message:

To help protect your privacy, links to images, sounds, or other external content in this message have been blocked. Click here to unblock content.

If users know that a message is legitimate, they can click the Click here to unblock content link in the warning message and unblock the content. If your users do not recognize the sender or the message, they can open the message without unblocking the content and then delete the message without triggering beacons. If your organization does not want to use this feature, you can disable the blocking option for Outlook Web Access.

To disable the blocking option

- On the user's Outlook Web Access Options page, under Privacy and Junk E-mail Prevention, clear the Block external content in HTML e-mail messages check box.

---

**Blocking Attachments**

With Outlook Web Access, you can block users from opening, sending, or receiving specified attachment types. In particular, you can:

- **Prevent users from accessing certain file type attachments**  By default, all new Exchange 2003 installations block attachments of Levels 1 and 2 file types, and Levels 1 and 2 MIME types. This feature is particularly useful in stopping Outlook Web Access users from opening attachments at public Internet terminals, which could potentially compromise corporate security. If an attachment is blocked, a warning message indicating that the user cannot open the attachment appears in the InfoBar of the e-mail message. Outlook Web Access users who are working in their offices or connected to the corporate network from home can open and read attachments. You can enable full intranet access to attachments by providing the URL to the back-end servers and allowing attachments on the Exchange back-end servers.

- **Prevent users from sending or receiving attachments with specific file extensions that could contain viruses**  This feature in Outlook Web Access matches the attachment blocking functionality in Outlook. For received messages, a warning message indicating that an attachment is blocked appears in the InfoBar of the e-mail message. For sent messages, users cannot upload any files with extensions that appear on the block list.

To change the attachment blocking settings, you must modify the registry settings on the server.

**Warning**

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.
To modify the attachment blocking settings on an Exchange server

1. On the Exchange server, log on with the Exchange administrator account, and then start Registry Editor (regedit).
2. In Registry Editor, locate the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA
```
3. From the Edit menu, point to New, and then click DWORD Value.
4. In the details pane, name the new value DisableAttachments.
5. Right-click DisableAttachments, and then click Modify.
6. In Edit DWORD Value, under Base, click Decimal.
7. In the Value data box, type one of the following numbers:
   - To allow all attachments, type 0.
   - To disallow all attachments, type 1.
   - To allow attachments from back-end servers only, type 2.
8. Click OK.

Filtering Junk E-Mail Messages

You can control how Exchange 2003 manages junk e-mail for your organization. To do this, you need to enable filtering, and then configure sender, recipient, and connection filtering. For more information about controlling junk e-mail with Exchange 2003, see "Enabling Filtering to Control Junk E-mail Messages" in Chapter 5, "Understanding and Configuring Message Routing and Transport."
Simplifying the Outlook Web Access URL

The HTTP virtual server that is created by Exchange during installation has the following URLs for user access:

- **http://server_name/public**  This URL provides access to public folders.
- **http://server_name/exchange/mailbox_name**  This URL provides access to mailboxes.

However, users often request that a URL that is simpler than the default URL be made available for accessing their mailboxes. Creating this simple URL makes the URL both easier to remember and easier to enter into a Web browser. For example, http://www.contoso1.com is an easier URL for users to remember than http://contosoexchange01/exchange.

The following procedure provides a method for simplifying the URL that is used to access Outlook Web Access. This procedure configures a request sent to the root directory of the Web server (http://server_name/) to redirect to the Exchange virtual directory. For example, a request to http://server_name/ is directed to http://server_name/exchange/, which then triggers implicit logon.

**To simplify the Outlook Web Access URL**

1. Using Internet Services Manager, open the properties for the Default Web Site.
2. Click the Home Directory tab, and then select A redirection to a URL.
3. In Redirect to, type /directory name, and then click A directory below URL entered.
   For example, if you want to redirect http://mail/ requests to http://mail/exchange, in Redirect to, you would type /exchange.
4. To require users to use SSL, in Redirect to, type https://mail/directory name, and then click The exact URL above option.
   This setting hard codes the name of the server. Therefore, if you redirect client requests to https://mail, the client must be able to resolve the name "mail."

For information about another method for redirecting clients to SSL, see Microsoft Knowledge Base Article 279681, "How to Force SSL Encryption for an Outlook Web Access 2000 Client" ([http://support.microsoft.com/?kbid=279681](http://support.microsoft.com/?kbid=279681)).
Managing Exchange ActiveSync

Using Exchange ActiveSync, users with a Windows-powered mobile device with the desktop ActiveSync software can synchronize their devices with their Exchange servers over the Internet. Users connect across the Internet to their Exchange front-end server and request information from their Exchange mailbox server. When you enable access to Exchange using Exchange ActiveSync, you should perform the following steps.

1. Use the front-end and back-end server architecture to provide a single namespace for users to connect to your network (recommended). For more information, see the book Planning an Exchange Server 2003 Messaging System (http://www.microsoft.com/exchange/library).


3. Inform users how to connect to the Internet from their device and use ActiveSync on their device to connect to their Exchange server. For more information, see the book Exchange Server 2003 Deployment Guide (http://www.microsoft.com/exchange/library).

The following sections provide information about how to manage Exchange ActiveSync for your organization, including how to enable and disable the Exchange ActiveSync application, and how to enable ActiveSync for your users.

Enabling Exchange ActiveSync for Your Organization

By default, Exchange ActiveSync is enabled for all of the users in your organization. If your users have Windows-powered mobile devices, you can inform them how to configure their devices to use Exchange ActiveSync. For information about informing your users how to use Exchange ActiveSync, see "Configuring Exchange Server 2003 for Client Access" in the book Exchange Server 2003 Deployment Guide (http://www.microsoft.com/exchange/library).

To enable and disable Exchange ActiveSync for your organization, you use Exchange System Manager. However, when you add new users to your organization and you want to enable them to use Exchange ActiveSync to access Exchange with a Windows-powered mobile device, you use Active Directory Users and Computers to modify the settings for a user or groups of users. The following procedures describe how to enable or disable the Exchange ActiveSync application for your organization, and how to modify Exchange ActiveSync settings to accommodate new users.
To enable or disable Exchange ActiveSync for your organization

1. On the Exchange front-end server that is running Exchange ActiveSync, log on with the Exchange administrator account, and then start Exchange System Manager.

2. Expand Global Settings, right-click Mobile Services, and then click Properties.

3. On the Mobile Services Properties page, in the Exchange ActiveSync pane, select or clear the check box next to Enable user initiated synchronization.

4. Click OK.

To modify Exchange ActiveSync settings

1. On the Exchange server with the user's mailbox, log on with the Exchange administrator account, and then start Active Directory Users and Computers.

2. Expand the domain, and then open the location for the users that you want to manage.

3. Right-click the user or users whose Exchange ActiveSync settings you want to modify, and then select Exchange Tasks.

4. In Exchange Task Wizard, on the Available Tasks page, select Configure Exchange Features, and then click Next.

5. On the Configure Exchange Features page, select User initiated synchronization, and then select one of the following:

   • To permit users to use Exchange ActiveSync to synchronize their Exchange mailbox with their mobile devices, select Enable.

   • To prevent users from using Exchange ActiveSync, select Disable.

   • To prevent the users' settings from being modified when you have selected more than one user, select Do not modify.

6. Click Next to apply your changes.

7. Click Finish.

Note
If you want to view a detailed report of the settings and the changes you made to users, select View detailed report when this wizard closes.
Enabling Up-to-Date Notifications for Your Organization

After you configure your organization to use Exchange ActiveSync, you can configure your Exchange 2003 servers so that users can receive up-to-date notifications to keep their devices up-to-date with the changes that occur when a new item arrives in their Exchange mailbox.

Up-to-date notifications are notifications that are sent to a user's device when a new item arrives in their Exchange mailbox. This notification prompts the user's device to synchronize the device with the Exchange mailbox automatically.

To enable up-to-date notifications for your organization

1. On the Exchange front-end server running Exchange ActiveSync, log on with the Exchange administrator account, and then start Exchange System Manager.
2. Expand Global Settings, right-click Mobile Services, and then click Properties.
3. On the Mobile Services Properties page, in the Exchange ActiveSync pane, select Enable up-to-date notifications.
4. Click OK.

To modify up-to-date notifications settings for your users

1. On the Exchange server with the user's mailbox, log on with the Exchange administrator account, and then start Active Directory Users and Computers.
2. Expand the domain, and then open the location for the users whose settings that you want to modify.
3. Right-click the user or users whose up-to-date notifications settings you want to modify, and then select Exchange Tasks.
4. In Exchange Task Wizard, on the Available Tasks page, select Configure Exchange Features, and then click Next.
5. On the Configure Exchange Features page, select Up-to-date notifications, and then select one of the following:
   - To allow users to use up-to-date notifications, select Enable.
   - To prevent users from using up-to-date notifications, select Disable.
   - To prevent the users' settings from being modified when you have selected more than one user, select Do not modify.
Allowing Users to Use a Mobile Operator to Receive Notifications

If you enable the Exchange ActiveSync up-to-date notifications feature, your users use a mobile operator to deliver messages from the corporate network to their devices. There are two ways in which you can allow your users to receive notifications:

Option 1: Specify a mobile operator for your users
If you want to specify a mobile operator for your users, you disable the **Enable notifications to user specified SMTP addresses** on the Exchange server that has the mailboxes for these users. If you choose this option, you need to inform your users how to set their devices to use the mobile operator that you specify for up-to-date notifications.

Option 2: Allow users to use their own mobile operators
If your users have their own Windows-powered mobile devices, you can allow them to use their own mobile operators to deliver notifications to their devices. If you choose this option, you need to inform your users how to set their devices to use the mobile operators that they want to use for up-to-date notifications.

The following two procedures describe how to configure these options. The first procedure describes how to set the **Enable notifications to user specified SMTP address** option, and the second procedure describes how to set the mobile operator on a user's device.

To set the **Enable notifications to user specified SMTP address** option for your organization

1. On the Exchange front-end server that is running Exchange ActiveSync, log on with the Exchange administrator account, and then start Exchange System Manager.
2. Expand **Global Settings**, right-click **Mobile Services**, and then click **Properties**.
3. On the **Mobile Services Properties** page, in the Exchange ActiveSync pane, set the **Enable notifications to user specified SMTP address** option as follows:
   - If you want to specify a mobile operator for your user, clear **Enable notifications to user specified SMTP address**.
   - If you want to allow your users to specify their own mobile operators, select **Enable notifications to user specified SMTP address**.
4. Click **OK**.

To specify a mobile operator for up-to-date notifications on a device

1. In ActiveSync, on a Windows-powered mobile device, tap **Tools**, and then tap **Options**.
2. On the **Server** tab, tap **Options**.
3. On the **Server Synchronization Options** screen, tap **Device Address**.
4. On the **Device Address** screen, do one of the following:
• If your users are using a mobile operator that you specify, select Corporate Service Provider, and then enter the Device Phone Number and Service Provider Name in the fields that are provided.

• If your users are using their own mobile operators, select Device SMS Address, and then enter the device address in the field provided.

Managing Outlook Mobile Access

Using Outlook Mobile Access, users can browse their Exchange mailbox using a device such as a Microsoft Windows-powered Smartphone or a cHTML-capable device. You can also enable users to use devices that are not officially supported by Microsoft, but which are likely to function properly with only minor compatibility issues by enabling unsupported devices to use Outlook Mobile Access.

The following sections provide information about how to manage Outlook Mobile Access for your organization, including how to enable the Outlook Mobile Access application for your organization and how to enable users for Outlook Mobile Access.

Configuring Exchange to Use Outlook Mobile Access

By default, Outlook Mobile Access is disabled when you install Exchange Server 2003. For users to use Outlook Mobile Access, you must first enable it. When you enable access to Exchange using Outlook Mobile Access, you should do the following:

1. Use the front-end and back-end server architecture to provide a single namespace for users to connect to your network. For more information, see the book Planning an Exchange Server 2003 Messaging System (http://www.microsoft.com/exchange/library).


3. Inform users how to connect to the Internet from their devices, and how to use Outlook Mobile Access to access their Exchange information. For more information, see the book Exchange Server 2003 Deployment Guide (http://www.microsoft.com/exchange/library).
Enabling Outlook Mobile Access for Your Organization

To enable Outlook Mobile Access for your organization, you use Exchange System Manager. After you enable Outlook Mobile Access, you can use Active Directory Users and Computers to modify the Outlook Mobile Access settings for users or groups of users.

**To enable Outlook Mobile Access for your organization**

1. Log on as an Exchange administrator to the Exchange server with the user's mailbox, and then start Exchange System Manager.
2. Expand Global Settings, right-click Mobile Services, and then click Properties.
4. To enable users to use unsupported devices, select Enable unsupported devices.
   
   **Note**
   
   For information about supported devices for Exchange and planning for mobile device support with Exchange, see the book Planning an Exchange Server 2003 Messaging System (http://www.microsoft.com/exchange/library/).
5. Click OK.

**To modify Outlook Mobile Access settings**

1. Log on as an Exchange administrator to the Exchange server with the user's mailbox, and then start Active Directory Users and Computers.
2. Expand the domain, and then open the location for the users whose settings that you want to modify.
3. Right-click the user or users whose Outlook Mobile Access settings you want to modify, and then select Exchange Tasks.
4. In Exchange Task Wizard, on the Available Tasks page, select Configure Exchange Features, and then click Next.
5. On the **Configure Exchange Features** page, select **Outlook Mobile Access**, and then select one of the following:
   - To allow users to use Outlook Mobile Access, select **Enable**.
   - To prevent users from using Outlook Mobile Access, select **Disable**.
   - To prevent the users' settings from being modified when you have selected more than one user, select **Do not Modify**.

6. Click **Next** to apply your changes.

7. Click **Finish**.
CHAPTER 7
Managing Mailbox Stores and Public Folder Stores

The Microsoft® Exchange store is a storage platform that provides a single repository for managing multiple types of unstructured information in one infrastructure. Mailbox stores and public folder stores are two of the components that make up the Exchange store. The Exchange store is also known as the Web Storage System.

The first section of this chapter describes the permissions that protect the Exchange store, which in some ways function differently than permissions elsewhere in Exchange.

The next three sections of this chapter describe how to work with the different elements of the Exchange store:

- **Storage groups, mailbox stores, and public folder stores** These components control how information on a specific server is stored and maintained.

- **Storage-related aspects of mailboxes** Mailbox information resides both in mailbox stores and in user objects in the Active Directory® directory service. Most management tasks for mailboxes involve working in Active Directory.

- **Public folders** Public folders can reside on many servers simultaneously (or on none at all), so Exchange treats public folder management tasks as largely server-independent.

The following appendixes of this book provide information about store-related administrative tasks that are more detailed and complex than those included in this chapter:

- **Appendix D, "Identifying and Accessing Exchange Store Components"** This appendix describes the components of the Exchange store and identifies the different tools that you can use to manage them.

- **Appendix E, "Controlling Public Folder Replication"** This appendix includes procedures for configuring replication. To help you troubleshoot replication issues, this appendix also describes how replication works and what aspects of your Exchange topology impact the replication process.
• Appendix F, "Using Full-Text Indexing"  This appendix describes how to set up full-text indexes, and how to optimize and maintain the indexes.

• Appendix G, "Troubleshooting and Repairing Store Problems"  This appendix describes the common problems, events, and messages that are related to managing mailbox and public folder stores. It also includes information about what causes the problems, and possible solutions.

Note
For detailed information about the internal workings of the stores, and for detailed backup and recovery procedures, see Disaster Recovery for Microsoft Exchange 2000 Server (http://go.microsoft.com/fwlink/?LinkID=18350). Although existing recovery functionality has not changed, Microsoft Exchange Server 2003 has new recovery features. For more information about the new features, see the book What's New in Exchange Server 2003 (www.microsoft.com/exchange/library).

Working with Permissions for Public Folders and Mailboxes

Managing administrative access to mailbox and public folder stores is similar to managing administrative access to the server itself. This section contains an overview of the permissions that you need to manage public folders and mailboxes. Before you begin management tasks on public folders and mailboxes, be sure to read the sections that pertain to the tasks that you plan to perform:

• Using Exchange Administrative Roles with Exchange Store Components  This section explains what access the various Exchange administrative roles (Exchange Full Administrator, Exchange Administrator, and Exchange View Only Administrator) provide to mailbox stores, public folder stores, and public folder trees.
• **Understanding the Types of Permissions That Control Access to Mailboxes and Public Folders, Using Mailbox Permissions, and Using Public Folder Permissions**  These sections explain how the permissions on store contents—mailboxes, public folders, and the messages they store—are much more complex than permissions used elsewhere in Exchange, and provide basic information about how to use these permissions.

**Important**
A detailed explanation of how these permissions work is beyond the scope of this chapter. For a full explanation of how store permissions work, see the Exchange technical article, "Working with Store Permissions in Microsoft Exchange 2000 and 2003" (http://go.microsoft.com/fwlink/?LinkId=18612).

If you are doing any troubleshooting with store permissions, or if you need to modify permissions in ways other than the delegation methods described later in this chapter, it is strongly recommended that you study "Working with Store Permissions in Microsoft Exchange 2000 and 2003" first.

• **Maintaining the Minimum Permissions Required for Mailbox Stores and Public Folder Stores**  This section explains the minimum permissions that are required for mailbox stores and public folder stores to function correctly.

---

**Using Exchange Administrative Roles with Exchange Store Components**

To perform most of the tasks in this chapter, you must have at least Exchange Administrator permissions on the administrative group where you are working. For more information about the Exchange administrative roles and the Exchange Administration Delegation Wizard, see "Managing Permissions" in Chapter 2, "Managing an Exchange Organization."

Use the information in Table 7.1 and Figure 7.1 to identify what permissions are involved, and how the Exchange store objects inherit these permissions. This will help you to recognize situations where you may need a different administrative role or different permissions.

Table 7.1 summarizes the permissions for the three Exchange administrative roles on Exchange store objects.
### Table 7.1 Permissions for the Exchange administrative roles on mailbox stores, public folder stores, and public folder trees

<table>
<thead>
<tr>
<th>Role</th>
<th>Allowed</th>
<th>Denied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Full Administrator</td>
<td>Full Control</td>
<td>Receive-As, Send-As</td>
</tr>
<tr>
<td></td>
<td>Additional permissions in Active Directory to allow you to work with deleted items and offline address lists</td>
<td></td>
</tr>
<tr>
<td>Exchange Administrator</td>
<td>All except Change Permissions</td>
<td>Receive-As, Send-As</td>
</tr>
<tr>
<td></td>
<td>Additional permissions in Active Directory to allow you to work with offline address lists</td>
<td></td>
</tr>
<tr>
<td>Exchange View Only Administrator</td>
<td>Read</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>List object</td>
<td></td>
</tr>
<tr>
<td></td>
<td>List contents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>View Information Store Status</td>
<td></td>
</tr>
</tbody>
</table>

Figure 7.1 summarizes how mailbox stores, public folder stores, and public folder trees inherit permissions.

![Direction of inheritance of permissions for Exchange Full Administrators, Exchange Administrators, or Exchange View Only Administrators](image)

**Figure 7.1** Direction of inheritance of permissions for Exchange Full Administrators, Exchange Administrators, or Exchange View Only Administrators
As Figure 7.1 shows, objects in the Exchange store inherit permissions from their administrative group, with the following exceptions:

- Delegating Exchange administrative roles on an administrative group gives administrators in those roles limited permissions on mailboxes—enough to create or delete mailboxes, and set options such as storage limits.

- A public folder inherits some administrative permissions from the public folder tree where it resides. It does not inherit permissions from the public folder store.

- Administrative rights on a public folder include many folder-specific permissions that are not available on the public folder tree. For example, although an Exchange Administrator cannot modify the permissions on a public folder tree, the administrator can modify permissions on a public folder in that tree.

**Note**
For an administrator to apply a system policy to a store, the administrator must have the appropriate permissions on both the System Policies container and on the target store. If you are using a distributed administration model with multiple administrative groups that have separate administrators, each administrator will be able to interact only with the stores in that administrator’s own administrative group.

**Important**
Public folder trees and their public folders can only be administered in the administrative group where they were created, even though you can replicate folders in the tree to multiple administrative groups. If you are using a distributed administration model with multiple administrative groups that have separate administrators, each administrator can work with the public folder stores in that administrator’s own administrative group, but may not have access to the public folders that those stores support.

---

### Understanding the Types of Permissions That Control Access to Mailboxes and Public Folders

The access control lists (ACLs) on public folders, mailboxes, and the messages that they contain use Microsoft Windows® 2000 permissions to control access (with a few additional permissions that are specific to Exchange). This is a change from Microsoft Exchange 5.5, in which the ACLs used MAPI permissions. Exchange 2003 substitutes MAPI permissions for Windows 2000 permissions in the following circumstances:

- When communicating with MAPI-based client applications, such as Microsoft Outlook®. In this case, Exchange converts the permissions to MAPI permissions when displaying them to the user. If the user modifies the permissions, Exchange converts them back to Windows 2000 permissions to save them.
• When replicating data to Exchange 5.5 servers in a deployment that contains coexisting servers that run Exchange 5.5 and servers that run Exchange 2003. Because Exchange 5.5 servers only use MAPI permissions, Exchange 2003 replicates permissions to them in the MAPI format. When the permissions replicate back to Exchange 2003 servers, Exchange 2003 converts them to the Windows 2000 format before saving them.

**Note**
Both of these circumstances apply to mailboxes and to public folders in the Public Folders tree (and all of the folders and messages contained in it). Folders and messages in general-purpose public folder trees cannot be accessed by MAPI-based clients and are not replicated to Exchange 5.5 servers. Therefore, Exchange always uses Windows 2000 permissions with these folders and messages. For more information about the differences between the Public Folders tree and general-purpose public folder trees, see "Configuring Public Folder Stores" later in this chapter.

Exchange handles all conversions between Windows 2000 permissions and MAPI permissions automatically. However, as an administrator, be aware that when you use Exchange System Manager to set permissions, you may need to work with either Windows 2000 permissions or MAPI permissions, depending on the type of object you are securing.

### Using Mailbox Permissions

When you create a new mailbox, Exchange uses information from the mailbox store to create the default permissions for the new mailbox. The default folders in the new mailbox inherit permissions from the mailbox itself. Users can modify the permissions on folders in their mailbox using Outlook. Outlook uses MAPI permissions, which Exchange automatically converts to Windows 2000 permissions when it is storing the changes.

Although you can use Exchange System Manager to delete or move mailboxes, you cannot use it to access mailbox content or mailbox-related attributes of the user. Use Active Directory Users and Computers to perform administrative tasks on the Exchange-related attributes of user objects. In addition, you must use Active Directory Users and Computers to give users permission to access the mailbox itself, as discussed in the next section.

### Designating a User as a Mailbox Delegate

For administration and troubleshooting purposes, there are times when you need to access a user's mailbox. There also may be occasions where it is appropriate for a second user to have access to a mailbox. This second user is referred to as a mailbox delegate.
You can give users delegate permissions for a mailbox by modifying the Active Directory user account that is associated with the mailbox. Use Active Directory Users and Computers for this task. You can give different levels of access to the mailbox:

- If you give the second user the access level of Full Mailbox Access, Exchange treats that user as the mailbox owner. The second user does not need any other permissions on folders in the mailbox.

  **Important**
  Always use care when modifying permissions. An unscrupulous user with Full Mailbox Access to other users' mailboxes could cause damage to the mailboxes or their contents.

- If you give the second user an access level other than Full Mailbox Access, the original mailbox owner can use Outlook to set permissions for the second user on folders in the mailbox.

To give someone access to another user's mailbox, you must have the appropriate permissions to modify user objects in Active Directory (see the Windows Help for more information about these permissions).

**To give a user full access to another user's mailbox**

1. In Active Directory Users and Computers, right-click the organization domain name, point to View, and then click Advanced Features.
2. Click the Users container or the organizational unit where the user is located.
3. Right-click the user account, and then click Properties.
4. Click Exchange Advanced, and then click Mailbox Rights.
5. Click Add to add a user to the list of users that are allowed to access this mailbox.
6. In the permissions list, for the Full Mailbox Access permission, select the Allow check box.

**To give a user the ability to send mail on behalf of another user**

1. In Active Directory Users and Computers, click the Users container or the organizational unit where the user is located.
2. Right-click the user account, and then click Properties.
3. Click Exchange General, and then click Delivery Options.
4. Click Add to specify a user.

  **Important**
  In this situation, the second user does not need permissions on the mailbox itself or items in the mailbox.
Using Public Folder Permissions

Controlling access to public folders is more complex than controlling access to mailboxes. This section presents information that will help you understand:

- The different types of permissions that can be set on public folders.
- What you need to consider when you work with client permissions. Be sure to read this section before modifying client permissions.
- What you need to consider when setting public folder permissions in an environment where Exchange 2003 and Exchange 5.5 servers coexist.
- How to designate a user as a public folder delegate.
- The minimum permissions that are required for mail-enabled public folders to function correctly.

Understanding the Three Types of Public Folder Permissions

You can control access to public folders using the following types of permissions:

- **Client permissions** These settings control who can use client applications to access folders and messages. By default, all users have permissions to read and write content in the public folder. You can change permissions for all users or create different permissions for specific users. The default client permissions do not include the Exchange administrative roles (Exchange Full Administrators, Exchange Administrators, or Exchange View Only Administrators).
  
  Depending on the type of public folder that you are working with, you may see different forms of the client permissions.
  
  - Folders in the **Public Folders** tree use MAPI permissions.
  - Folders in general-purpose public folder trees use Windows 2000 permissions.

- **Directory rights** These settings are normal Active Directory permissions, and control who can change the e-mail–related attributes of a mail-enabled public folder. Exchange stores these attributes in Active Directory, in the public folder's directory object in the Microsoft Exchange System Objects container. The default directory permissions include extensive permissions for the domain local Administrators group. Normally, any user that you have assigned to one of the Exchange administrative roles is a member of this group.

  - **Administrative rights** These settings control who can use Exchange System Manager (or a custom administration program) to change the replication, limits, and other settings for a public folder. Some of these permissions are inherited from the public folder store and include permissions for the Exchange administrative roles. These permissions are Windows 2000 permissions, although they reside only in the public folder store.
If you are working with a public folder tree that has multiple levels of public folders, you can modify client permissions or administrative rights for a single folder, and you can use the Propagate Settings command to propagate the changes to all subfolders of that folder. To propagate client permissions, use Propagate Settings with the Folder rights option. To propagate administrative rights, use Propagate Settings with the Administrative rights option.

Special Considerations for Working with Client Permissions

When you use Exchange System Manager to view client permissions for a public folder, the information that you see can depend on what type of folder tree you are working with. You also have access to different views of the same information. The procedures in this section provide information about how to use and how not to use the different views.

Important
Always use care when modifying permissions. An unscrupulous user with Owner permissions on a public folder could cause damage to the folder or its content, or could run malicious scripts.

To view permissions that control client access to a public folder

1. In Exchange System Manager, right-click the folder that you want to change, and then click Properties.
2. In the Properties dialog box, click the Permissions tab (see Figure 7.2), and then click Client permissions.

![Figure 7.2 The first Permissions tab that is displayed for a mail-enabled public folder](image)
After clicking **Client Permissions**, one of two different dialog boxes appears, depending on the type of public folder tree with which you are working:

- If you are working with a folder in the **Public Folders** tree, you see a dialog box that contains MAPI permissions and roles (see Figure 7.3a).
- If you are working with a folder in a general-purpose public folder tree, you see a dialog box that contains Windows 2000 permissions, users, and groups (see Figure 7.3b).

You can also use Exchange System Manager to view the Windows 2000 version of the permissions on a folder in the **Public Folders** tree.

**Warning**

Although you can view the Windows 2000 version of the **Public Folders** tree permissions, do not attempt to edit the permissions in this view. The Windows user interface that displays the permissions formats the ACL in such a way that Exchange will no longer be able to convert the permissions to their MAPI form. If this happens, you will no longer be able to use Outlook or the regular Exchange System Manager dialog boxes to edit the permissions.
To view the Windows 2000 version of MAPI permissions

1. In Exchange System Manager, right-click the folder whose permissions you want to view, and then click Properties.

2. In the Properties dialog box, click the Permissions tab, and then press and hold the CTRL key and click Client permissions.

The resulting dialog box is shown in Figure 7.4. Note that all of the permissions check boxes are cleared.

![Permissions dialog box for a folder in the Public Folders hierarchy](image)

Figure 7.4 Windows 2000 Permissions dialog box for a folder in the Public Folders hierarchy
3. To see the actual permissions information, click **Advanced**. The resulting dialog box is shown in Figure 7.5.

![Advanced version of the Windows 2000 Permissions dialog box](image)

**Figure 7.5** Advanced version of the Windows 2000 Permissions dialog box
4. To view detailed permissions information, click a permissions entry and then click View/Edit.

Remember, do not use this dialog box to edit the permissions. As stated earlier, using this interface to modify permissions would save the changes in a form that Exchange could not convert to the MAPI format. Figure 7.6 shows an example of the detailed Windows 2000 permissions information you can view.

![Figure 7.6 Detailed view of Windows 2000 permissions](image)

**Figure 7.6** Detailed view of Windows 2000 permissions
Special Considerations for Coexisting Exchange 2003 and Exchange 5.5 Servers

If your deployment includes both Exchange 2003 and Exchange 5.5 servers, you have an additional level of complexity to deal with when managing permissions, especially public folder permissions. Although the information that follows is technical, you must be aware of these details to ensure that your mixed-mode deployment operates smoothly. For a more detailed explanation of how Exchange passes access control information between Exchange 2003 and Exchange 5.5 servers, see the Exchange technical article, Public Folder Permissions in a Mixed-Mode Microsoft Exchange Organization (http://go.microsoft.com/fwlink/?LinkId=10228).

The important points in the article that relate to managing public folder permissions are the following:

- Before any data can be replicated between Exchange 2003 and Exchange 5.5 servers, any users or groups that have mailboxes on the Exchange 5.5 servers must have accounts in Active Directory.
  - If the user or group account has only an Active Directory account (not a Microsoft Windows NT® 4.0 account), the Active Directory account is an enabled account.
  - If the user or group has a Windows NT 4.0 account, the Active Directory account is a disabled account. This disabled account, created using the Active Directory Migration Tool, is a placeholder that associates an Active Directory security identifier (SID) with the existing Windows NT 4.0 account.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Important</strong> If you plan to maintain user accounts in Windows NT 4.0 for a period of time and then fully migrate those accounts to Active Directory, you need to create disabled accounts that have a SID history. The Active Directory Migration Tool can migrate the Windows NT 4.0 SID into the <strong>sidHistory</strong> attribute of the newly disabled account in Active Directory. If you enable the accounts at a later date, Exchange can use the SID history information to determine where newly enabled accounts have replaced Windows NT 4.0 accounts in access control entries (ACEs). For more information about this process, see Microsoft Knowledge Base Article 316047, &quot;XADM: Addressing Problems That Are Created When You Enable ADC-Generated Accounts&quot; (<a href="http://support.microsoft.com/?kbid=316047">http://support.microsoft.com/?kbid=316047</a>).</td>
</tr>
</tbody>
</table>

- Exchange 5.5 uses MAPI-based permissions, identifies users and groups by their distinguished names in the Exchange Directory, and uses a property called **ptagACLData** to store access control information. Exchange 2003 uses two additional properties, **ptagNTSD** and **ptagAdminNTSD**, to store access control information.
When Exchange 2003 replicates access control information to an Exchange 5.5 server, it does the following:

a. Converts the Active Directory security identifiers (SIDs) of users and groups to Exchange Directory distinguished names.

b. Converts the Windows 2000 permissions to MAPI permissions.

c. Stores the converted access control information in \texttt{ptagACLData}.

d. Replicates \texttt{ptagNTSD}, \texttt{ptagAdminNTSD}, and \texttt{ptagACLData} to the Exchange 5.5 server.

When an Exchange 2003 server receives data replicated by an Exchange 5.5 server, it does the following:

a. Discards the incoming values of \texttt{ptagNTSD} and \texttt{ptagAdminNTSD}. This step protects against any changes that may have been made to these properties while they were under the control of Exchange 5.5.

b. Extracts the user and group distinguished names from \texttt{ptagACLData} and converts them to Active Directory SIDs.

c. Extracts the permissions from \texttt{ptagACLData} and converts them to Windows 2000 permissions.

d. Stores the converted access control information in \texttt{ptagNTSD}. (The original value of \texttt{ptagAdminNTSD} remains unaffected.)

e. Discards the value of \texttt{ptagACLData}, unless a problem occurred during the conversion in Step b or Step c. If a conversion problem occurs, Exchange 2003 keeps the \texttt{ptagACLData} value.

- Exchange 5.5 applies permissions to folders. You cannot assign permissions to individual messages (item-level permissions) explicitly, as you can with Exchange 2003. If you are replicating folders and their contents from Exchange 5.5 to Exchange 2003, do not attempt to set explicit permissions on messages. Exchange 2003 manages permissions so that the messages are secure, but if you attempt to change the message permissions in this situation, the changes will be lost in the next replication cycle.

### Designating a User as a Public Folder Delegate

You can configure a mail-enabled public folder so that a user can send mail on the public folder's behalf. For example, if the folder serves as a shared storage location or workspace for a group of users, one user could send notifications to the group. A custom application could also perform such a function, if you created an account for it to use.
To give a user the ability to send mail on behalf of a public folder

1. In Exchange System Manager, under Folders, right-click the public folder for which you want to give a user the ability to send mail and click Properties.
2. Click Exchange General, and then click Delivery Options.
3. Click Add to specify a user.
4. You may need to make additional modifications if the following conditions apply:
   - The user's mailbox resides in a domain that is different from the public folder's domain.
   - The user's mailbox resides on a server that is located in a site that does not contain any domain controllers for the domain that hosts the public folder.

Use one of the following additional steps:
   - Add the Exchange Domain Servers security group of the child domain with Read permissions to the ACL of the Microsoft Exchange System Objects container in the parent domain. This method is the recommended method for working around this problem.
   - Move one domain controller from the parent domain to the user's Exchange 2003 site.

Maintaining the Minimum Permissions Required for Mail-Enabled Public Folders

If you modify the default client permissions and roles on a mail-enabled public folder, make sure you maintain the Contributor role for the Anonymous account. Otherwise, mail sent to the public folder will be returned as undeliverable. When the public folder receives e-mail from a user who has no permissions on the folder, it treats the mail as a message posted using the Anonymous account.

Note
This is a change from Exchange 5.5, where the default role of the Anonymous account was None.

Maintaining the Minimum Permissions Required for Mailbox Stores and Public Folder Stores

If you modify the default permissions on Exchange Server 2003 mailbox stores and public folder stores, make sure you maintain the following minimum permissions:

- **Administrators group** Full Control
- **Authenticated Users group** Read and Execute, List Folder Contents, and Read
• **Creator Owner**  None
• **Server Operators group**  Modify, Read and Execute, List Folder Contents, Read, and Write
• **System account**  Full Control

You may experience difficulties in mounting the mailbox stores or public folder stores if you do not maintain these permissions for these groups and accounts. The following error messages and events indicate that the accounts and groups in the preceding list do not have the correct permissions:

• An internal processing error has occurred. Try restarting Exchange System Manager or the Microsoft Exchange Information Store service, or both.
• MAPI or an unspecified service provider. ID no: 00000476-0000-00000000.
• Information Store (2520) An attempt to determine the minimum I/O block size for the volume "[drive:]" containing "[drive:]Exchsrvr\Mdbdata\" failed with system error 5 (0x00000005): "Access is denied." The operation will fail with error –1032 (0xfffffbf8).
• Error 0xfffffbf8 starting Storage Group [dn of storage group] on the Microsoft Exchange Information Store.
• The MAPI call 'OpenMsgStore' failed with the following error: The Microsoft Exchange Server computer is not available. Either there are network problems or the Microsoft Exchange Server computer is down for maintenance. The MAPI provider failed. Microsoft Exchange Server Information Store ID no: 8004011d-0526-00000000.

You may also encounter problems when mounting public folder stores if you have cleared the Allow inheritable permissions from parent to propagate to this object option for the public folder hierarchy. The following error messages indicate that you have cleared this option:

• The store could not be mounted because the Active Directory information was not replicated yet.
• The Microsoft Exchange Information Store service could not find the specified object. ID no: c1041722

**To restore the permissions required by Exchange**

1. In Exchange System Manager, right-click the public folder tree, and then click **Properties**.
2. In the **Properties** dialog box, click the **Security** tab, click **Advanced**, and then select Allow inheritable permissions from parent to propagate to this object.
3. Wait for Active Directory to replicate the change to all of the domain controllers.
4. Right-click the public folder store and click **Mount Store**.
Managing Storage Groups and Stores

The Exchange store uses two types of databases:

- Mailbox stores
- Public folder stores

These databases (or stores) are organized into storage groups. All of the databases in a storage group share a single set of transaction log files, a single backup schedule, and a single set of logging and backup-related settings.

Exchange System Manager lists the storage groups for each server, and the mailbox stores and public folder stores in those storage groups. To view stores and storage groups in Exchange System Manager, expand the server node in the Exchange System Manager console tree. Figure 7.7 shows the mailbox and public folder stores in the First Storage Group of a single server.

![Exchange System Manager](image)

*Figure 7.7 Store information in Exchange System Manager*
If you are using Exchange Server 2003 Standard Edition, each Exchange server can have one storage group, which contains one mailbox store and one public folder store. If you are using Exchange Server 2003 Enterprise Edition, each server can have as many as four storage groups, each of which contains as many as five databases (either mailbox stores or public folder stores).

Using either Exchange Server 2003 Standard Edition or Exchange Server 2003 Enterprise Edition, you can create a Recovery Storage Group in addition to your other storage groups. Use this special storage group to recover mailbox data when restoring data from a backup. For more information about how to configure and use a Recovery Storage Group, see "Recovering Mailbox Stores and Mailboxes with a Recovery Storage Group" in the Exchange Server 2003 Help.

You can use multiple mailbox stores to increase the reliability and recoverability of your Exchange organization. If the users are spread across multiple mailbox stores, the loss of a single store impacts only a subset of the users rather than the entire organization. In addition, reducing the number of users per store reduces the time that you need to recover a damaged store from a backup.

**Note**
Increasing the number of mailbox stores on a server can increase the server resources consumed relative to the resources consumed for the same number of users in a single store. However, the benefits of using multiple stores usually outweigh the resource costs.

You can use multiple public folder stores to spread public folders across multiple servers. You can place multiple replicas of the same folder on several servers, to increase the system's ability to handle user traffic. If you have multiple routing groups, you may want to distribute folders among the routing groups so that users have easy access to the folders that they use most often.

This section includes information about the following:

- For each storage group, how to configure settings for the transaction logs.
- For each storage group, how to overwrite deleted data during backups.
- How to add new storage groups.
- How to mount or dismount stores.
- For each store, how to move the database files out of the system directory. This task is the same for mailbox stores and public folder stores.
- For each store, how to configure maintenance and backup options. These tasks are the same for mailbox stores and public folder stores.
- How to create and configure mailbox stores. These tasks are specific to the type of store that you are working with.
- How to create and configure public folder stores. These tasks are specific to the type of store that you are working with.
Configuring Transaction Logs for a Storage Group

The most important aspect of a storage group is its transaction logs. Even if you use only the default **First Storage Group**, you need to consider your transaction log configuration to be sure that you can recover data if the stores are damaged.

In the standard transaction logging that Exchange uses, each store transaction (such as creating or modifying a message) in a storage group is written to a log file and then to the store. When it is written to the log file, each transaction is labeled with an identifier that Exchange uses to associate the transaction with a particular store. In this manner, all of the stores in a storage group share a single set of transaction logs.

This process ensures that records of transactions exist if a store is damaged between backups. In many cases, recovering a damaged store means restoring the store from a backup, replaying any backed-up log files, and then replaying the most recent log files to recover transactions that were made after the last backup.

**Note**

For detailed information about how transaction logs work and how to recover store data in a variety of circumstances, see the book *Disaster Recovery for Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?LinkID=18350). Although existing functionality has not changed, Exchange Server 2003 has new recovery features. For more information about the new recovery features, see the book *What's New in Exchange Server 2003* (www.microsoft.com/exchange/library).

When a log file reaches 5 megabytes (MB), it is renamed and a new log file is started. As the number of transactions grows, a set of log files is created. The set continues to grow until you run a full backup (also called a normal backup) or an incremental backup. As part of the backup process, old transaction logs are removed and the current log file becomes the first file of a new log file set. You can control the size of the log file set by using a regular schedule of backups. Using the Windows 2000 backup utility or a third-party backup product, any storage group or database can be backed up at any time.

You can perform four types of online backups on the Exchange store:

- **Full backup** A full backup (called a normal backup in Windows Backup) backs up the store and transaction log files. After the backup, transaction log files in which all transactions are complete are deleted.

- **Copy backup** A copy backup backs up the store and transaction log files, but leaves the transaction logs in place.
Chapter 7: Managing Mailbox Stores and Public Folder Stores

- **Incremental backup**  An incremental backup backs up the transaction logs and removes all transaction logs in which all transactions are completed.
- **Differential backup**  A differential backup backs up the transaction logs, but leaves them in place.

**Important**
You can perform an incremental or differential backup only if you have previously performed a normal backup. If you need to recover a store, you must recover the store itself from the last normal backup, and then you can recover log files from an incremental or differential backup.

**To configure transaction logs and choose other storage group options**
- In Exchange System Manager, right-click the storage group, and then click Properties. Figure 7.8 shows the options that are available for configuring a storage group.

![Figure 7.8 The storage group Properties dialog box](image-url)
Moving Transaction Log Files to a Separate Drive

When you install Exchange, Setup creates transaction log files and database files on the same drive. You can significantly improve the performance and fault tolerance of an Exchange server by placing its transaction log files and database files on separate drives. Because these files are critical to the operation of a server, the drives should be protected against failure, ideally by hardware mirroring using redundant array of independent disks (RAID). It is recommended that you use RAID 1, RAID 0+1, or RAID 10. Use the NTFS file system for transaction log drives.

For optimum performance, the set of transaction logs for each storage group should be placed on a separate drive. Because each storage group has its own set of transaction logs, the number of dedicated transaction log drives for your server should equal the number of planned storage groups. Although it is possible to place multiple sets of transaction logs on the same drive, if you do so server performance may decline significantly.

Tip
Distribute your database drives across many Small Computer System Interface (SCSI) channels or controllers, but configure them as a single logical drive to minimize SCSI bus saturation.

An example disk configuration is as follows:

- C:\ System and boot (mirror set)
- D:\ Pagefile
- E:\ Transaction logs for storage group 1 (mirror set)
- F:\ Transaction logs for storage group 2 (mirror set)
- G:\ Database files for both storage groups (multiple drives configured as hardware stripe set with parity)

To configure new locations for the transaction logs

1. In Exchange System Manager, right-click the storage group and click Properties.
2. On the General tab, specify a new location for the files.
   For example, if the E:\ drive will contain only log files for this storage group, in Transaction log location, click Browse, and then choose the E:\ drive.
Using Circular Logging

Circular logging overwrites and reuses a single log file after the data that it contains has been written to the database. Circular logging is disabled by default. By enabling circular logging, you reduce drive storage space requirements. However, you cannot recover anything more recent than the last full (normal) backup, because the transaction logs no longer contain all of the transactions that were completed since the last backup. Therefore, in a normal production environment, circular logging is not recommended.

Warning
Using the Enable circular logging option prevents you from creating a set of log files, and you can restore only from your last backup. Reserve this option for storage groups that support Network News Transfer Protocol (NNTP) folders (in public folder stores), which do not require log files.

Overwriting Deleted Data During Backup

As with most applications, data that Exchange deletes is not actually removed from the disk. Although Exchange treats it as deleted data, it usually remains until it is overwritten by more recent data. If you want to make sure that deleted data is overwritten on a regular basis, use the Zero out deleted database pages option. When this option is enabled, Exchange overwrites chunks of deleted data during the online backup process.

Important
Enabling the Zero out deleted database pages option can slow backup performance and increase the size of the database files. The option is turned off by default.

Adding a Storage Group

A storage group includes between one and five databases (mailbox stores and public folder stores) and one set of transaction log files for those databases. You may want to add a storage group under the following conditions:

- You want to have more than five databases on a particular server. For example, to improve the backup or recovery time for each mailbox store, you increase the number of mailbox stores and put fewer users in each store.

- You have databases with different backup or restore requirements. For example, you have one database that you cannot afford to have offline for more than a few hours, even if it must be completely reconstructed.
To create a new storage group

1. In Exchange System Manager, right-click the server where the new storage group will reside, point to New, and click Storage Group.

2. When prompted, type a name for the storage group. Exchange fills in default values for Transaction log location and System path location. You can change the defaults, or you can change these values at a later time.

Mounting or Dismounting Stores

A mounted store is a store that is operating normally and is available for user and administrator access. If the store is dismounted or offline, no users can access it and you may not be able to view or change all of the store properties. In most cases, Exchange mounts and dismounts stores automatically, if needed. For example, if you move a store's database files to a new directory, the store will be dismounted automatically until the move is complete.

Under certain conditions, you may need to mount or dismount stores manually. For example, you can configure stores so that, if the server restarts, the store must be mounted manually. That way you can check the server for problems before allowing users to access the store again. For more information, see "Configuring Store Maintenance and Backup Options" later in this chapter.

The Mount Store and Dismount Store commands are available in the Action menu for each store that appears in Exchange System Manager.

Note
If you do not have permissions on a particular store, the store may appear to be dismounted in Exchange System Manager when it is actually running. This may occur if you are using a distributed administration model, with multiple administrative groups with separate administrators. Each administrator will only be able to interact with the stores in that administrator's own administrative group.

Moving Store Files to a New Directory

When you install Exchange, Setup creates database files on the same drive as the Exchange program files. To get better performance and more storage space, you can move the Exchange databases (mailbox stores and public folder stores) out of the default drive or directory. The stores are dismounted automatically during the move, and will not be available to users.

Tip
Distribute your database drives across many SCSI channels or controllers, but configure them as a single logical drive to minimize SCSI bus saturation.
When you move a store, remember the following:

- Use Exchange System Manager on the server on which the stores reside to move the .edb and .stm database files of the stores. Moving these files requires that you specify new file locations on the Database tab of the Properties dialog box (see Figure 7.9 in the next section).

- You should perform a normal backup when the move is finished. This process backs up and removes existing transaction log files, and simplifies future recovery operations.

For more information about recovery operations and transaction log files, see the book *Disaster Recovery for Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?LinkId=18350).

### Configuring Store Maintenance and Backup Options

The maintenance processes and backup options are the same for mailbox stores and public folder stores. You can check and configure these options on the Database tab (see Figure 7.9) of the store that you want to check or configure.

![Figure 7.9 The Database tab for a mailbox store](image)
The **Database** tab for a mailbox store includes the following maintenance and backup options.

- **Maintenance interval**  Specifies the schedule for the automatic database maintenance process. This process:
  
  - Checks that none of the storage limit settings have been exceeded on any mailbox or public folder.
  - Sends mail to the administrator or the mailbox owner if storage limits have been exceeded.
  - Checks for deleted items that have been retained for the amount of time configured for the store.
  - Checks for and deletes expired items in the folders if age limits have been set on any public folders.

  Because this process can consume significant server resources, you should schedule it to run during off-peak hours.

  **Note**
  For more information about the settings that the maintenance process enforces, see "Configuring the Default Mailbox Limits," "Configuring the Default Public Folder Limits," and "Configuring Limits on a Specific Public Folder Replica" later in this chapter.

- **Do not mount this store at start-up**  When this option is selected, the mailbox store does not mount automatically when Exchange is started. By default, this check box is cleared.

- **This database can be overwritten by a restore**  Do not use this option for normal restore operations. Select this option only if a restore operation fails with an error that indicates the database cannot be overwritten. By default, this option is not selected.
Configuring Mailbox Stores

Mailboxes are the delivery location for all incoming mail messages for a designated owner. A mailbox can contain messages, message attachments, folders, documents, and other files. Information in a user's mailbox is stored in a mailbox store on an Exchange server. Figure 7.10 shows a list of the mailboxes on a single mailbox store.

Figure 7.10  Mailbox store information in Exchange System Manager

Mailboxes inherit many of their properties (such as storage limits) from the mailbox store. You can create different mailbox stores for different groups of users. For example, you may place mailboxes for workers in one store and mailboxes for executives in another store, and give the executives double the normal storage limits by configuring the store instead of configuring the individual mailboxes.

This section describes the following:

- The relationship between a mailbox store and its associated public folder store.
- Single instance storage of messages (when it applies and when it does not).
- How to add a mailbox store.
• How to configure the default mailbox storage limits and the length of time that deleted items and mailboxes will be retained.
• How to control mailbox store settings with system policies.
• Interfaces to use for monitoring mailbox store activity.

For information about configuring the store for full-text indexing updates, see Appendix F, "Using Full-Text Indexing."

### Linking Mailbox Stores and Public Folder Stores

Each mailbox store must be associated with a public folder store. You specify the public folder store when you create a mailbox store. The public folder store that is installed by default on each server supports the **Public Folders** tree (also called the MAPI public folder tree). You can have only one **Public Folders** tree in your Exchange organization, and it is associated with each server's default public folder store.

**Note**
Using the default public folder store on the same server as the mailbox store may improve performance when users access public folders, and may make it easier to troubleshoot public folder access problems.

For more information about public folder trees and the default public folder store, see "Configuring Public Folder Stores" and "Managing Public Folders" later in this chapter.

### Understanding Single Instance Message Storage

To help control the size of the mailbox stores, Exchange supports single instance message storage. This means that when a message is sent to more than one mailbox in the same store, only one instance of the message is stored, in one mailbox. The other mailboxes contain pointers to the stored message.

If the message is sent to mailboxes in a different mailbox store, the message is written once to each mailbox store.

Single instance storage may not be maintained when a mailbox that contains a message is moved to a server that contains a mailbox store with the same message.

**Tip**
To maximize single instance message storage, place similar users in the same mailbox store, such as users in the same department who use Reply All or users that send large attachments to one another frequently.
Adding a Mailbox Store

**To create a new mailbox store**

1. In Exchange System Manager, right-click the storage group where the new store will reside, point to New, and click Mailbox Store.

2. When prompted, type a name for the mailbox store.
   Exchange automatically selects a default public store (associated with the Public Folders tree) and offline address book (which users will download for offline use) for your new mailbox store.

   You can modify these options now or at a later time (by right-clicking the mailbox store and clicking Properties). Figure 7.11 shows the properties of a mailbox store.

   ![Figure 7.11 The General tab for a mailbox store](image)

   For more information about creating mailboxes, see "Managing Mailboxes" later in this chapter.
Configuring the Default Mailbox Limits

Using the limits settings in the Limits tab, you can control the maximum size of mailboxes in the mailbox store and control how deleted items are handled. You can access the limits settings on the Limits tab of the mailbox store’s Properties dialog box (see Figure 7.12).

![Figure 7.12 The Limits tab for a mailbox store](image)

**Note**
For an individual user, you can override the store’s limits settings by using Active Directory Users and Computers to configure limits settings for the user.

Table 7.2 describes the possible limits that can be set for a mailbox store. By default, no limits are set.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue warning at (KB)</td>
<td>When a user’s mailbox exceeds the specified size limit, the user receives an e-mail alert to delete messages from the mailbox. By default, this option is not selected.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Prohibit send at (KB)</strong></td>
<td>When a user's mailbox exceeds the specified size limit, the user receives an e-mail alert to delete messages from the mailbox. In addition, the user is unable to send e-mail messages until the mailbox size is reduced below the specified limit. By default, the option is not selected.</td>
</tr>
<tr>
<td><strong>Prohibit send and receive at (KB)</strong></td>
<td>When a user's mailbox exceeds the specified size limit, the user receives an e-mail alert to delete messages from the mailbox. In addition, the user is unable to send e-mail messages until the mailbox size is reduced below the specified limit, and incoming e-mail messages are returned to the sender with a non-delivery report (NDR).</td>
</tr>
<tr>
<td><strong>Warning message interval</strong></td>
<td>Use this drop-down list to schedule when warning messages are generated. You can select one of the standard maintenance schedules, or click <strong>Customize</strong> to set up your own schedule. This process is CPU-intensive and disk-intensive, and can slow server performance. You should schedule maintenance of this type at off-peak times.</td>
</tr>
<tr>
<td><strong>Keep deleted items for (days)</strong></td>
<td>You can designate the number of days that deleted items (such as e-mail messages) remain on the server before they are removed permanently. You can type a number from 0 to 24855. If you type 0, deleted items are removed from the server immediately. As long as deleted items remain on the server, Outlook users can retrieve them using Outlook’s <strong>Recover Deleted Items</strong> function.</td>
</tr>
<tr>
<td><strong>Keep deleted mailboxes for (days)</strong></td>
<td>You can designate the number of days that deleted mailboxes remain on the server before they are removed permanently. After this value is set, you have the specified number of days to recover mailboxes that were deleted by accident. You can type a number from 0 to 24855. If you type 0, deleted mailboxes are removed from the server immediately.</td>
</tr>
<tr>
<td><strong>Do not permanently delete mailboxes and items until the store has been backed up</strong></td>
<td>You can keep deleted mailboxes and items on the server until a backup is performed. After a backup is performed, mailboxes and items are deleted, according to the settings that you specified.</td>
</tr>
</tbody>
</table>
Setting Up Mailbox Store Policies

You can create policies to manage mailbox stores in the same way that you create other system policies. For detailed information about all types of system policies, see "Using System Policies" in Chapter 2, "Managing an Exchange Organization."

You can set the following options using policies:

- **General** tab
  - Default public store
  - Offline address list
  - Archive all messages sent or received by mailboxes on this store
  - Clients support S/MIME signatures
  - Display plain text messages in a fixed-size font

- **Database** tab
  - Maintenance interval

- **Limits** tab
  - Issue warning at (KB)
  - Prohibit send at (KB)
  - Prohibit send and receive at (KB)
  - Warning message interval
  - Keep deleted items for (days)
  - Keep deleted mailboxes for (days)
  - Do not permanently delete mailboxes and items until the store has been backed up

- **Full-Text Indexing** tab
  - Update interval

Use the **System Policies** node in Exchange System Manager to create and apply policies. After you create a mailbox store policy, you can apply that policy to one or more mailbox stores on any server.

**Note**
You can only apply a policy to a store if you have permissions to modify that store. If you are using a distributed administration model, with multiple administrative groups that have separate administrators, each administrator will only be able to interact with the stores in that administrator's own administrative group.
To apply a policy to one or more mailbox stores

1. In Exchange System Manager, right-click the policy, and click **Add Mailbox Store**.
2. Select the appropriate stores.

After you have applied the policy, the options that the policy controls are no longer available in the mailbox store's **Properties** dialog box. This prevents local settings from overriding the policy. For a list of all of the policies that are applied to a particular mailbox store, go to that mailbox store's **Policies** tab.

### Monitoring Mailbox Store Activity

Exchange System Manager provides up-to-date information about items in the mailbox store. You can use this information for troubleshooting system problems, or evaluating whether the system needs tuning or reconfiguring. For example, Figure 7.13 shows the list of mailboxes in a mailbox store, the users that have been accessing those mailboxes, and the size of the mailboxes. Except where noted, Exchange View Only Administrators can access this information.

![Figure 7.13 Mailbox store information in Exchange System Manager](image-url)
Table 7.3 lists the status information that is available for each of the nodes under the mailbox store.

To display different columns of information in the right pane, click the node that you want to view. On the View menu, click Add/Remove columns, and then select the types of information that you want to display. For a detailed listing of the available columns, see "Administer a Mailbox Store" in the Exchange Server 2003 Help.

Table 7.3 Status information for a mailbox store

<table>
<thead>
<tr>
<th>Node</th>
<th>Status Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logons</strong></td>
<td>Users that are currently logged on to their mailboxes, and their activities.</td>
</tr>
<tr>
<td></td>
<td>Use this information to look for mailbox users that are unusually active or inactive. The <strong>Total Ops</strong> column is especially useful for this purpose.</td>
</tr>
<tr>
<td></td>
<td>You must be at least an Exchange Administrator to view this information.</td>
</tr>
<tr>
<td><strong>Mailboxes</strong></td>
<td>Current mailboxes in the store.</td>
</tr>
<tr>
<td></td>
<td>Although this node provides information about mailboxes, it does not provide access to the messages in the mailboxes.</td>
</tr>
<tr>
<td></td>
<td>You must be at least an Exchange Administrator to view this information.</td>
</tr>
<tr>
<td><strong>Full-Text Indexing</strong></td>
<td>Status of current full-text indexes.</td>
</tr>
</tbody>
</table>

You can also use the Windows Performance application to monitor activity related to the mailbox store. The following counters (available on the MSExchangeIS Mailbox performance object) provide especially useful information:

- Average Delivery Time
- Local delivery rate
- Logon Operations/sec
- Folder opens/sec
- Message Opens/sec
- Message Delivered/min
- Messages Sent/min
- Message Submitted/min
- Receive Queue Size

For more information about how to use these counters, see the Windows Performance Help.
Configuring Public Folder Stores

A public folder store holds information associated with a particular public folder tree, such as how the tree is structured and what folders the tree contains. It also holds public folder content.

Each new Exchange server has one default public folder store (called Public Folder Store). This store supports the Exchange default public folder tree, which is called Public Folders in Exchange System Manager and All Public Folders in Outlook, and is sometimes called the MAPI public folder tree. Users can access this tree with MAPI-based clients, such as Outlook, and with HTTP-based clients, such as Microsoft Outlook® Web Access. There is only one Public Folders tree in each Exchange organization, and all of the default public folder stores replicate this tree and its content amongst themselves.

You can create new public folder trees, called general-purpose public folder trees, (also called non-MAPI public folder trees). Users can access folders in general-purpose trees using Web-based clients, NNTP clients, and standard Windows applications in which the folders are mapped as network drives using WebDAV. Use general-purpose public folder trees as file repositories for departments, groups, or projects. For more information, see "Configuring a New Public Folder Tree and Public Folder Store" later in this section.

If you create a new public folder tree, you can then create an additional public folder store to support that tree. Each server can only have one store for each public folder tree. In other words, the server can have multiple public folder stores if each store supports a different public folder tree. For more information, see "Creating a New Public Folder Store for an Existing Public Folder Tree" later in this section.

Figure 7.14 shows an example of a set of public folder servers that support multiple trees:

- Each server has a Public Folder Store, which supports the Public Folders tree.
- Two servers also support a second public folder tree. These servers run one public folder store per tree.

![Figure 7.14 Multiple public folder trees, each spread across multiple servers](image)
If you try to create a public folder store without an available public folder tree, the following error message appears:

All the public folder trees already have an associated public store on the server. You need to create a new public folder tree before creating this new public folder store.

Figure 7.15 shows where to find public folder store information in Exchange System Manager.
This section describes the following:

- Functions of the Public Folder Store, especially when it is associated with a mailbox store.
- How to add a public folder store when you work with an existing public folder tree.
- How to configure a new public folder tree and public folder store.
- How to configure the default public folder storage limits:
  - Maximum size of public folders and of individual items in the folders.
  - Length of time deleted items are retained.
  - Age limits for items in public folders.
- How to control public folder store settings with system policies.
- Interfaces to use for monitoring public folder store activity.

For information about configuring the store's options for the default public folder replication interval, see Appendix E, "Controlling Public Folder Replication."

**Understanding the Relationship Between Mailbox Stores and Default Public Folder Stores**

Each mailbox store is associated with a default public folder store, either on the local server or another server. For each mailbox-enabled user that is supported by a particular mailbox store, the associated public folder store is the user's home public folder store. If possible, you should use the default public folder store on the same server as the mailbox store. This improves performance when users access public folders, and may make it easier to troubleshoot public folder access problems.

**Creating a New Public Folder Store for an Existing Public Folder Tree**

A tree can have multiple stores when each store exists on a separate server. In such a configuration, Exchange replicates information among the stores to keep the tree consistent.

**To create a public folder store on a new server for an existing tree**

1. In Exchange System Manager, on a server that does not already have a store for the tree with which you are working, right-click a storage group, point to New, and then click Public Store.

2. When prompted, select the existing tree that you want to use for this store, and then finish creating the store.

3. In Exchange System Manager, under the Folders node, go to the tree that you are working with and configure the folders that you want to replicate to the new store.
Configuring a New Public Folder Tree and Public Folder Store

In Exchange System Manager, each new public folder tree exists at the same level as the Public Folders tree. You must create the tree first, and then create the store. If you want multiple servers to support this tree, first create the tree, create a store associated with that tree on each server, and then configure folders to replicate. For more information, see Appendix E, "Controlling Public Folder Replication."

To create a new hierarchy and public folder store

1. In Exchange System Manager, right-click the Folders node, point to New, and then click Public Folder Tree.
2. In the Properties dialog box (see Figure 7.16), in the Name box, type a name for the new tree.
   
   ![Figure 7.16 The Properties dialog box for a new public folder tree](image)

3. In Exchange System Manager, on the server that you want to host the new store, right-click a storage group, point to New, and then click Public Store.
4. On the new store's **General** tab (see Figure 7.17), type a name for the new store and then, under **Associated public folder tree**, click **Browse**.

![Figure 7.17 The General tab for a new public folder store](image)

5. In the **Select a Public Folder Tree** dialog box, choose a public folder tree.

6. In Exchange System Manager, under the node for the server that holds the new store, double-click **Protocols**, right-click **HTTP**, point to **New**, and then click **HTTP Virtual Server**.

7. When prompted, provide a name for the virtual server and select the new public folder tree.

When you have finished configuring this virtual server, Exchange automatically configures a corresponding Web site using Microsoft Internet Information Services (IIS). Users access the public folder with Outlook Web Access using this Web site. For more information about configuring HTTP virtual servers and IIS Web sites, see the book *Exchange Server 2003 Deployment Guide* (www.microsoft.com/exchange/library).
Configuring the Default Public Folder Limits

Use the limits settings to control the maximum size of public folders in the public folder store, the maximum size of messages in the public folders, and how deleted items are handled. You can access the limits settings on the Limits tab of the public folder store's Properties dialog box (see Figure 7.18).

![Figure 7.18 The Limits tab for a public folder store](image)

Table 7.4 describes the options that you can set on the Limits tab for a public folder store.

**Warning**
Do not set an age limit on folders that contain Contact or Calendar items.

**Note**
You can also set limits on individual public folders that override the store settings. If you use only the store settings, the same folder may have different limits on different servers. If you use individual folder settings, the limits are the same for all replicas of the folder.
Table 7.4 Options available on the Limits tab for a public folder store

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issue warning at (KB)</strong></td>
<td>When a folder exceeds the specified size limit, the administrator receives an e-mail alert to delete messages from the folder. You can type a number from 0 to 2097151. By default, this option is not selected.</td>
</tr>
<tr>
<td><strong>Prohibit post at (KB)</strong></td>
<td>When a folder exceeds the specified size limit, the administrator receives an e-mail alert to delete messages from the folder. In addition, no users can post messages to the folder until the folder size is reduced below the specified limit. You can type a number from 0 to 2097151. By default, this option is not selected.</td>
</tr>
<tr>
<td><strong>Maximum item size (KB)</strong></td>
<td>The maximum size for individual messages that can be posted to the folder. You can type a number from 0 to 2097151.</td>
</tr>
<tr>
<td><strong>Warning message interval</strong></td>
<td>Use this drop-down list to schedule when warning messages are generated. You can select one of the standard maintenance schedules, or click <strong>Customize</strong> to set up your own schedule. This process is CPU-intensive and disk-intensive, and can slow server performance. You should schedule maintenance of this type at off-peak times.</td>
</tr>
<tr>
<td><strong>Keep deleted items for (days)</strong></td>
<td>You can designate the number of days that deleted items (such as messages in a folder) remain on the server, before they are removed permanently. You can type a number from 0 to 24855. If you type 0, deleted items are removed from the server immediately. Because items deleted from public folders are not held in a Deleted Items folder, if you set this option, you can recover deleted items without having to use a backup of the public folder.</td>
</tr>
<tr>
<td><strong>Do not permanently delete items until the store has been backed up</strong></td>
<td>You can keep deleted items on the server until a backup is performed. After a backup is performed, items are deleted, according to the settings that you specified. You can use this setting for folders that contain important information. For other folders, such as Newsgroup folders, you may want to leave this setting cleared to save storage space.</td>
</tr>
<tr>
<td><strong>Age limit for all folders in this store (days)</strong></td>
<td>The number of days after which items in this folder will be deleted automatically if they have not been modified.</td>
</tr>
</tbody>
</table>
Configuring Limits on a Specific Public Folder Replica

You can set additional age limits, which affect only a specific public folder replica. These limits override limits set on the folder (using the folder's Properties dialog box), but only in the public folder store where you set them. Other replicas of the public folder (on other servers) are not affected.

To view these additional age limit settings

1. In Exchange System Manager, under the public folder store node, click Public Folder Instances.

2. In the right pane, right-click the folder you want, and then click Replica Properties. The Replica Properties dialog box appears (see Figure 7.19).

![Figure 7.19   The Replica Properties dialog box for a public folder on a specific store](image)
This dialog box lists all of the limits that are applied to this folder instance:

- **Age limit of all replicas of this folder (days)** This is the limit (if any) that is set in the public folder's properties.
- **Age limit of all folders on this public store (days)** This is the limit (if any) that is set in the public folder store's properties.
- **Effective age limit of this folder on this public store (days)** This is the final value of the age limit for this replica.

To set a specific age limit for this folder replica, click **Age limit of this folder on this public store (days)** and type a value. Exchange automatically updates **Effective age limit of this folder on this public store (days)**.

### Setting Up Public Folder Store Policies

You can create policies to manage public folder stores in the same way that you create other system policies. You can set the following options using policies:

- **General** tab
  - Clients support S/MIME signatures
  - Display plain text messages in a fixed-size font

- **Database** tab
  - Maintenance interval

- **Replication** tab
  - Replication interval
  - Replication interval for always (minutes)
  - Replication message size limit (KB)
• **Limits** tab
  • Issue warning at (KB)
  • Prohibit send at (KB)
  • Prohibit send and receive at (KB)
  • Warning message interval
  • Keep deleted items for (days)
  • Do not permanently delete items until the store has been backed up
  • Age limit for all folders in this store (days)

• **Full-Text Indexing** tab
  • Update interval

Use the **System Policies** node in Exchange System Manager to create and apply policies. After you create a public folder store policy, you can apply that policy to one or more public folder stores on any server.

**To apply a policy to one or more public folder stores**

1. In Exchange System Manager, right-click the policy, and click **Add Public Store**.
2. Select the appropriate stores.

After you have applied the policy, the options that the policy controls are no longer available in the public folder store's **Properties** dialog box. For a list of all of the policies that are applied to a particular public folder store, go to that store's **Policies** tab.

**Note**
You can only apply a policy to a store if you have permissions to modify that store. If you are using a distributed administration model, with multiple administrative groups that have separate administrators, each administrator will be able to interact only with the stores in that administrator's own administrative group.
Monitoring Public Folder Store Activity

Exchange System Manager provides up-to-date information about items in the public folder store. You can use this information for troubleshooting system problems, or for evaluating whether the system needs to be tuned or reconfigured. For example, Figure 7.20 shows the list of public folders in a public folder store, and the location of each folder in the public folder tree. Except where noted later in this section, Exchange View Only Administrators can access this information.

![Public folder store information in Exchange System Manager](image)

Figure 7.20  Public folder store information in Exchange System Manager
Table 7.5 lists the status information that is available in Exchange System Manager for a public folder store.

To display different columns of information in the right pane, click the node that you want to view, click Add/Remove columns on the View menu, and select the types of information that you want to display. For a detailed listing of the columns that are available for you to view, see "Administer a Public Folder Store" in the Exchange Server 2003 Help.

Table 7.5 Status information for a public folder store

<table>
<thead>
<tr>
<th>Node</th>
<th>Status Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logons</td>
<td>Users that are currently logged on to the public folders.</td>
</tr>
<tr>
<td></td>
<td>Use this information to look for users that are unusually active or inactive. The</td>
</tr>
<tr>
<td></td>
<td>Total Ops column is especially useful for this purpose.</td>
</tr>
<tr>
<td></td>
<td>You must be at least an Exchange Administrator to view this information.</td>
</tr>
<tr>
<td>Public Folder Instances</td>
<td>Current public folder replicas in the store, and their replication configuration.</td>
</tr>
<tr>
<td>Public Folders</td>
<td>Current public folders in the store.</td>
</tr>
<tr>
<td></td>
<td>Although this node provides information about the folders, it does not provide</td>
</tr>
<tr>
<td></td>
<td>access to messages in the folders.</td>
</tr>
<tr>
<td>Replication</td>
<td>Replication status of the public folders in this store.</td>
</tr>
<tr>
<td>Full-Text Indexing</td>
<td>Status of current full-text indexes.</td>
</tr>
</tbody>
</table>

You can also use the Windows Performance application to monitor activity related to the public folder store. The following counters (available on the MSExchangeIS Public performance object) provide especially useful information:

- Average Delivery Time
- Folder opens/sec
- Message Opens/sec
- Message Delivered/min
- Receive Queue Size

For more information about how to use these counters, see the Windows Performance Help.
Managing Mailboxes

Mailbox information resides both in Active Directory (in mailbox-enabled user objects) and in mailbox stores. Although this section mentions ways to work with mailbox-enabled users in Active Directory, it focuses on the storage aspects of mailboxes:

- Creating a mailbox by mailbox-enabling a user in Active Directory
- Deleting mailboxes and removing them from the mailbox store
- Recovering deleted mailboxes
- Moving mailboxes from one store to another

Detailed procedures for working with mailbox-enabled users in Active Directory are described in Chapter 4, "Managing Recipients and Recipient Policies."

Creating a Mailbox

This section describes what happens in the mailbox store when you create a mailbox.

To create mailboxes, use Active Directory Users and Computers. You can create mailboxes in two ways:

- **Create a new user** You can create the mailbox as part of the process of creating a user.
- **Create a mailbox for an existing user** You can right-click a user, and then click Exchange Tasks to start the Exchange Task Wizard. Creating a mailbox is one of the tasks you can perform with this wizard.

The mailbox is not immediately accessible. Although Active Directory attributes for the mailbox are configured immediately, the attributes for the mailbox in the Exchange store are not configured completely until one of the following occurs:

- The user attempts to access the mailbox.
- Exchange receives a message that is addressed to the new mailbox. For this reason, you may want to automatically send new e-mail users an introductory or hello message after their accounts have been configured, especially if the users may not be using Outlook.

Either of these events will trigger Exchange to finish configuring the mailbox in the store.
Deleting a Mailbox

There are two ways to make an Exchange mailbox unusable:

- Use Exchange System Manager to delete the mailbox.
- Delete a mailbox-enabled user from Active Directory. This makes the mailbox unowned. The mailbox still exists, but no user can access it.

Deleting a Mailbox Without Deleting the User

Use the Exchange Task Wizard to delete mailboxes. This wizard is available in both Exchange System Manager (right-click the mailbox to access the wizard) and Active Directory Users and Computers (right-click the user to access the wizard).

The mailbox is not removed from the store immediately. The next time the mailbox management process runs, it marks the mailbox as deleted. The mailbox remains in the store, viewable using Exchange System Manager, for the length of time that is specified by the mailbox store settings Keep deleted mailboxes for (days) and Do not permanently delete mailboxes and items until the store has been backed up. After this time has passed (or after the store has been backed up), the mailbox will be purged automatically.

After a mailbox has been marked as deleted, you can also purge it manually. In the mailbox listing, right-click the mailbox and click Purge. For more information, see the Exchange Server 2003 Help.

Important
After a mailbox has been purged, you cannot recover it, except from a backup of the mailbox store.

Deleting a User Without Deleting Mailbox Data

If you use Active Directory Users and Computers to delete a user, the mailbox information in the mailbox store is not deleted. The next time the mailbox management process runs, it marks the mailbox as unowned. Unowned mailboxes are purged automatically according to the store's Keep deleted mailboxes and items for setting. The default value is 30 days. You can also purge the mailbox from the store manually. For more information about purging mailboxes, see the Exchange Server 2003 Help.
Recovering a Mailbox

Deleted mailboxes can be recovered only by restoring them from a backup. However, mailboxes that belong to users that were deleted from Active Directory can be recovered by associating them with existing users that do not have mailboxes. This is called reconnecting the mailbox. When you reconnect a mailbox, Exchange presents a list of users from which you can choose. Even if you have re-created the original deleted user, the re-created user object has a different security ID (SID) and will not be recognized as the original user. The selected user becomes the new owner of the mailbox.

**Note**

In specific disaster recovery circumstances, you may need to remove Exchange attributes from a user object before reconnecting the Exchange mailbox. If Exchange-related attributes are present, Exchange may assume that the user already has a mailbox, and leave the user off of the list of possible users that you can associate with the mailbox.

There are two methods for recovering mailboxes:

- Recover a single mailbox on a single mailbox store. Use the **Reconnect** command, which is available when you select the mailbox in Exchange System Manager. During the reconnect process, select the user that you want to associate with the mailbox.

- Use **Mailbox Recovery Center** to recover one or more mailboxes on one or more mailbox stores. You can export the mailbox properties to a file, and you can associate the mailboxes with users in Active Directory and reconnect the mailboxes.

**To recover one or more mailboxes on one or more mailbox stores**

1. In Exchange System Manager, expands **Tools**.

2. To choose a mailbox store to work with, right-click **Mailbox Recovery Center** and then click **Add Mailbox Store**.

3. If you want to export the mailbox properties, right-click the mailbox that you want to export, and then click **Export**.
   This is a useful way to store the mailbox properties if you do not intend to associate the mailbox with a user.
4. If you want a user to be able to access the mailbox, do the following to reconnect the mailbox:
   a. To associate a user with a mailbox, right-click the mailbox that you want to match to a user (or group), and then click **Find Match**. If a mailbox matches more than one user (or if no match exists), right-click the mailbox, and then click **Resolve Conflicts**. Follow the instructions in the Mailbox Conflict Resolution Wizard to identify a single matching user.
   b. To reconnect the mailbox, select the mailbox, right-click the selected mailbox, and then click **Reconnect**.

5. When you have finished reconnecting mailboxes, remove the mailbox stores from the Mailbox Recovery Center.

   For more detailed information about recovering mailboxes, including how to remove the mailbox stores from the **Mailbox Recovery Center**, see the Exchange Server 2003 Help.

---

**Moving a Mailbox Within an Administrative Group**

To move a mailbox to another store within the same administrative group, use the Move Mailbox Wizard. For detailed information about using this wizard, see the book *Exchange Server 2003 Deployment Guide* ([www.microsoft.com/exchange/library](http://www.microsoft.com/exchange/library)).

---

**Managing Public Folders**

This section presents an overview of how Exchange classifies public folders and what those classifications mean when you are working with the folders. It provides detailed information about how you can configure public folders, and how you can tune public folder settings to make the best use of your system storage and performance capabilities.

---

**Understanding Types of Public Folders**

Depending on context, public folders can be referred to in different ways:

- Public folders or system folders
- Content replicas
- Mail-enabled or non-mail-enabled folders
Understanding Public Folders and System Folders

Each public folder tree contains two subtrees:

- **Public folders (also called the IPM_Subtree)** Users can access these folders directly with client applications like Outlook. In its default configuration, Exchange System Manager displays these folders when you expand a public folder tree.

- **System folders (also called the Non IPM_Subtree)** Users cannot access these folders directly. Client applications like Outlook use these folders to store information such as free and busy data, offline address lists, and organizational forms. Other system folders hold configuration information used by custom applications or by Exchange itself. The Public Folders tree contains extra system folders, such as the EFORMS REGISTRY folder, that do not exist in general-purpose public folder trees.

By default, Exchange System Manager displays public folders rather than system folders (see Figure 7.21).

![Exchange System Manager](image)

**Figure 7.21** The Folders node in Exchange System Manager
Under normal operating conditions, you will not need to interact with system folders frequently. In Exchange System Manager, you can view the system folders for a specific public folder tree by right-clicking the public folder tree node and clicking View System folders (see Figure 7.22).

Figure 7.22   Folders node in Exchange System Manager, showing the system folders

System folders include the following:

- **EFORMS REGISTRY and Events Root**   By default, one content replica of each of these folders resides in the default public folder store on the first Exchange 2003 or Exchange 2000 server that is installed in the first administrative group.

- **Site folders (OFFLINE ADDRESS BOOK and SCHEDULE+ FREE BUSY)**   In most respects, these folders function in the same manner as other public folders, with the following additions:
  
  - Site folders exist only in the Public Folders tree.
  
  - The OFFLINE ADDRESS BOOK folder and the SCHEDULE+ FREE BUSY folder automatically contain a subfolder for each administrative group (or site) in your topology. By default, a content replica of a specific administrative group folder resides on the first server that is installed in the administrative group.
  
  - Each administrative group has a Site Folder Server, identified in the administrative group's object in Active Directory. By default, the first server in the site is a Site Folder Server. This server is responsible for ensuring that site folders exist. If you need to remove the Site Folder Server from the site, first make sure that the site folders have been replicated to a new server that can take over as the Site Folder Server.
• **OWAScratchPad folders** Each public folder store has an OWAScratchPad folder, which is used to temporarily store attachments that are being accessed with Outlook Web Access. You should not modify these folders.

• **StoreEvents folders** Each public folder store has a StoreEvents folder, which holds registration information for custom store events. You should not modify these folders.

• **Other folders** To support internal store operations, a tree may contain several other system folders. Do not modify these folders.

### Understanding Content Replicas

Public folder stores replicate two types of public folder information:

• **Hierarchy** Properties of the folders and organizational information about the folders (including the tree structure). All stores that support a tree have a copy of the hierarchy information. For a specific folder, the store can use hierarchy information to identify the following:
  
  • Permissions on the folder  
  • Servers that hold content replicas of the folder  
  • The folder's position in the public folder tree (including its parent and child folders, if any)

• **Content** The messages that form the content of the folders. To replicate content, you must configure a folder to replicate its content to a specific public folder store or list of stores. Only the stores that you specify will have copies of the content. A copy of the folder that includes content is called a content replica.

When a client such as Outlook connects to a store and requests a folder (for example, when an Outlook user opens a folder):

1. The store checks that the client has the correct permissions to access the folder.
2. If the client has sufficient permissions, the store determines whether it has a content replica of the folder that it can connect the client to.
3. If the store has only the folder properties, it uses the properties to identify another public folder store that has a content replica, and then refers the client to that store.
4. The new public folder store checks that the client has correct permissions to access the folder, and then locates the content replica. Additional permissions checks occur when the client accesses individual content items.
The preceding scenario is simplified. For more information about how Exchange routes clients among the public folder stores, see "Understanding Public Folder Referrals" later in this chapter. For more information about permissions and access checks, see "Working with Permissions for Public Folders and Mailboxes" earlier in this chapter.

**Understanding Mail-Enabled Folders**

Mail-enabling a public folder provides an extra level of functionality to users. In addition to being able to post messages to the folder, users can send e-mail to, and in some cases receive e-mail from, the folder. If you are developing custom applications, you can use this feature to move messages or documents into or out of public folders.

A mail-enabled folder is a public folder that has an e-mail address. Depending on how the folder is configured, it may appear in Address Book. Each mail-enabled folder has an object in Active Directory that stores its e-mail address, Address Book name, and other mail-related attributes. For more information about configuring mail-enabled folders, see "Mail-Enabling a Public Folder" later in this chapter.

In Exchange 5.5, all public folders were mail-enabled. By default, their Exchange Directory objects were hidden and created in the Recipients container. In Exchange 2003, folders can be mail-enabled or not mail-enabled, depending on whether the Exchange organization is in mixed mode or native mode. Table 7.6 summarizes the default settings for public folders, depending on the type of configuration that you have.

### Table 7.6 Default mail-enabled settings

<table>
<thead>
<tr>
<th>Tree</th>
<th>Defaults in mixed mode</th>
<th>Defaults in native mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public Folders</strong></td>
<td>Mail-enabled.</td>
<td>Not mail-enabled.</td>
</tr>
<tr>
<td>tree</td>
<td>Hidden from Address Book.</td>
<td>Can be mail-enabled, and is visible to Address Book by default.</td>
</tr>
<tr>
<td><strong>General-purpose trees</strong></td>
<td>Not mail-enabled.</td>
<td>Not mail-enabled.</td>
</tr>
<tr>
<td></td>
<td>Can be mail-enabled, and is visible to Address Book by default.</td>
<td>Can be mail-enabled, and is visible to Address Book by default.</td>
</tr>
</tbody>
</table>

**Note**
The mixed-mode defaults for the **Public Folders** tree support backward compatibility with Exchange 5.5. The Exchange 5.5 Administrator program requires a directory object for each public folder, and without one you cannot administer the folder from Exchange 5.5. If you mail-disable a folder in this tree, or if the Active Directory object is accidentally deleted or damaged, you will not be able to view the folder with Exchange 5.5 Administrator. You can mail-enable the folder again.
Because mail goes directly to the public folder store rather than to a mailbox in the mailbox store, Exchange routes e-mail messages using a method that is slightly different from the method that it uses for e-mail messages that go to a regular mailbox.

When it is choosing an initial public folder store, Exchange attempts to determine which public folder store is "closest" to the server that has the incoming message. Exchange determines which public folder store is the "closest," based on the following order of preference:

1. The store on the local server.
3. A store on an Exchange 2003 or Exchange 2000 server in the local administrative group.
4. If the folder is in the Public Folders tree, a store on an Exchange 5.5 server in the local administrative group or site.
5. The store on the Exchange 2003 or Exchange 2000 server that appears first in the tree's list of servers. This will probably be the server that was added most recently.
6. If the folder is in the Public Folders tree, the store on the Exchange 5.5 server that appears first in the tree's list of servers. This situation is rare, and would only occur in a newly configured mixed-mode topology where configuration information may not have replicated completely.

**Note**

When it is selecting a public folder store, Exchange avoids selecting a public folder store that is less than two days old unless no other public folder store is available. In this way, Exchange avoids using a store to which all of the hierarchy or content information has not yet replicated. This feature is new in Exchange 2003.

If Exchange cannot locate an appropriate public folder store, it sends a non-delivery report (NDR) to the sender of the message.

After the e-mail message has been delivered to a public folder store and the public folder store has retrieved the hierarchy information for the folder, Exchange determines the closest content replica using the following order of preference:

1. The content replica in the local public folder store.
2. A content replica in a store in the same routing group.
3. A content replica in a store with the lowest routing cost (as determined by the routing engine). If Exchange must use a store outside of the local routing group, it also takes into account other routing properties, such as link state information. This feature is new in Exchange 2003.

The closest content replica is the final destination of the message. If Exchange cannot locate a content replica of the folder, it sends an NDR to the sender of the message.
Figure 7.23 provides an overview of how Exchange delivers e-mail messages to public folders.

The following process occurs:

1. A message addressed to a public folder is submitted to Exchange. The message arrives first at ExFront01.
2. ExFront01 looks up recipients in Active Directory and finds the mail-enabled folder object for the public folder.
3. From the mail-enabled folder object's attributes, ExFront01 identifies the public folder tree to which the folder belongs.
4. ExFront01 looks up the public folder tree object in Active Directory, and identifies the public folder stores that support the tree.

5. ExFront01 selects a public folder store from the list, and sends the message to that store.

6. ExPF01 looks up the hierarchy information for the requested folder in its local public folder store.

7. Using the hierarchy information, ExPF01 determines that its public folder store does not contain a content replica of the requested folder, but that the public folder store on ExPF02 does.

8. ExPF01 sends the message to ExPF02.

9. ExPF02 looks up the hierarchy information for the requested folder in its local public folder store.

10. ExPF02 identifies the content replica of the requested folder and delivers the message to it.

**Understanding Public Folder Referrals**

When a user connects to a public folder store that does not contain a copy of the content that the user is looking for, the user is redirected to another store that has a copy of the content. You can use public folder referrals to control this redirect traffic. Referrals perform the function that public folder affinities performed in Exchange 5.5, although in a slightly different manner. (If you need information about Exchange 5.5 affinities, see the Exchange 5.5 documentation.)

**Note**

When you work with public folder referrals, you need to understand your organization's routing structure. For more information about routing, routing groups, routing costs, and routing group connectors, see Chapter 5, "Understanding and Configuring Message Routing and Transport."

Using the default referral configuration, Exchange follows the organization's routing group structure to find an appropriate server. However, to modify the flow of user traffic, you can override this configuration by specifying whether to allow referrals over certain connectors. For Exchange 2003 servers, you can also specify a list of referral servers and assign routing costs to each server. For example, you can limit referrals to a single routing group, or only allow referrals between certain servers in each routing group. Use the following methods to configure referrals.
To configure a connector to allow or block referrals from one routing group to another

1. In Exchange System Manager, in the Connectors container, right-click the connector that you want to configure and click Properties.

2. In Routing Group Connector Properties, select or clear the Do not allow public folder referrals option (see Figure 7.24) according to the following criteria:
   - For a connector between Exchange 2003 or Exchange 2000 routing groups, the Do not allow public folder referrals option is selected by default. You may want to clear this option if the connector uses a slow network connection, or if one of the connected routing groups does not have public folder information.
   - For a connector between an Exchange 2003 or Exchange 2000 routing group, and a routing group that contains Exchange 5.5 servers, the Do not allow public folder referrals option is not selected by default. The default setting is appropriate for such a connector if your users access public folders primarily with Outlook Web Access. Outlook Web Access users cannot view public folder content that resides on Exchange 5.5 servers, so allowing referrals serves little purpose. However, if your users access public folders primarily with Outlook, you can allow referrals to distribute user traffic to the Exchange 5.5 servers.

![Figure 7.24 The General properties tab for a routing group connector](image)
To configure an Exchange 2003 server to use a specific list of servers and costs for referrals

1. In Exchange System Manager, right-click the server and click Properties.
2. Use the Public Folder Referrals tab to set up your referral list (see Figure 7.25).

![Image of the Public Folder Referrals properties tab](image)

Figure 7.25  The Public Folder Referrals properties tab for a server (Exchange 2003 only)

For detailed instructions about how to use the Public Folder Referrals tab, see the Exchange Server 2003 Help.
Understanding the Basic Process for Referring Clients

When a user connects to Exchange and requests access to a public folder with Outlook (or another MAPI-based client), Exchange locates a content replica of the public folder using information supplied by the public folder store that is associated with the user's mailbox store. The public folder store retrieves the replica list of the requested folder, and if needed, retrieves routing and cost information from the routing engine. Exchange uses the following process to locate a content replica:

1. Determine whether a content replica exists in this public folder store. If so, connect the user to the local replica.
2. Determine whether a content replica exists on another public folder store on a server in the local routing group. If so, refer the user to the appropriate server.
3. If the user must be referred to another routing group, use the routing engine to determine how to connect the user to the store on the server with the lowest routing cost.

If you have created a custom list of referral servers and costs, Exchange uses this information instead of the server and cost information that the routing engine provides. To reduce calls to the routing engine, Exchange caches the cost information that the routing engine returns for one hour.

**Note**

If multiple servers meet the criteria for a referral, Exchange uses a hashing algorithm to select one preferred server for the user. Using this algorithm, Exchange can load balance users among the public folder stores while consistently sending a specific user to a specified store.

If at any point in this process the selected server is down or unreachable, Outlook tries to reach the next most appropriate server.

Understanding Referrals in Mixed-Mode Topologies

If the user's mailbox resides on an Exchange 2003 or Exchange 2000 server, the user will be routed according to the Exchange 2003 or Exchange 2000 public folder referral configuration (as set for that server and routing group). In addition, Exchange 2003 or Exchange 2000 routing group connectors will only refer users to routing groups that contain Exchange 5.5 servers if you explicitly configure them to do so. If the user's mailbox resides on an Exchange 5.5 server, the user will be routed according to the Exchange 5.5 public folder affinity configuration.

**Important**

Outlook Web Access cannot view public folder content replicas that reside on Exchange 5.5 servers.
Referring Outlook Web Access in a Front-end/Back-end Topology

Using a front-end Exchange server to proxy incoming client requests increases the fault tolerance and load balancing capability of your topology, as compared with allowing clients to access the back-end servers directly. For detailed information about deploying a front-end/back-end topology, see the books *Planning an Exchange Server 2003 Messaging System* and *Exchange Server 2003 Deployment Guide* (www.microsoft.com/exchange/library).

Figure 7.26 shows how a front-end server (ExFront01) handles an incoming request for a folder in the Public Folders tree. The front-end server queries Active Directory for information about the user, queries the user's public folder store for the location of the content replica, and queries another public folder store for the replica itself.

![Diagram of Exchange routes an Outlook Web Access user to a public folder](image)

Figure 7.26   An example of how Exchange routes an Outlook Web Access user to a public folder in the Public Folders tree
The details of this process are as follows:

1. An authenticated user who has a mailbox in this Exchange organization tries to view the contents of a public folder in the Public Folders tree. Outlook Web Access sends the following request:

   HTTP GET "http://<virtdir_front>/public/<folder>"

2. The front-end server ExFront01 receives the GET request, and contacts the global catalog server. ExFront01 looks up the user in Active Directory and retrieves the value of the user's msExchHomePublicMDB attribute. This value identifies the default public folder store that is associated with the user's mailbox store. In the example shown in Figure 7.26, this store is on the server ExBack01.

   This example depicts a specific case. Under other circumstances (for instance a server is down, the user is anonymous, or the requested folder is not in the Public Folders tree), ExFront01 would perform one of the following actions in Step 2 instead of the action described:

   - If the server with the user's associated public folder store is not available or is an Exchange 5.5 server, the front-end server sends a GET request to another server in the local routing group. The store on that server follows the basic referral process, outlined earlier in this section, to locate a content replica.

   - If the user is anonymous (using the IIS Anonymous account), the front-end server uses a hashing algorithm to select a server in the local routing group, and sends a GET request to that server. Because anonymous users have a single account, in this step they will always be sent to the same server.

   - If the public folder is in a general-purpose public folder tree, the front-end server uses a hashing algorithm to select a server in the local routing group, and sends a GET request to that server. The store on that server follows the basic referral process, outlined earlier in this section.

3. ExFront01 sends the request HTTP GET "HTTP://ExBack01/public/<folder>" to ExBack01.

4. ExBack01 accesses its hierarchy information for the Public Folders tree, and finds that the closest available content replica is on the server ExBack02. ExBack01 sends the location of the content replica to ExFront01 in the form of the message:

   HTTP 305 "HTTP://ExBack02/public/<folder>".

5. ExFront01 sends the request HTTP GET "HTTP://ExBack02/public/<folder>" to ExBack02.

6. ExBack02 returns the requested content and an HTTP 200 OK message to ExFront01.

7. ExFront01 forwards the content and an HTTP 200 OK message to Outlook Web Access.
Using this process, the Outlook Web Access user remains unaware of the topology behind the front-end server. If you do not use a front-end server, users would need to know the name of at least one of your public folder servers to use Outlook Web Access with public folders.

To expedite repeated client access to folders while minimizing network traffic, Exchange caches much of the information that it needs during the process that is shown in Figure 7.26. This information, including routing costs, replica locations, and server-down status, is cached for 10 minutes.

### Configuring Public Folders

In Exchange System Manager, public folder trees that are native to a specific administrative group are listed under the **Folders** node for that administrative group (see Figure 7.27). From this location, you can work with the properties of the public folder tree or with the individual folders, regardless of which stores hold replicas of the folders.

![Exchange System Manager](image)

**Figure 7.27** The Details tab for a public folder
Important
Because Exchange regards public folder administration and public folder store administration as separate tasks, it is possible to configure your administrative group topology so that some Exchange administrators have access to the public folder stores, but not to the public folders.

For example, consider a topology with public folder servers grouped into two administrative groups, each of which has its own Exchange Administrator. Martin is the Exchange Administrator for AG1, and Sam is the Exchange Administrator for AG2. Each of the public folder servers has a default public folder store, which supports the Public Folders tree. As you might expect, Martin can administer the default public folder stores on the servers in AG1, and Sam can administer the default public folder stores on the servers in AG2. However, note that the Public Folders tree was created in AG1, which was the first administrative group in the topology. As a result, only Martin can administer folders in the Public Folders tree. As the AG2 administrator, Sam can administer only public folder trees created in AG2.

For more information about this and other permissions issues, see "Using Exchange Administrative Roles with Exchange Store Components" earlier in this chapter.

Connecting to a Public Folder Store
Because public folder trees are not limited to single servers, you can view the properties of the tree or its folders by connecting to any of the servers that support the tree.

By default, the information in the Folders node of Exchange System Manager comes from the public folder store on the server that is running Exchange System Manager, or from a store that is hosting the public folder tree that you used most recently.

If you have a mailbox, Exchange System Manager connects to the server that runs the default public store that is associated with your mailbox. If the Exchange System Manager server does not have a public folder store for the public folder tree that you want to connect to, use the Connect to command to connect Exchange System Manager to a public folder store on another server. The Connect to commands are available on the Action menu for each public folder tree that appears in Exchange System Manager. Exchange View Only Administrators can use the Connect to command.

Tip
After creating a public folder store, you may need to refresh the information in Exchange System Manager to enable the Connect to command.
Creating a New Public Folder

After you create a public folder hierarchy, you can create the folders and subfolders to hold content.

You can create public folders using either Exchange System Manager or a client, such as Outlook or Outlook Web Access. In Exchange System Manager, the **New Public Folder** command is available on the *Action* menu for public folders and public folder trees. In Outlook and Outlook Web Access, the **New Folder** command is available on the context menu for the **Public Folder** node (in Outlook, the node is called *All Public Folders*) and all folders below that node. When you create a new folder, the only attribute that you need to supply is the folder name. After the folder has been created, you can mail-enable it and configure other folder properties.

Propagating Folder Settings

The **Propagate settings** command is available only for folders that have subfolders. Use this command to apply the options that you set for a parent folder to all of its subfolders. In this way, you can ensure that all of the subfolders have the same settings as their parent folder, without configuring each folder individually. After the parent's settings are applied, you can still change the subfolder's settings. Changing the settings on the subfolders does not affect the settings on the parent or other subfolders.

Use the **Propagate settings** command in Exchange System Manager by right-clicking the parent folder and clicking **Propagate settings**. You can then specify which settings to apply.

Configuring Individual Public Folder Limits

Size and age limits help you to control the size of your public folder stores by limiting the amount of content and by removing old content. As discussed previously in this chapter, you can set size and age limits on public folders three different ways. For information about configuring limits on a specific public folder store or a specific replica on a store, see "Configuring Public Folder Stores" earlier in this chapter. This section discusses folder-level limits settings.
Figure 7.28 shows the **Limits** tab for a public folder.

![The Limits tab for a public folder](image)

**Figure 7.28  The Limits tab for a public folder**

You can use the **Limits** tab of the public folder **Properties** dialog box to control the maximum size of folders, set the length of time that deleted messages will be retained, and set message age limits. Setting age limits on message storage can help you conserve disk space.

Unless you set limits at the folder level, all settings use the limits that are set on the public folder store. Clear the **Use public store defaults** check box to set folder-level limits.

Table 7.7 describes the possible limits that can be set for a public folder. By default, if no limits are set on the folder, any limits that have been set on the public folder store will be used.
### Table 7.7 Options available on the Limits tab for a public folder

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use public store defaults</td>
<td>When this option is selected, the options in the respective group (Storage limits, Deletion settings, and Age limits) use the values that are set in the public folder store, and cannot be configured for individual folders. You can set this option separately for each option group.</td>
</tr>
<tr>
<td>Issue warning at (KB)</td>
<td>The first size limit on a public folder. When the public folder reaches this size, a warning is sent to the administrator automatically. You can type a number from 0 to 2097151.</td>
</tr>
<tr>
<td>Prohibit post at (KB)</td>
<td>The second size limit on a public folder. When the public folder reaches this size, users can no longer post items to the public folder. You can type a number from 0 to 2097151.</td>
</tr>
<tr>
<td>Maximum item size (KB)</td>
<td>The maximum size of any individual item that is posted to a public folder. You can type a number from 0 to 2097151.</td>
</tr>
<tr>
<td>Keep deleted items for (days)</td>
<td>The number of days before deleted items are removed from the public folder permanently. The value can range from 1 to 24855.</td>
</tr>
<tr>
<td>Age limit for replicas (days)</td>
<td>The number of days that replicated items can remain on the server. The value can range from 1 to 24855. Replicated items are tracked separately from items that are posted to this public folder. When an item is posted to this public folder, the age limit does not apply until the item has been replicated.</td>
</tr>
</tbody>
</table>
Age Limit Settings and System Folders

Age limit settings affect some system folders, as well as regular public folders. Age limit settings can have the following effects:

- **Free/Busy folder**  Outlook typically publishes three months of a user's free/busy data at a time, and updates this information each time the user modifies his or her calendar. As long as the age limit is large enough (for example, 90 days), and the user modifies his or her calendar regularly, the age limit removes only information that is out-of-date.

- **Offline Address List folder**  Exchange rebuilds this folder regularly, based on a schedule that is set in Exchange System Manager. Make sure that the update interval is shorter than the age limit.

- **System Configuration folder**  This folder is not affected by the public folder store's age limit settings. Do not set age limits on the System Configuration folder.

- **Application Configuration folder**  This folder is not affected by the public folder store's age limit settings. Do not set age limits on the Application Configuration folder.

Mail-Enabling a Public Folder

You can allow users to send mail to a public folder by mail-enabling the folder and displaying the name of the folder in Address Book.

**Note**
Folders created in native-mode Exchange Server 2003 must be mail-enabled manually. To mail-enable a folder manually, right-click the folder, point to All Tasks, and then click Mail Enable. Folders that you migrate from Exchange 5.5 are mail-enabled by default.

Exchange creates an Address Book entry for each mail-enabled public folder. However, by default, the folder is hidden from users until you make the entry visible and specify a display name. For more information about configuring specific settings for mail-enabled public folders, see the sections that follow.

For information about configuring permissions for a mail-enabled public folder, including how to specify a user that can send mail on behalf of a public folder, see "Using Public Folder Permissions" in the section "Working with Permissions for Public Folders and Mailboxes" earlier in this chapter.
Configuring the Address Book Listing and E-Mail Alias

Users can address mail to a public folder by using the folder's full name from Address Book (also called the address list name) or by using an alias (usually an abbreviation of the folder's full name). By default, both the address list name and the alias are the same as the public folder name.

You can also configure an American National Standards Institute (ANSI)-only form of the public folder name for Address Book to use, which may be required by older e-mail client software. You can define custom attributes for the public folder, and if you do not want the public folder to be listed in Address Book, you can hide it. These options may be useful if you are developing custom applications to work with your public folders. If you are working with a folder in the Public Folders tree and Exchange is in mixed mode, you must clear the hidden attribute of the folder before it will be visible in Address Book.

You can configure the address list name on the General tab of the public folder's Properties dialog box, shown in Figure 7.29.

![Figure 7.29 The General tab for a mail-enabled public folder](image-url)
Select one of the following options for **Address list name**:

- **Same as folder name**: Displays the folder in Address Book as it is displayed in Exchange System Manager.
- **Use this name**: Displays the folder in Address Book using the name that you enter.

You can configure the alias using the **Exchange General** tab of the public folder's **Properties** dialog box, shown in Figure 7.30.

![Figure 7.30 The Exchange General tab for a mail-enabled public folder](image-url)
If the public folder name contains non-ANSI characters, you can also provide a simple display name for Address Book to use. This name can only include ANSI characters, which can be read by any computer. You can configure the simple display name using the **Exchange Advanced** tab of the public folder's **Properties** dialog box, shown in Figure 7.31.

![Figure 7.31 The Exchange Advanced tab for a mail-enabled public folder](image)

When the **Hide from Exchange address lists** check box is selected, the public folder is not visible in Address Book. In mixed mode, this check box is selected by default for folders in the **Public Folders** tree.

To create custom attributes for the public folder, click **Custom Attributes**. A standard dialog box for creating attributes in Active Directory will appear. You can define up to 15 custom attributes.

**Note**
If a particular folder in Address Book is hidden, users can still post messages to the folder if they know its address and type it in the **To** box of a message. However, if you designate a delegate for the public folder who can send mail on the folder's behalf, the folder must not be hidden. If the folder is hidden, the delegate will not be able to send mail on the folder's behalf.

For more information about sending mail on behalf of a public folder, see "Designating a User as a Public Folder Delegate" earlier in this chapter.
Configuring E-Mail Addresses

By default, Exchange uses the Recipient Update Service to use recipient policies to configure e-mail addresses for mail-enabled public folders automatically. The necessary recipient policies are created automatically when you mail-enable the folder. For more information about how recipient policies work, see Chapter 4, "Managing Recipients and Recipient Policies."

Most of the time, recipient policies provide an efficient and consistent mechanism for configuring e-mail addresses. If you want to configure more than one address for mail-enabled public folders, you can do so by using recipient policies rather than by configuring a new address for each folder. If you want to modify e-mail addresses on a small number of folders, you can do so by using the E-mail Addresses tab of each folder's Properties dialog box (see Figure 7.32). This feature may be useful if you are designing custom applications to work with your public folders.

![Figure 7.32 The E-mail Addresses tab for a mail-enabled public folder](image)

By default, the Automatically update e-mail addresses based on recipient policy check box is selected. This allows recipient policies to override explicitly configured addresses that are set on individual folders.
If you do need to modify the list of e-mail addresses for a folder, for detailed instructions, see the Exchange Server 2003 Help.

**Note**
The folder's primary e-mail address is the address to which replies will be sent when an e-mail message is sent on behalf of the public folder.

### Setting Delivery Restrictions

Because e-mail messages sent to or from a public folder are routed as e-mail and not as messages posted directly to the folder, Exchange provides an additional set of size and access restrictions for mail-enabled public folders. These options help you regulate e-mail traffic to and from the public folders.

To limit the size of both incoming and outgoing messages for a public folder, or to choose to accept or reject messages from specific users for the public folder, click **Delivery Restrictions** on the **Exchange General** tab of the public folder's **Properties** dialog box. You can then set message limits in the **Delivery Restrictions** dialog box (see Figure 7.33).

**Note**
You can set delivery restrictions only if Exchange is in native mode.

![Figure 7.33 The Delivery Restrictions dialog box for a mail-enabled public folder](image-url)
In the **Delivery Restrictions** dialog box, you can set the following options:

- **Sending message size**  Limits the size of messages that are sent using the e-mail alias of the public folder. You can use the default size limit, or you can type a maximum message size in the **Maximum KB** box. The maximum message size for outgoing messages can be a value from 1 to 2097151.
  
  **Note**
  Specifying too large a value for **Sending message size** can increase traffic on your network. Additionally, large messages can take a long time to download over slower network connections. Use a value that is appropriate for your network's usage pattern.

- **Receiving message size**  Limits the size of messages that are sent to the public folder. You can use the default size limit, or you can type a maximum message size in the **Maximum KB** box. The maximum message size for incoming messages can be a value from 1 to 2097151.
  
  **Note**
  Specifying too large a value for **Receiving message size** can increase traffic on your network. Additionally, large messages can take a long time to download over slower network connections. Use a value that is appropriate for your network's usage pattern.

- **Message restrictions**  Specifies who can and cannot send e-mail to the folder. Choose from the following options:
  
  - **From authenticated users only**  Regardless of the type of restriction that you apply (**From everyone**, **Only from**, or **From everyone except**), the public folder will only accept e-mail messages from authenticated users.
  
  - **From everyone**  The public folder will accept all incoming e-mail messages.
    
    **Important**
    If you select the **From everyone** message restriction, any user will be able to send e-mail messages to the public folder. Use this option only when no security restrictions are required.
  
  - **Only from**  The public folder will only accept e-mail messages from the specified users. Click **Add** to specify a list of users.
  
  - **From everyone except**  The public folder will refuse to accept e-mail messages from the specified users. Click **Add** to specify a list of users.
Configuring a Forwarding Address

You can configure a public folder to send a copy of incoming mail to a user's mailbox or to another public folder (or to multiple destinations) using the Exchange General tab (see Figure 7.34).

Figure 7.34  The Exchange General tab for a mail-enabled public folder
To configure a forwarding address for a public folder, click **Delivery Options** on the **Exchange General** tab of the public folder's **Properties** dialog box. The **Delivery Options** dialog box appears (see Figure 7.35).

![Delivery Options dialog box for a mail-enabled public folder](image)

**Figure 7.35** The Delivery Options dialog box for a mail-enabled public folder
In the **Delivery Options** dialog box, you can set up a forwarding address by configuring the following options:

- **Forwarding address**  Specifies an e-mail address (other than that of the public folder) where messages that are addressed to the public folder will be delivered. Specify one of the following:
  - **None**  Messages will only be delivered to the public folder. This is the default setting.
  - **Forward to**  Forwards all e-mail messages that are addressed to the public folder to a designated user. To create a list of users, click **Modify**.

- **Deliver messages to both forwarding address and folder**  When this check box is selected, all e-mail messages that are addressed to this public folder are delivered to both the public folder and a user that you specify. If this check box is not selected, only the user will receive the e-mail messages.

---

**Maintaining Public Folders**

Much of the actual maintenance work on public folders (such as removing expired or deleted messages, or notifying you if the public folders become too large) happens automatically when Exchange runs its public folder maintenance process. This process runs on a regular schedule, usually during off-peak hours. (For more information about the Exchange automated folder maintenance process, see "Configuring Store Maintenance and Backup Options" earlier in this chapter). You can fine-tune this process by setting size limits and age limits on the public folder stores or on individual public folders, as described in "Configuring the Default Public Folder Limits," and "Configuring Limits on a Specific Public Folder Replica" in the section "Configuring Public Folder Stores," or in "Configuring Individual Public Folder Limits" in the section "Configuring Public Folders" earlier in this chapter.

Exchange also provides several ways to view status information on public folders that may be helpful in troubleshooting public folder issues. For information about viewing the status of folders in a specific public folder store, see "Configuring Public Folder Stores" earlier in this chapter. For information about viewing the replication status of public folders, see "Configuring Replicas" in Appendix E, "Controlling Public Folder Replication." The rest of this section describes the other status views of public folders that are available.
Viewing Public Folder Status

Exchange System Manager provides multiple tabs for viewing public folder information. The Details tab displays basic information about the selected folder. Exchange View Only Administrators can access information in the Details tab (see Figure 7.36) and the Status tab (see Figure 7.37).

Figure 7.36   The Details tab for a public folder
For actively updated information about public folders, use the **Status** tab (see Figure 7.37). The **Status** tab lists all of the content replicas of the folder, the servers and where they reside, and statistics about the folder content.
Viewing Public Folder Content Using Exchange System Manager

When you troubleshoot public folder issues, you may need to check that messages have been added to or deleted from a public folder as expected. You can use the Content tab to view what a user who is connecting to the folder using Outlook Web Access would see (see Figure 7.38).

Important
To display the Content tab, Exchange System Manager must be able to log on to an IIS virtual directory for the public folder in question, the same way Outlook Web Access would. The virtual directories must be configured on the server running Exchange System Manager, and the World Wide Web Service must be running. To view the contents of a general-purpose public folder tree, make sure that you have created a virtual directory for that tree. For more information about IIS and the World Wide Web Service, see the Windows Help.

Note
Depending on your security settings, you may need to provide credentials to view the content of the folder.

Exchange View Only Administrators can access this information.

Figure 7.38   Content tab of a public folder
Searching for Public Folders Using Exchange System Manager

Use the Find tab to search for public folders within the selected public folder or public folder hierarchy. The Find tab is available at the top of the public folder tree, as well as at the folder level (see Figure 7.39). Exchange View Only Administrators can use the Find tab.

![Figure 7.39  Find tab of a public folder](image)

You can specify a variety of search criteria, such as the folder name or age. Table 7.8 lists the different options and criteria that you can use when searching.
Table 7.8 Options you can use when searching for a public folder

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name contains</td>
<td>All or part of the folder name.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Permissions for a specific user or group.</td>
</tr>
<tr>
<td>Replicated to</td>
<td>The name of the server that holds a replica of the folder.</td>
</tr>
<tr>
<td>Specify folder</td>
<td>The folder was created or modified within a certain date range. Select either Modified or Created, and then use the Begin date and End date lists to specify the date range.</td>
</tr>
<tr>
<td>Folder age</td>
<td>The age of the folder, within a certain range. Click days or older, days or newer, or days, and then specify the age in days.</td>
</tr>
</tbody>
</table>

Moving Public Folders Within a Public Folder Tree

You can move a public folder to a new location within the same public folder tree by cutting and pasting the folder in the left pane of Exchange System Manager. You can also copy the folder or move a group of folders within a folder tree.

**Important**

You cannot move, copy, or paste a folder from one public folder tree to another.

Moving a public folder within a tree is considered a change to the hierarchy of the tree, and is not the same as placing content replicas of folders on new public folder stores. For more information about configuring content replicas, see "Configuring Replicas" in Appendix E, "Controlling Public Folder Replication."
Maintaining the Organizational Forms Library

An organization's forms library is a repository for forms that are commonly accessed by all users in a company. Forms are templates that help users to enter and view information. For example, a standard supply request form can be stored in an organizational forms library.

You can create new forms libraries using Exchange System Manager, and you can create new forms using Outlook. After a form is created, it is saved in the organizational forms library. You can use the system folders to create libraries for other languages, set permissions for libraries, and replicate libraries.

Tip
For more information about creating a form, see the documentation that comes with Microsoft Outlook.

An organizational forms library is a special type of public folder that is listed only with system folders. When you create an organizational forms library, you assign a language to it. By default, clients logged on to Exchange search for forms in the library that matches their language. For this reason, you should create individual libraries to hold forms that you want to be available to non-English language clients. If there is no language-specific organizational forms library, the client defaults to the library on the server. You can have only one organizational forms library for each language. Exchange stores these libraries in the EFORMS REGISTRY system folder.

Note
You can only create organizational forms libraries in the system folders subtree of the Public Folders tree. Even if you have created new public folder hierarchies to work with the organizational forms libraries, only the Public Folders tree supports the EFORMS REGISTRY system folder.

For instructions about how to create and modify organizational forms libraries, see "Maintain the Organizational Forms Library" in the Exchange Server 2003 Help.
CHAPTER 8
Managing Exchange Clusters

After deploying Microsoft® Exchange Server 2003 in a cluster, proper management of that cluster ensures high availability of your servers that are running Exchange. One important part of managing your Exchange Server clusters is the customization of your cluster configuration, including management of your Exchange Virtual Servers and cluster nodes. For example, you may want to add functionality to the default cluster configuration, such as enabling Internet Message Access Protocol version 4 (IMAP4) or Post Office Protocol version 3 (POP3) access for your users. Other important management tasks include monitoring the performance of Exchange 2003 clusters, troubleshooting problems when they occur, and perhaps rebuilding a server or restoring your databases from backup.

Before you start managing your Exchange cluster, you may want to review what constitutes an Exchange Virtual Server and its associated Exchange resources. You may also want to become more familiar with Cluster Administrator—the primary tool used to configure and manage clusters.

**Note**

Reviewing Exchange Clusters

Exchange clusters consist of physical computers (nodes) and logical Exchange Virtual Servers (see Figure 8.1). Exchange Virtual Servers are Microsoft Windows® cluster groups with Exchange resources (instances of Exchange services). Exchange Virtual Servers are the basic units of failover for your cluster.

Figure 8.1   Sample Exchange 2003 cluster with four physical nodes and three logical Exchange Virtual Servers

Note

Reviewing the Exchange Resources Associated with Exchange Clusters

For each Exchange Virtual Server in your cluster, there are associated Exchange resources. Table 8.1 describes each of these cluster resources, including information about when and how each resource is created.
### Table 8.1 Cluster resource descriptions

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
<th>When created</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Manages the Internet Protocol (IP) address resources in a cluster.</td>
<td>Created manually during initial cluster deployment.</td>
</tr>
<tr>
<td>Network name</td>
<td>Provides an alternate computer name to identify your Exchange cluster.</td>
<td>Created manually during initial cluster deployment.</td>
</tr>
<tr>
<td>Physical disk</td>
<td>Manages a disk that is on a cluster storage device.</td>
<td>Created manually during initial cluster deployment.</td>
</tr>
<tr>
<td>Exchange System Attendant</td>
<td>Controls the creation and deletion of all resources in the Exchange Virtual Server.</td>
<td>Created automatically during initial cluster deployment.</td>
</tr>
<tr>
<td>SMTP</td>
<td>Handles the relay and delivery of e-mail.</td>
<td>Created automatically after the creation of the Exchange System Attendant resource.</td>
</tr>
<tr>
<td>IMAP4</td>
<td>Optional component that provides access to e-mail for IMAP4 clients.</td>
<td>Added manually after initial cluster deployment.</td>
</tr>
<tr>
<td>POP3</td>
<td>Optional component that provides access to e-mail for POP3 clients.</td>
<td>Added manually after initial cluster deployment.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Provides access to an Exchange mailbox and public folders through HTTP (for example, using Outlook Web Access).</td>
<td>Created automatically after the creation of the Exchange System Attendant resource.</td>
</tr>
<tr>
<td>Exchange Microsoft Search Instance</td>
<td>Provides content indexing for the Exchange Virtual Server.</td>
<td>Created automatically after the creation of the Exchange System Attendant resource.</td>
</tr>
<tr>
<td>Message transfer agent (MTA)</td>
<td>Handles communication with X.400 systems and interoperation with Exchange Server 5.5. There can be only one MTA per cluster. The MTA is created on the first Exchange Virtual Server. All additional Exchange Virtual Servers are dependent on this MTA.</td>
<td>Created automatically after the creation of the Exchange System Attendant resource.</td>
</tr>
<tr>
<td>Routing service</td>
<td>Builds the link state tables.</td>
<td>Created automatically after the creation of the Exchange System Attendant resource.</td>
</tr>
</tbody>
</table>
Figure 8.2 shows the dependency between Exchange 2003 resources. (A resource dependency indicates what other Exchange resources must be brought online before a specific Exchange resource can be brought online.) In the figure, the arrows point to the resource or resources on which a specific resource depends. For example, the arrow from Simple Mail Transfer Protocol (SMTP) points to Exchange System Attendant. Thus, SMTP is dependent on Exchange System Attendant. Similarly, Exchange System Attendant has one arrow that points to the network name and one that points to the physical disk. This means that Exchange System Attendant is dependent on both of these resources.

Figure 8.2 Exchange 2003 resources and dependencies

Understanding How Failover Works in an Exchange Cluster

As noted earlier, Exchange Virtual Servers are the basic units of failover for your cluster. However, failover occurs differently in active/passive clusters and active/active clusters.

In an active/passive cluster, such as the 3-active/1-passive cluster shown in Figure 8.3, there are three Exchange Virtual Servers: EVS1, EVS2, and EVS3. This configuration can handle a single node failure at a time and still maintain 100 percent availability after a failure occurs. That is, if Node 3 fails, Node 1 still owns EVS1, Node 2 still owns EVS2, and Node 4 takes ownership of EVS3 with all of the storage groups mounted after the failure. However, if a second node fails while Node 3 is still down, the Exchange Virtual Server associated with the second failed node remains in a failed state because there is no stand-by node available for failover.
Chapter 8: Managing Exchange Clusters

Figure 8.3 Effect of failures on an active/passive cluster

In an active/active cluster (as shown in Figure 8.4), there are only two Exchange Virtual Servers: EVS1 and EVS2. This configuration can handle a single node failure at a time and still maintain 100 percent availability after the failure occurs. That is, if Node 2 fails, Node 1 still owns EVS1, and Node 1 also takes ownership of EVS2 with all of the storage groups mounted after the failover. However, if Node 1 fails while Node 2 is still down, the entire cluster is in a failed state, because no nodes are available for failover.

Figure 8.4 Effect of failures on an active/active cluster
Using Cluster Administrator to Manage Exchange Clusters

As with standard Windows clusters, you perform most of the configuration tasks, as well as the management tasks, associated with Exchange clusters using Cluster Administrator (see Figure 8.5). Cluster Administrator is installed by default on servers that have Cluster Service installed and are running one of the following operating systems: Microsoft Windows Server 2003, Microsoft Windows 2000, or Microsoft Windows NT® 4.0 Service Pack 3 (or later).

You can also use Cluster Administrator to remotely administer a server cluster. Computers that are used to administer a server cluster remotely must be secure and restricted to trusted personnel. For more information, see "Best practices for securing server clusters" (http://go.microsoft.com/fwlink/?Linkid=18173).

To open Cluster Administrator

- On a computer that is running Cluster Administrator, on the Start menu, point to Programs, point to Administrative Tools, and then click Cluster Administrator.

Note
As an alternative to Cluster Administrator, you can administer clusters from the command line. For information about using the command line to manage cluster settings, see "Managing a Server Cluster from the Command Line" in the Cluster Administrator Help.
Customizing Your Exchange Cluster Configuration

When you deploy Exchange Server 2003 in a cluster, you must accept many default settings. For instance, your Exchange cluster consists of Exchange Virtual Servers that are created using the New Group Wizard. However, this wizard does not allow you to configure all of the possible failover options for your Exchange Virtual Servers. Similarly, the New Resource Wizard, which creates an Exchange System Attendant resource for your Exchange Virtual Server, automatically creates the remaining Exchange resources, like the Exchange store and the MTA, using the default settings for each of these additional resources.

Because initial cluster deployment usually involves so many default settings, you may need to customize your cluster configuration settings. This customization is important not only to achieve your cluster objectives, but also to achieve optimal cluster performance. Improper cluster configuration is the source of many of the Exchange-related issues handled by Microsoft Product Support Services. For this reason, carefully follow the recommendations in this chapter to ensure your clusters perform optimally.

Note
If you upgraded your Exchange cluster from Exchange 2000 to Exchange 2003, you can ignore this section about customizing your cluster configuration because your configuration settings will not have changed.

There are two levels of settings that you may want to adjust in your Exchange cluster configuration:

- Settings for the Exchange Virtual Servers.
- Settings for the Exchange resources that are associated with a specific Exchange Virtual Server.

Configuring Exchange Virtual Server Settings

When you create your Exchange Virtual Servers, the default properties that are applied at that time should allow your Exchange cluster to operate adequately. However, you may want to modify these settings to customize your clusters to accommodate your specific Exchange environment.

To change the configuration settings for an Exchange Virtual Server, you use the property settings associated with that Exchange Virtual Server object. These property settings instruct Cluster Service in how to manage your Exchange Virtual Servers.
To access the properties of an Exchange Virtual Server

- In Cluster Administrator, in the console tree, right-click the Exchange Virtual Server that you want to configure, and then click **Properties**.

After you open the **Properties** dialog box for a specific Exchange Virtual Server, you can use the options on the various tabs to customize the preferred owner, failover, and failback settings.

**Specifying Preferred Owners**

During the creation of an Exchange Virtual Server, you have the option of defining a list of preferred cluster nodes or *preferred owners* for that server. Cluster Service uses this list of preferred owners when assigning the Exchange Virtual Server to a node. Cluster Service first tries to assign the Exchange Virtual Server to the first node in the list. If that node is unavailable, Cluster Service tries the next node in the list. If that node is unavailable, Cluster Service continues down the list, until it can assign the Exchange Virtual Server to a node. If Cluster Service cannot find an available node in the preferred owners list, it tries to fail over to the other available nodes in the cluster that have Exchange installed.

By default, you do not have to specify any preferred owners. If you do not specify owners, Cluster Service assigns an Exchange Virtual Server to the next available node that has Exchange installed.

However, it is recommended that you specify preferred owners if you have a cluster that hosts multiple applications. In this scenario, the first nodes in the list should be those nodes whose resources are best able to handle any existing applications on those nodes, and the Exchange Virtual Server for which Cluster Service is trying to find a node.

The preferred owners list is also important if you configure your Exchange Virtual Server to fail back automatically. With automatic failback enabled, an Exchange Virtual Server that is trying to come back online attempts to fail back to the first node in the preferred owners list. Again, this first node should be the node that is best able to accommodate the Exchange Virtual Server. If the Exchange Virtual Server is unable to fail back to any of the nodes in the list, the server will not come online, and the mailboxes on that server will not be available for your users.
When setting the preferred owners for your Exchange Virtual Servers, follow the rules outlined in Table 8.2.

**Table 8.2  Rules for setting the preferred owners for an Exchange Virtual Server**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Rule</th>
</tr>
</thead>
</table>
| Specifying a single node as the preferred owner for each Exchange Virtual Server | You should assign a different node to each server. For example, the 4-node/3 Exchange Virtual Server example, shown earlier in Figure 8.1, could have the following preferred owners:  
  - EVS1 to Node 1  
  - EVS2 to Node 2  
  - EVS3 to Node 3 |
| Specifying a list of nodes as the preferred owners for each Exchange Virtual Server | You should ensure that the first node that is listed for one Exchange Virtual Server is not listed as the first node for any other Exchange Virtual server. For example, the 4-node/3 Exchange Virtual Server example, shown earlier in Figure 8.1, could have the following preferred owner lists:  
  - EVS1 to Node 1, Node 2, and Node 3  
  - EVS2 to Node 2, Node 3, and Node 1  
  - EVS3 to Node 3, Node 1, and Node 2 |
To specify a list of preferred owners

- On the **General** tab (see Figure 8.6) in the Exchange Virtual Server's **Properties** dialog box, under **Preferred owners**, click **Modify** to specify the nodes that are to be preferred owners for this server.

![Figure 8.6 The General tab in the Properties dialog box for an Exchange Virtual Server](image)
Specifying Failover Options

When configuring how Cluster Service manages failovers, consider the Threshold and Period options on the Failover tab (see Figure 8.7). The Threshold setting determines the number of times that the Exchange Virtual Server can fail over during the failover Period. If the actual number of failovers exceeds the threshold during the failover period, the Exchange Virtual Server may be in a failed state, and Cluster Service will not bring it online. The default and recommended settings for these failover options are to have Exchange fail over 10 times in a 6-hour period.

To specify the failover options for an Exchange Virtual Server

- On the Failover tab (see Figure 8.7) in the Exchange Virtual Server's Properties dialog box, type a value for the Threshold and Period options.

Figure 8.7 Failover tab in the Properties dialog box for an Exchange Virtual Server
Considering Other Factors that Affect Failover

The failover options that you set for your Exchange Virtual Servers are only one factor that affects the speed at which an Exchange Server 2003 cluster fails over. In addition to those settings, many other factors can influence failover rates. Table 8.3 lists these additional factors. By understanding these factors, you should be able to configure your Exchange clusters for optimal failover.

**Table 8.3 Factors that affect failover performance of Exchange 2003 clusters**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State of the Exchange store</td>
<td>The state of the Exchange database and logs at the time of startup or shutdown affects failover performance. For example, if Exchange databases were shut down abruptly, there may be a large number of log files to roll through before starting the Exchange databases on the new Exchange Virtual Server.</td>
</tr>
<tr>
<td>Number of storage groups and databases on your servers</td>
<td>In general, the greater the number of Exchange databases on your Exchange Virtual Server, the longer it takes to move resources to the new Exchange Virtual Server.</td>
</tr>
<tr>
<td>Number of service connections into the Exchange store</td>
<td>The Exchange store performs cleanup routines before it releases and allows failover to occur. An unloaded server that takes 100 seconds to fail over takes 120 seconds to fail over when that server has 3,000 simultaneous Microsoft Office Outlook® Web Access or Microsoft Outlook connections.</td>
</tr>
<tr>
<td>Size of the SMTP queue</td>
<td>If the SMTP queue size is greater than 1,000 messages, the time to fail over from one cluster node to another can be significant. You can modify this setting by creating and configuring the <strong>SMTP Max Handle Threshold</strong> registry key value: <code>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SMTPSVC\Queuing\MsgHandleThreshold</code>  For more information about creating and configuring this registry key, see the procedure following this table.</td>
</tr>
</tbody>
</table>
To add the MsgHandleThreshold registry key value

1. Start Registry Editor.
2. In the console tree, navigate to the following registry key:
   
   ```
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SMTPSVC
   ```
3. In the console tree, right-click SMTPSVC, point to New, and then click Key.
4. For the key name, type Queuing.
5. Right-click Queuing, point to New, and then click DWORD Value.
6. In the details pane, type MsgHandleThreshold for the registry key value.
7. Right-click MsgHandleThreshold and click Modify.
8. Under Base, click Decimal.
9. Enter a value based on the following:
   
   - To configure your cluster for optimum failover performance, set the value to 1,000.
   - For optimum run-state performance, set the value to 10,000.

---

Setting Failback Options

Used in conjunction with the Failover tab, the Failback tab (see Figure 8.8) helps define what happens during a failover. On this tab, you have the option of preventing failback from occurring automatically (the default), or allowing failback to occur automatically.

- **Preventing Failback**  If you do not allow an Exchange Virtual Server to fail back, an administrator must intervene and manually move the server back to the original, preferred node.

   This may be your preferred setting because it allows you to control when the failback occurs. For example, you may want to select Prevent failback if you want to take time to troubleshoot or run diagnostics on the failed node before allowing the node to take ownership of the Exchange Virtual Server again.

   You can also use this setting to minimize downtime for users. For example, consider a scenario where a failover that occurs at 3:00 P.M. causes EVS1 to move from Node 1 to Node 4 (the stand-by node). By preventing failback, you can wait until the end of the work day to manually move EVS1 back to Node 1, and users do not have to experience downtime waiting for the server to come back online after the move.

- **Allowing Failback**  By allowing an Exchange Virtual Server to fail back to the preferred node automatically, you can also specify when this failback should happen: either immediately or during a specified time interval. This is the preferred setting if you want to have Cluster Service manage the cluster without any manual administrator intervention.
To specify the failback options for an Exchange Virtual Server

- On the **Failback** tab (see Figure 8.8) in the Exchange Virtual Server's **Properties** dialog box, select the failback options for the server.

![Figure 8.8 Failback tab in the Properties dialog box for an Exchange Virtual Server](image)

**Configuring Exchange Cluster Resources**

Like the configuration settings for your Exchange Virtual Servers, the default configuration settings for the Exchange resources (instances of Exchange services) that are associated with each server should allow your cluster to work adequately. However, there may be specific settings that you want to adjust, based upon your Exchange environment.
For each Exchange Virtual Server, you can see its associated Exchange resources in the details pane of Cluster Administrator (see Figure 8.9). In Figure 8.9, the CORP-MSG-01 server has all of the default Exchange resources. Because the CORP-MSG-01 server is the first Exchange Virtual Server in this cluster, this server also has an MTA resource.

![Figure 8.9](image)

**Figure 8.9 Exchange resources for the CORP-MSG-01 Exchange Virtual Server**

To change the configuration for an Exchange cluster resource, you use the property settings that are associated with the resource. These property settings instruct Cluster Service in how to manage the resource.

**To access the properties of an Exchange cluster resource**

1. In Cluster Administrator, in the console tree, click the Exchange Virtual Server that contains the resource that you want to configure.

2. In the details pane, right-click the resource that you want to configure, and then click Properties.

After you open the Properties dialog box for a specific Exchange resource, you can use the options on the various tabs to customize resource settings, including possible owners options, resource dependency options, and restart options.
Specifying Possible Owners

You can specify which nodes are capable of running an Exchange resource. In general, you should specify all nodes in the cluster as possible owners for a resource. This enables failover for that resource.

However, you can specify a single node as a possible owner. Even though having a single node as a possible owner disables failover for the specified Exchange resource, you still may want to specify a single owner if:

- The other nodes do not have the ability to handle the resource.
- Maintaining performance is more important than keeping the resource available.
- You want to control Exchange Virtual Server failover scenarios effectively.

The nodes that you list as possible owners of a resource limit where the Exchange Virtual Server can run. If all of the resources on an Exchange Virtual Server have the same possible owners, the server can run on any of the listed nodes. If one of the resources fails to list a node, the Exchange Virtual Server cannot run on that node, even if all of the remaining resources list the node as a possible owner.
To specify the possible owners for an Exchange resource

- On the **General** tab (see Figure 8.10) in the resource's **Properties** dialog box, under **Possible owners**, click **Modify**, and then specify the nodes that you want to be possible owners for this resource.

![Figure 8.10](image-url)  
*General tab in the Properties dialog box for the Exchange Information Store Instance resource*
Specifying a Separate Resource Monitor

By default, an Exchange resource runs in the same resource monitor as the other Exchange resources that are associated with an Exchange Virtual Server. Although it is not recommended, you may want to change this default setting on the General tab and run an Exchange resource in a separate resource monitor when you troubleshoot this cluster resource. For more information about the preferred ways of troubleshooting cluster resources, search for "troubleshoot cluster resources" in the Microsoft Product Support Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=18175).

To run an Exchange resource in a separate resource monitor

- On the General tab in the resource's Properties dialog box, select Run this resource in a separate Resource Monitor.

Understanding Resource Dependencies

Before an Exchange resource can be brought online, there are often other Exchange resources that must be brought online before it. This requirement is called a resource dependency.

The Resource dependencies list on a specific Exchange resource object lists the other resources that must be brought online before this resource can be brought online. Table 8.4 lists the Exchange 2003 cluster resources and their default dependencies.

> Note
> For a visual representation of these dependencies, see Figure 8.2 earlier in this chapter.

Table 8.4  Exchange 2003 default resource dependencies

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Attendant</td>
<td>Network name resource and shared disk resources</td>
</tr>
<tr>
<td>Exchange store</td>
<td>Exchange System Attendant</td>
</tr>
<tr>
<td>SMTP</td>
<td>Exchange System Attendant</td>
</tr>
<tr>
<td>IMAP4</td>
<td>Exchange System Attendant</td>
</tr>
<tr>
<td>POP3</td>
<td>Exchange System Attendant</td>
</tr>
<tr>
<td>HTTP</td>
<td>Exchange System Attendant</td>
</tr>
<tr>
<td>Exchange Microsoft Search Instance</td>
<td>Exchange System Attendant</td>
</tr>
</tbody>
</table>
### Adding Disk Resource Dependencies

If you are adding disk resources to an Exchange Virtual Server, you must ensure that the Exchange System Attendant resource is dependent on the new disk resource.

**To make the Exchange System Attendant dependent on a new disk resource**

1. On the Dependencies tab (see Figure 8.11), in the Exchange System Attendant Properties dialog box, click **Modify**.

![Figure 8.11 Dependencies tab of the Exchange System Attendant Properties dialog box](image)

#### Table

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTA</td>
<td>Exchange System Attendant</td>
</tr>
<tr>
<td>Routing service</td>
<td>Exchange System Attendant</td>
</tr>
</tbody>
</table>

**Note**

Other than to add disk resource dependencies, altering dependencies is not recommended because it can adversely affect your system.
2. In the Modify Dependencies dialog box (see Figure 8.12), in the Available resources list, double-click the disk that you want to add, and then click OK.

![Figure 8.12 Dependencies for the Exchange System Attendant](image)

**Specifying Service Restart Options**

By default, when a resource experiences a failure, Cluster Service attempts to restart the resource three times before attempting to move the Exchange Virtual Server to another node. It is strongly recommended that you keep this default option because restarting a service may correct a problem that the node is experiencing. Also, restarting a service takes much less time than moving an Exchange Virtual Server to another node.

However, there are additional restart options that you might want to adjust:

- **How many restarts are allowed before the resource fails** You can specify the number of resource failures (Threshold) that can occur in a certain length of time (Period) before the resource causes the associated Exchange Virtual Server to fail over.

- **Whether a resource failure causes a failover** You can specify whether you want a resource failure (as defined by your Threshold and Period settings) to affect the whole group and force Cluster Service to fail over the associated Exchange Virtual Server to a different node. Because it is advisable to have failover occur for all essential resources on your Exchange Virtual Server, you should select the Affect the group check box for those resources. For non-essential resources (for example, POP3) that affect only a few users, you may not want to fail over the server when that resource fails, and you would therefore clear the Affect the group check box for that resource.
To adjust the restart options for an Exchange resource

- On the **Advanced** tab (see Figure 8.13), in the resource's **Properties** dialog box, select the restart options for the server.

![Figure 8.13 Advanced tab for an instance of the Exchange store](image)

**Setting Polling Cluster Resources**

Cluster Service polls Exchange resources using a set of Exchange-specific polling intervals that do not need to be changed. Therefore, configuring the polling intervals "Looks Alive" poll interval and "Is Alive" poll interval on the **Advanced** tab in the resource **Properties** dialog box has no effect on polling intervals.
Setting Pending States

By default, Cluster Service allows a resource to be in a pending state (online pending or offline pending) for only 180 seconds (3 minutes) before Cluster Service terminates the resource, and the resource enters a failed state. An Exchange 2003 or Windows Server 2003 cluster resource must go offline and come back online during the Pending timeout period. Cluster Service makes an exception to the Pending timeout period for the Microsoft Exchange Information Store instance. Although the Exchange store instance must go offline during that period, the store does not have to come back online within the Pending timeout period. This is because the length of time that the Exchange store takes to restart depends on whether the store shut down properly. If the Exchange store did not shut down properly, the store must roll through log files upon restarting, and the number of log files to be rolled through determines the time it takes to bring the store back online.

Because of the way that the Exchange store writes log files to an Exchange database, the Exchange store for which you might want to increase the Pending timeout period. Increasing the pending time-out period allows the store more time to shut down properly.

To change the length of time that a resource remains pending before failing

- On the Advanced tab in the resource's Properties dialog box, type a value (in seconds) for Pending timeout.

Viewing the Exchange Virtual Server That Connects to a Protocol Resource

Exchange automatically selects the Exchange Virtual Server that is used to connect the protocol resource to the cluster. Exchange makes this selection based upon the information that you enter when you create the various resources:


- For an IMAP4 or POP3 virtual server instance, Exchange sets the Server Instance option to the Exchange Virtual Server name that you specified in the Group box when you created the IMAP4 or POP3 resource. For information about creating an IMAP4 or POP3 virtual server instance on a cluster, see "Adding IMAP4 and POP3 Resources" later in this chapter.
To view the Exchange Virtual Server that is used to connect the protocol resource

- On the Parameters tab (see Figure 8.14) of the resource's Properties dialog box, look at the Server Instance option.

![Figure 8.14 Parameters tab of an instance of the Exchange HTTP resource](image)

**Note**

You should not need to modify the Server Instance option.

### Taking Exchange Virtual Servers or Exchange Resources Offline

Occasionally, you need to take an Exchange Virtual Server or resource offline. For example, you might need to apply a service pack. In that case, you would bring each Exchange Virtual Server offline, and apply the service pack to the associated node.

You take Exchange Virtual Servers and Exchange resources offline the same way you do with cluster groups and Windows resources. The following procedure describes this standard process.
To take an Exchange Virtual Server or Exchange resource offline

- In Cluster Administrator, right-click the Exchange Virtual Server or Exchange resource that you want to take offline, and then click **Take Offline**.

*Important*
Taking an Exchange Virtual Server or Exchange resource offline stops client connectivity to user mailboxes.

Besides being online or offline, Exchange Virtual Servers and Exchange resources can be in other states. Table 8.5 and Table 8.6 list the various states that are possible for Exchange Virtual Servers and Exchange cluster resources, respectively.

**Table 8.5 Description of Exchange Virtual Server states**

<table>
<thead>
<tr>
<th>Group state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed</td>
<td>One or more resources in the Exchange Virtual Server cannot be brought online or offline in the allowed time.</td>
</tr>
<tr>
<td>Online</td>
<td>All resources in the Exchange Virtual Server are online.</td>
</tr>
<tr>
<td>Offline</td>
<td>All resources in the Exchange Virtual Server are offline.</td>
</tr>
<tr>
<td>Partially Online</td>
<td>One or more resources in the Exchange Virtual Server are online, and one or more are offline.</td>
</tr>
<tr>
<td>Pending</td>
<td>One or more resources in the Exchange Virtual Server are Online Pending or Offline Pending.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The state of the entire Exchange Virtual Server cannot be determined.</td>
</tr>
</tbody>
</table>

**Table 8.6 Description of Exchange cluster resource states**

<table>
<thead>
<tr>
<th>Resource state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed</td>
<td>The resource cannot be brought online or offline in the allowed time.</td>
</tr>
<tr>
<td>Online</td>
<td>The resource is online.</td>
</tr>
<tr>
<td>Offline</td>
<td>The resource is offline.</td>
</tr>
<tr>
<td>Online (Offline) Pending</td>
<td>The resource is Online Pending or Offline Pending.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The state cannot be determined.</td>
</tr>
</tbody>
</table>
Adding IMAP4 and POP3 Resources

For improved security, the Windows IMAP4 and POP3 protocol services are no longer enabled by default on servers that are running Windows Server 2003. Similarly, the IMAP4 and POP3 protocol resources are no longer created by default upon creation of an Exchange 2003 virtual server.

If you want to enable either of those protocols, you must do the following:

- Enable the Windows IMAP4 or POP3 service on those cluster nodes that will be running the Exchange Virtual Server with the IMAP4 or POP3 resource. To ensure that the service works properly with clustering, you must also configure the service to start manually.
- Manually add the respective IMAP4 or POP3 virtual server as a resource to each Exchange Virtual Server on which you want to enable the selected protocol, and then bring the resource online.

The following procedures take you through these steps. For additional information about using IMAP4 and POP3 with Exchange 2003, see Chapter 6, "Managing Client Access to Exchange."

To enable a newly created IMAP4 or POP3 resource and configure it to start manually

1. On the Start menu, point to All Programs, point to Administrative Tools, and then click Services.
2. In Services, in the console tree, click Services (Local).
3. In the details pane, right-click Microsoft Exchange IMAP4 or Microsoft Exchange POP3, and then click Properties.
4. On the General tab, under Startup type, click Manual, and then click Apply.
5. Under Service status, click Start, and then click OK.
6. Repeat this procedure on all nodes that will be running the Exchange Virtual Server with IMAP4 or POP3 resources.
To add an IMAP4 or POP3 virtual server as a resource to an Exchange Virtual Server

1. In Cluster Administrator, right-click the Exchange Virtual Server to which you want to enable IMAP4 or POP3, point to New, and then click Resource.

2. In the New Resource dialog box, do the following:
   a. In Name, type either one of the following names:
      - If you are adding the IMAP4 resource, type Exchange IMAP4 Virtual Server - (<EVSName>), where EVSName is the name of the selected Exchange Virtual Server.
      - If you are adding the POP3 resource, type Exchange POP3 Virtual Server - (<EVSName>), where EVSName is the name of the selected Exchange Virtual Server.
   b. In the Resource Type drop-down list, click one of the following options:
      - If you are adding the IMAP4 resource, click Microsoft Exchange IMAP4 Server Instance.
      - If you are adding the POP3 resource, click Microsoft Exchange POP3 Server Instance.
   c. Verify that the Group drop-down list contains the name of the selected Exchange Virtual Server, and then click Next.

3. In the Possible Owners dialog box (see Figure 8.15), verify that all nodes appear in the Possible owners list, and then click Next.

Figure 8.15   Possible Owners dialog box for an IMAP4 Virtual Server Instance
4. In the Dependencies dialog box, under Available Resources, double-click the <System Attendant Resource Name> to add the System Attendant to the Resource dependencies list, and then click Next.

5. In the Virtual Server Instance dialog box, in the Server Instance list, select the IMAP4 or POP3 virtual server for the resource, and then click Finish.

6. In Cluster Administrator, right-click the IMAP4 or POP3 resource, and then click Bring Online.

Adding a Node

There are times when you might want to add a node to an existing Exchange cluster. For example, you may decide that you want to upgrade your existing 3-node, 2-active/1-passive configuration to a 4-node, 2-active/2-passive configuration.


After installing Exchange on the new node in the cluster, consider these settings:

- Preferred ownership of your Exchange Virtual Servers  By default, the new node is not a preferred owner of any Exchange Virtual Server. Therefore, if you want the new node to be listed as a preferred owner you must change the properties on the respective Exchange Virtual Server in Cluster Administrator.

- Possible ownership of the Exchange resources in an Exchange Virtual Server  By default, the new node that you created is added as a possible owner for all of the resources for the Exchange Virtual Servers in your cluster. If you do not want the new node to be a possible owner for any of the resources in the Exchange Virtual Servers in your cluster, remove that node from the list of possible owners in Cluster Administrator.

Adding an Exchange Virtual Server

You may want to add an Exchange Virtual Server to an Exchange cluster. For example, you may decide that you want to change your 4-node, 2-active/2-passive configuration into a 4-node, 3-active/1-passive configuration. Although you will have one less node available for failover purposes, the advantage of having an additional Exchange Virtual Server is that you can have more users on your Exchange cluster.

While you are performing this procedure, you have the opportunity to configure preferred ownership for the Exchange Virtual Server, as well as possible ownership for the Exchange resources of that Exchange Virtual Server:

- **Preferred ownership of your Exchange Virtual Servers**  By default, you do not have to choose a preferred owner when you create a new Exchange Virtual Server. However, if you want to enforce a preferred order in which the Exchange Virtual Server fails over, you can do so. See "Step 3: Creating the Group to Host the Exchange Virtual Server" in the book *Exchange Server 2003 Deployment Guide* (www.microsoft.com/exchange/library).

- **Possible ownership of the Exchange resources in an Exchange Virtual Server**  When you create an Exchange Virtual Server, the default option is to list all cluster nodes that have Exchange installed as possible owners of the resources. However, you do not have to accept this default setting, and you can customize which nodes can be possible owners for the resources of your new Exchange Virtual Server.

### Removing an Exchange Virtual Server

Though it does not happen often, there are times when you may need to remove an Exchange Virtual Server from an Exchange cluster. In particular, you may need to do this if:

- You are reconfiguring the cluster from an active/active configuration to an active/passive configuration. That is, you are keeping the same number of nodes in the configuration, but you want one of those nodes to be passive instead of active.

- You are planning to remove Exchange 2003 from a cluster. For more information, see "Removing Exchange 2003 from a Cluster Node" later in this chapter.

Regardless of your reasons for removing an Exchange Virtual Server, you need to consider the requirements shown in Table 8.7 prior to removing that server.
Table 8.7  Requirements for removing an Exchange Virtual Server

<table>
<thead>
<tr>
<th>If the Exchange Virtual Server to be removed</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owns the message transfer agent (MTA)</td>
<td>You must remove all other Exchange Virtual Servers prior to removing the Exchange Virtual Server that owns the MTA resource. The first Exchange Virtual Server created in a cluster owns the MTA resource. All other Exchange Virtual Servers in the cluster depend on this resource. Thus, the Exchange Virtual Server that owns the MTA resource cannot be removed first.</td>
</tr>
<tr>
<td>Is a routing master of a routing group</td>
<td>You must make another Exchange Virtual Server the routing master of that group prior to removing the server.</td>
</tr>
<tr>
<td>Is the home for the postmaster account</td>
<td>You must move the postmaster account to another Exchange Virtual Server prior to removing the server.</td>
</tr>
<tr>
<td>Is the home for the last public store in a mixed-mode administrative group</td>
<td>You must move the contents of that public store to a public store on a different Exchange Virtual Server.</td>
</tr>
<tr>
<td>Is responsible for running the Recipient Update Service</td>
<td>You must make another Exchange Virtual Server the owner of the Recipient Update Service.</td>
</tr>
<tr>
<td>Is a target bridgehead server for any routing group</td>
<td>You must designate another server as the bridgehead server prior to removing the Exchange Virtual Server.</td>
</tr>
</tbody>
</table>

After you have performed any necessary actions listed in Table 8.7 to ensure that the Exchange Virtual Server can be removed, you can then remove that server. The process of removing a single Exchange Virtual Server from a cluster consists of the following five tasks:

1. Backing up critical data and securing resources hosted by the Exchange Virtual Server.

   **Note**
   For information about how to back up Exchange data, see the book *Disaster Recovery for Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?LinkId=18350).

2. Moving all mailboxes and public folder content to another Exchange Virtual Server (as described later in this chapter).

3. Taking the Exchange System Attendant resource offline (as described later in this chapter).
4. Removing the Exchange Virtual Server (as described later in this chapter).
5. Deleting remaining cluster resources (as described later in this chapter).

**Important**
Deleting components of an Exchange Virtual Server without removing the entire server can cause interruptions in mail flow. As a result, it is recommended that you follow all of the steps in the procedure when removing an Exchange Virtual Server from a cluster.

---

### Moving All Mailboxes and Public Folder Content

After backing up data, you must move any mailboxes residing on the Exchange Virtual Server to another server in your Exchange organization. Any mailboxes that are not moved to another server must be deleted. If mailboxes remain on an Exchange Virtual Server, you will not be able to completely delete the Exchange Virtual Server, and the server object remains in the Microsoft Active Directory® directory service, even though you succeeded in deleting the Exchange System Attendant resource.

To move mailboxes from one server (source) to another server (target), you use the Exchange Task Wizard. This wizard is available in either Active Directory Users and Computers or Exchange System Manager, as described in the following procedure.

**Note**
For more information about moving mailboxes, see Chapter 7, "Managing Mailbox Stores and Public Folder Stores." For information about moving a large number of mailboxes, see Microsoft Knowledge Base Article 297393, "HOWTO: Programmatically Move an Exchange 2000 Mailbox Using CDOEXM in Visual C++" ([http://support.microsoft.com/?kbid=297393](http://support.microsoft.com/?kbid=297393)).

**To move mailboxes from one server to another**

- In Active Directory Users and Computers, right-click the user object, click **Exchange Tasks**, and then click **Move Mailbox**.
  
  —or—

- In Exchange System Manager, right-click the mailbox object, click **Exchange Tasks**, and then click **Move Mailbox**.

In addition to moving mailboxes, you must move all public folder content from the server prior to removing the server.

**To move public folder content from one server to another**

- In your Internet browser, open the Microsoft Knowledge Base Article 288150, "XADM: How to Rehome Public Folders in Exchange 2000" ([http://support.microsoft.com/?kbid=288150](http://support.microsoft.com/?kbid=288150)), and follow the instructions.
Taking the Exchange System Attendant Resource Offline

An Exchange Virtual Server cannot be removed while any of its resources are online. Taking the Exchange System Attendant resource offline takes all of a server's dependent resources offline.

**To take the Exchange System Attendant resource offline**

1. In Cluster Administrator, select the Exchange Virtual Server that you want to remove.
2. In the details pane, right-click *System Attendant resource*, and then click *Take Offline*.

Using Cluster Administrator to Remove the Exchange Virtual Server

In Exchange 2000 Server, you removed an Exchange Virtual Server by deleting the Exchange System Attendant resource. However, this is not how you remove an Exchange Virtual Server in Exchange 2003.

To remove an Exchange Virtual Server in Exchange 2003, you must use the appropriate shortcut menu option in Cluster Administrator. Trying to remove the server by just deleting the Exchange System Attendant resource does not work. If you delete the Exchange System Attendant, you must re-create it, and then properly delete the Exchange Virtual Server, as described in the following procedure.

**To remove an Exchange Virtual Server**

1. In Cluster Administrator, in the console tree, select *Groups*.
2. In the details pane, right-click the Exchange Virtual Server that you want to remove, and then click *Remove Exchange Virtual Server*.
3. In the *Microsoft Exchange Cluster Administrator Extension* dialog box (see Figure 8.16), click *Yes* to delete the Exchange Virtual Server and all resources that are either directly or indirectly dependent on the Exchange System Attendant resource.

![Microsoft Exchange Cluster Administrator Extension](image)

Figure 8.16 Warning when removing an Exchange Virtual Server
Clicking Yes also removes the Exchange Virtual Server information from Active Directory; the physical disk, the IP Address, and Network Name resources remain.

Deleting the Remaining Cluster Resources

After you delete the Exchange resources of your Exchange Virtual Server, you must manually remove the Windows resources, including the IP Address and Network Name resources.

To delete the remaining resources after removing an Exchange Virtual Server

1. In Cluster Administrator, select the cluster group that contains the Exchange Virtual Server that you just deleted.
2. In the details pane, right-click IP Address resource, and then click Take Offline.
3. Right-click IP Address resource again, and then click Delete.
4. In the Delete Resources dialog box, click Yes.
   This deletes both the IP Address and Network Name resources.
5. Move the Physical Disk resource by dragging it to another group that is owned by this node.
6. Delete the cluster group by right-clicking the group in the console tree, and then selecting Delete.

If you have followed all of the procedures for removing an Exchange Virtual Server, you have deleted this server. After deleting this server, if you want this node to be a passive node in your Exchange cluster, ensure that the possible owner and preferred owner settings are correct.

If you want to completely remove the Exchange 2003 installation, see the next section, "Removing Exchange 2003 from a Cluster Node."

Removing Exchange 2003 from a Cluster Node

To remove Exchange 2003 from a cluster node, you must uninstall Exchange 2003 as you would from a stand-alone (non-clustered) server. However, only remove Exchange from those nodes that you no longer want Exchange to use. If you want Exchange 2003 to use the node (for example, as a passive node), do not uninstall Exchange 2003 from the node.
Before removing Exchange from a node, do the following:

- Move all Exchange Virtual Servers that the node owns to another node or perform the steps in the previous section "Removing an Exchange Virtual Server" to remove every Exchange Virtual Server that the node owns.
- Move any important cluster resources owned by the node to another node before proceeding. If you do not move these resources, Exchange Setup blocks removal of Exchange 2003 from the node.

To remove Exchange 2003 from a node

1. In Control Panel, open Add/Remove Programs.
2. In the Currently Installed Programs list, select Microsoft Exchange 2003.
3. Click Change/Remove.
4. In the Welcome dialog box, click Next.
5. In the Component Selection dialog box, ensure that the action next to Microsoft Exchange 2003 is Remove, and then click Next.
6. In the Component Summary dialog box, verify your installation selections, and then click Next.
7. In the Microsoft Exchange 2003 Installation Wizard dialog box (see Figure 8.17), click Yes if you are removing the last node in the cluster, or click No if it is not the last node.

![Microsoft Exchange 2003 Installation Wizard]

Are you removing Exchange 2003 from the last node in the cluster? Choosing YES will remove the Exchange resource types from the cluster.

[Yes] [No]

Figure 8.17 Warning when removing Exchange 2003 from a cluster

If you remove Exchange from the last node in the cluster, Exchange Setup removes Exchange cluster resource types from the cluster.

8. In the Completion dialog box, click Finish.
Migrating an Exchange Cluster Node to a Stand-Alone (Non-Clustered) Server

Migrating an Exchange 2003 cluster node (that is, an Exchange Virtual Server) to a stand-alone server is not supported. If you want to migrate a clustered server to a stand-alone server, you must create a third server, and then move mailboxes to the new server.

Similarly, you cannot migrate a stand-alone Exchange 2003 server to an Exchange cluster node.

Monitoring Performance of an Exchange Cluster

Monitoring your Exchange clusters is as important as managing them. By actively monitoring your clusters, you help ensure that your Exchange 2003 clusters perform well. To monitor the performance of the Exchange Virtual Servers in your cluster, use System Monitor. To monitor your Exchange Virtual Servers for errors that may be occurring, use Event Viewer.

Note
For more information about System Monitor and Event Viewer, see the Windows Server 2003 or Windows 2000 online documentation.

The following sections provide steps for monitoring, improving, and testing the performance of your Exchange 2003 clusters.

Monitoring Active/Passive Clusters

Active/passive clusters are the recommended configuration for Exchange 2003 clusters. Monitor active/passive clusters just as you would stand-alone server deployments.

For information about how you can monitor Exchange, see the technical article "Better Together: Microsoft Operations Manager and Exchange Server 2003" (http://go.microsoft.com/fwlink/?LinkId=18176) and the book Monitoring Exchange 2000 with Microsoft Operations Manager 2000 (http://go.microsoft.com/fwlink/?LinkId=18177).
Monitoring Active/Active Clusters

Exchange 2003 supports active/active clusters with at most two nodes. However, active/active clusters are not a recommended configuration for Exchange 2003 clusters.

If you have an active/active cluster, use a monitoring application (such as System Monitor) to monitor the following:

- **The number of concurrent connections (users) per node**  If the number of concurrent users per node exceeds 1,900 for more than 10 minutes, move users off of the node.

- **The CPU load for each server in the cluster**  If the CPU load generated from users exceeds 40 percent for more than 10 minutes, move users off of the server.

  **Note**  This CPU load restriction applies only to load increases caused by users. Increases in CPU load that result from administrative tasks, such as moving users, are not a problem.

Monitoring Virtual Memory in a Cluster

The biggest individual consumer of memory in Exchange 2003 is the Exchange store process (Store.exe). On an active, production Exchange Server 2003 computer, it is not uncommon to notice that the Exchange store process consumes nearly all of the server memory. Like Exchange Server 5.5, the Store.exe process uses a unique cache mechanism called Dynamic Buffer Allocation (DBA). This process self-governs how much memory it uses; that is, DBA balances the amount of memory it uses against the memory usage of other applications that are running on the server. If Exchange is the only application running, DBA allocates more memory to itself.

The memory required by the Exchange store depends upon the number of Exchange databases that you have on a server, the size of those databases, and the number of transactions per each of those databases. Although each server (or cluster node) in Exchange 2003 can handle as many as 20 databases (for a maximum of four storage groups and five databases per storage group), the more databases you have, the more memory the server requires. You can lessen the memory requirements by how you configure additional databases. The first database in a storage group consumes the greatest amount of virtual memory. Thus, wherever possible, fill your storage groups to the maximum number of databases before you create a new storage group. Filling a storage group:

- Reduces memory consumption
- Reduces disk overhead
However, there are a few disadvantages to filling a storage group with databases before creating another storage group:

- Only one backup process can occur in a single storage group at a time. Backing up one database in a storage group halts the online maintenance of all other databases in the storage group.
- The ability to configure circular logging (a feature that automatically deletes log files that are older than a specified checkpoint) for a specific set of user's mailboxes is minimized. This is because you enable circular logging for the storage group, not for individual databases. If all of your databases are in a single storage group, circular logging either applies to all of the databases or none of them. If you want to apply circular logging to only a few databases, you need to create a new storage group, add the appropriate databases to the new storage group, and then apply circular logging to the new storage group. For more information about circular logging, see the book *Disaster Recovery for Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?LinkId=1714).

### Deciding Which Virtual Memory Counters to Monitor

The task of monitoring virtual memory is especially important when you are deploying Exchange 2003 clusters. This section reviews important aspects of Exchange 2003, and how it uses memory. This section also describes the specific virtual memory counters that you should monitor closely.

Windows Server 2003 and Windows 2000 implement a virtual memory system based on a flat (linear), 32-bit address space. The 32 bits of address space translate into 4 gigabytes (GB) of virtual memory. On most systems, Windows allocates half of this address space (the lower half of the 4-GB virtual address space from x00000000 through x7FFFFFFF) to processes for its unique private storage and the other half (the upper half, addresses x80000000 through xFFFFFFFF) to its own protected operating system memory usage.

\[\text{Note}\]

For more information about virtual memory, see the Windows Server 2003 and Windows 2000 Server online documentation. You can also find information about virtual memory in the Microsoft Windows Server resource kits.

It is important to monitor the virtual memory on your Exchange 2003 clusters. It is especially important to monitor the virtual memory counters that are listed in Table 8.8.
Table 8.8 Exchange 2003 virtual memory counters

<table>
<thead>
<tr>
<th>Virtual memory counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSExchangeIS\VM Largest Block Size</td>
<td>Displays the size (in bytes) of the largest free block of virtual memory. This counter displays a line that slopes down while virtual memory is consumed. Monitor this counter to ensure that it stays above 32 megabytes (MB). When this counter drops below 32 MB, Exchange 2003 logs a warning (Event ID=9582) in the event log. When this counter drops below 16 MB, Exchange logs an error.</td>
</tr>
<tr>
<td>MSExchangeIS\VM Total 16MB Free Blocks</td>
<td>Displays the total number of free virtual memory blocks that are greater than or equal to 16 MB. This counter displays a line that may first rise, but then may eventually fall when free memory becomes more fragmented. It starts by displaying a few large blocks of virtual memory and may progress to displaying a greater number of separate, smaller blocks. When these blocks become smaller than 16 MB, the line begins to fall. To predict when the number of 16 MB blocks is likely to drop below 3, monitor the trend on this counter. If the number of blocks drops below 3, restart all of the services on the node.</td>
</tr>
<tr>
<td>MSExchangeIS\VM Total Free Blocks</td>
<td>Displays the total number of free virtual memory blocks, regardless of size. This counter displays a line that may first rise, but then may eventually fall, when free memory first becomes fragmented into smaller blocks, and then when these blocks are consumed. Use this counter to measure the degree to which available virtual memory is being fragmented. The average block size is the Process\Virtual Bytes\STORE instance divided by MSExchangeIS\VM Total Free Blocks.</td>
</tr>
<tr>
<td>MSExchangeIS\VM Total Large Free Block Bytes</td>
<td>Displays the sum, in bytes, of all of the free virtual memory blocks that are greater than or equal to 16 MB. This counter displays a line that slopes down when memory is consumed.</td>
</tr>
</tbody>
</table>
Important
The task to update the virtual memory performance counters for the Exchange store does not run until at least one Exchange Virtual Server starts on the node. Therefore, in active/passive cluster scenarios, all Exchange-related virtual memory performance counters are zero (0) on a passive node. These performance counters are zero because the store on the passive node is either not going to be running or the databases will not be mounted.

As a result, having performance counters set to zero may interfere with your virtual memory performance baseline. Therefore, when monitoring these performance counters, you can expect large, free virtual memory numbers on the passive nodes.

When you monitor the virtual memory counters, the most important counter to monitor is VM Total Large Free Block Bytes, which should always exceed 32 MB. If a node in the cluster drops below 32 MB, fail over the Exchange Virtual Servers, restart all of the services on the node, and then fail back the Exchange Virtual Servers.

The Exchange store logs the following events if the virtual memory for your Exchange 2003 server becomes excessively fragmented:

**Warning logged if the largest free block is smaller than 32 MB**

<table>
<thead>
<tr>
<th>EventID=9582</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity=Warning</td>
</tr>
<tr>
<td>Facility=Perfmon</td>
</tr>
<tr>
<td>Language=English</td>
</tr>
</tbody>
</table>

The virtual memory necessary to run your Exchange server is fragmented in such a way that performance may be affected. It is highly recommended that you restart all Exchange services to correct this issue.

**Warning logged if the largest free block is smaller than 16 MB**

<table>
<thead>
<tr>
<th>EventID=9582</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity=Error</td>
</tr>
<tr>
<td>Facility=Perfmon</td>
</tr>
<tr>
<td>Language=English</td>
</tr>
</tbody>
</table>

The virtual memory necessary to run your Exchange server is fragmented in such a way that normal operation may begin to fail. It is highly recommended that you restart all Exchange services to correct this issue.

---

**Enabling Exchange Logging**

After you install Exchange 2003 on your cluster nodes and create your Exchange Virtual Server, you may want to configure Exchange logging. Although it is helpful to enable Exchange logging when you troubleshoot message flow issues, it is not recommended that you enable logging at all times. This is because logging reduces Exchange performance.
Before enabling logging on an Exchange cluster, you should disable MTA monitoring on all servers that do not have MTA installed. Then, you can enable SMTP logging on the selected servers.

**Disabling MTA Monitoring on Nodes That Are Not Running MTA**

By default, an Exchange 2003 server monitors the MTA service. In a cluster environment, MTA runs only on one of the physical nodes (computers). This means that the monitoring process reports that the nodes that are not running MTA are in an error state. This, in turn, can cause problems if Exchange 2003 is installed in a cluster with two or more Exchange Virtual Servers.

To prevent the monitoring process from incorrectly reporting that Exchange Virtual Servers that are not running the MTA service are in an error state, you should disable MTA monitoring on the second Exchange Virtual Server (and if applicable, any other additional Exchange Virtual Servers) of a cluster. You do not need to disable MTA monitoring on the first Exchange Virtual Server of a cluster.

**To disable MTA monitoring on an Exchange Virtual Server**

1. In Exchange System Manager, in the console tree, expand Servers, right-click the appropriate Exchange Virtual Server, and then click Properties.
2. In the <Server Name> Properties dialog box, click the Monitoring tab.
3. On the Monitoring tab, select Default Microsoft Exchange Services from the list of services, and then click Details.
4. In the Default Microsoft Exchange Services dialog box, select Microsoft Exchange MTA Stacks, and then click Remove.
5. Click OK twice.

**Enabling SMTP Logging**

If you want to gather statistical data about server usage, you can enable logging of the SMTP resource. However, be aware that enabling SMTP logging reduces Exchange performance. Unless you are troubleshooting or in need of statistical data, you should disable logging (the default setting).

When enabled, Internet Information Services (IIS) creates SMTP log files on the system drive of the local computer (for example, C:\Winnt\System32\Logfiles, where C is the location of your Windows Server 2003 or Windows 2000 installation). To reliably configure SMTP logging in a clustered environment, you need to change the default location of the log files (that is, the local computer) to a folder on a shared disk.
To enable SMTP logging and log the files to a shared disk

1. In Exchange System Manager, in the console tree, expand Servers, and then expand the server on which you want to enable IIS logging for SMTP.
2. In the console tree, expand Protocols, and then expand SMTP.
3. In the console tree, right-click Default SMTP Virtual Server, and then click Properties.
4. In the Default SMTP Virtual Server Properties dialog box, on the General tab, click Enable logging, and then click Properties.
5. In the Extended Logging Properties dialog box, on the General Properties tab, in Log file directory, change the SMTP log file location to a folder on a shared disk.
6. Click OK twice.

Tuning Servers in a Cluster

Even with thoughtful management and attentive monitoring, it may become necessary to tune the servers in your clusters to maintain high availability. Exchange 2003 requires much less manual tuning than Exchange 2000. In fact, Exchange 2003 performs most necessary tuning automatically.

To capitalize on the tuning features in Exchange 2003, consider making the following tuning changes after the initial installation and configuration of your Exchange cluster:

- Remove Exchange 2000 tuning parameters
- Configure the /3GB switch
- Configure the /Userva and SystemsPages options

Removing Exchange 2000 Tuning Parameters

If a server in your cluster previously ran Exchange 2000, you may have performed the manual tuning changes that were recommended by previous Exchange documentation. If you have since upgraded that server to run Exchange 2003, that server no longer needs those manual tuning changes, and you should manually remove them from the server. For information about the settings that must be removed, see "Removing Exchange 2000 Tuning Parameters" in the book Exchange Server 2003 Deployment Guide (www.microsoft.com/exchange/library).
Setting the /3GB Switch

By default, Windows Server 2003 and Windows 2000 Advanced Server allocate 2 GB of virtual address space to user mode processes, such as the Exchange store process (Store.exe). If a server has 1 GB or more of physical memory, set the /3GB switch in the Boot.ini file to increase the virtual address space.

For more information about the /3GB switch, see Microsoft Knowledge Base Article 266096, "XGEN: Exchange 2000 Requires /3GB Switch with More Than 1 Gigabyte of Physical RAM" (http://support.microsoft.com/?kbid=266096).

Important
The /3GB switch is designed for all editions of Windows Server 2003 and for Windows 2000 Advanced Server. Do not set the /3GB switch if you are running Windows 2000 Server.

Configuring /Userva and SystemPages

If the server is running Windows Server 2003, set the SystemPages value to zero, and set the /Userva=3030 parameter in the Boot.ini file. These settings allow for more system page table entries on the server, which is critical for scale-up systems.

If the server is running Windows 2000, set the SystemPages registry key to a value between 24000 and 31000. The location of the SystemPages registry key is as follows:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\SystemPages]

For additional information about the /Userva switch, see Microsoft Knowledge Base Article 810371, "XADM: Using the /Userva Switch on Windows 2003 Server-Based Exchange Servers" (http://support.microsoft.com/?kbid=810371).

Troubleshooting Your Exchange Clusters

Clustering provides a mechanism for moving resources between cluster nodes when problems occur. When a single server fails, clustering moves Exchange 2003 resources from the failed server to another server in the cluster. This failover allows services to remain available to users.

By maintaining service availability in the case of a failure, clustering gives you time to diagnose and fix the problem. Diagnosing means not only determining whether the failure is related to a single server or the entire cluster, but also whether the failure is easily repaired or requires more complex disaster recovery steps.
Identifying the Cause of a Failure

An important task in disaster recovery processes for Exchange 2003 clusters is identifying what caused a specific resource to fail. When a failure occurs in an Exchange cluster, you should first determine if the failure is on a single node, which indicates that there are problems with the node's files, or on every node, which indicates that there are problems with the cluster's objects or the shared cluster resources.

To determine the cause of the failure:

- **Search the Application Log within Event Viewer** Begin by looking for **MSExchangeCluster** events. The event description should help you determine the cause of the problem. For example, Figure 8.18 shows an event description that states that the service for that resource cannot start. Based upon this description, you should focus your troubleshooting on the service startup.

![Event Properties](image)

**Figure 8.18** MSExchangeCluster event that provides information about the failure
• **Turn on and configure verbose logging for Cluster Service** While server clusters log errors and events to the System Event log, you can achieve advanced troubleshooting by having the Cluster Service perform verbose logging to a text file named Cluster.log. For information about this log and how to enable it, see Microsoft Knowledge Base Article 168801, "How to Turn On Cluster Logging in Microsoft Cluster Server" ([http://support.microsoft.com/?kbid=168801](http://support.microsoft.com/?kbid=168801)).

• **Search for resolutions in the Microsoft Knowledge Base** ([http://support.microsoft.com/](http://support.microsoft.com/)) Many cluster-related Knowledge Base articles that are applicable to Exchange 2000 are also applicable to Exchange 2003. For this reason, search the Knowledge Base for cluster information related to Exchange 2000 as well as Exchange 2003.

If you are still unable to determine the cause of the failure, you can perform the repair options listed in "Repairing Windows 2000" or "Repairing Exchange 2000" in the book *Disaster Recovery for Microsoft Exchange 2000 Server* ([http://go.microsoft.com/fwlink/?LinkId=1714](http://go.microsoft.com/fwlink/?LinkId=1714)). If repairing the node or entire cluster is unsuccessful, you must consider replacing the node or recovering the node, cluster, or resources (such as the quorum disk resource, or Exchange mailbox and public folder stores).

**Performing Disaster Recovery on Your Exchange Clusters**

After diagnosing the failure and trying to repair the failed node or cluster, it is time to perform disaster recovery on your Exchange cluster. This may involve replacing a damaged cluster node, restoring or rebuilding a cluster node from backups, restoring a shared disk resource from backups, or recovering the entire cluster.

Disaster recovery on an Exchange cluster is a complex process that centers around devising appropriate data backup and recovery strategies. As such, it is not possible to cover the entire subject of disaster recovery in this book. You can find detailed conceptual information and step-by-step procedures concerning backing up and restoring Exchange 2003 clusters in "Backing Up Exchange 2000 Clusters" and "Restoring Exchange 2000 Clusters" in the book *Disaster Recovery for Microsoft Exchange 2000 Server* ([http://go.microsoft.com/fwlink/?LinkId=1714](http://go.microsoft.com/fwlink/?LinkId=1714)).

For a brief overview of the detailed disaster recovery steps described in the book *Disaster Recovery for Microsoft Exchange 2000 Server*, see the following two topics.
Back Up Data on an Exchange 2003 Server Cluster Node

Securing the data on your Exchange 2003 clusters requires establishing a proper and thorough backup plan. To back up the important data on the nodes of your Exchange 2003 clusters, you can use Windows 2000 Backup. You can also use third-party backup solutions to meet your backup needs. For information about third-party backup solutions, see the Exchange 2000 Server Third-party Solutions Web site (http://go.microsoft.com/fwlink/?LinkId=5225).

To secure the data in your clusters, you must do the following:

- Back up Windows in each cluster node.
- Back up the quorum disk resource of each cluster.
- Back up all Exchange databases on your shared disk resources.
- Maintain informational records about your cluster configuration.

Recovering an Exchange 2003 Cluster

Recovering from disasters that affect the nodes of your Exchange 2003 clusters can be as simple as replacing a node with a stand-by recovery server, or it can be as difficult as rebuilding an entire cluster from the beginning. If you have a proper and thorough backup plan in place, you can recover from almost any disaster that affects your Exchange organization.

You may need to do the following to recover from disasters that affect your Exchange 2003 clusters:

- Replace damaged cluster nodes.
- Restore or rebuild a cluster node from backups.
- Restore shared disk resources.
- Restore quorum disk resource.
- Restore Exchange databases.
- Recover an entire Exchange 2003 cluster.
Appendix
In addition to Microsoft® Management Console (MMC) snap-ins, Exchange System Manager, and Active Directory Users and Computers, there are a host of tools that you can use to manage and troubleshoot a Microsoft Exchange Server 2003 organization. Some of these tools are installed with Microsoft Windows®, some with Exchange, and others can be found at the Exchange Server 2003 Tools and Update Web site (http://www.microsoft.com/exchange/2003/updates). The following table lists these tools. However, be aware that not all tools are supported.

Warning
Some tools can cause serious, sometimes irreversible, problems if used incorrectly. Before using tools in your production environment, always familiarize yourself with them on test servers first. Be sure to read the documentation associated with any tool and familiarize yourself with the risks involved.

### Table A.1 Exchange Tools

<table>
<thead>
<tr>
<th>Tool name</th>
<th>Description</th>
<th>Run from</th>
<th>Install from</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory Account Cleanup Wizard</strong></td>
<td>Use to find and merge multiple accounts in Active Directory that refer to the same person.</td>
<td>Start ➤ All Programs ➤ Microsoft Exchange ➤ Deployment ➤ Active Directory Account Cleanup Wizard</td>
<td>Installed during Exchange setup.</td>
</tr>
<tr>
<td>(adcclean.exe)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Active Directory Connector Services</strong></td>
<td>Use to replicate Exchange 5.5 directory objects to Active Directory.</td>
<td>Start ➤ All Programs ➤ Microsoft Exchange ➤ Active Directory Connector</td>
<td>Exchange CD &lt;drive&gt;:\ADC\i386\setup.exe</td>
</tr>
<tr>
<td>(adcmdadmin.msc)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Active Directory Users and Computers</strong></td>
<td>Use this MMC snap-in to manage mail recipients and other Active Directory objects.</td>
<td>Start ➤ All Programs ➤ Microsoft Exchange ➤ Active Directory Users and Computers</td>
<td>Installed during Exchange setup.</td>
</tr>
<tr>
<td><em>(dsa.msc)</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Address Rewrite</strong></td>
<td>Use to rewrite return e-mail addresses on outgoing messages routed from non-Exchange mail systems to Exchange and destined outside of the organization.</td>
<td>Command prompt</td>
<td><a href="http://www.microsoft.com/exchange/2003/updates">http://www.microsoft.com/exchange/2003/updates</a></td>
</tr>
<tr>
<td><em>(Exarcfg.exe)</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ADSI Edit</strong></td>
<td>Use for low level editing of Active Directory.</td>
<td><code>&lt;drive&gt;:\Program Files\Support Tools</code></td>
<td>[Windows Server 2003 CD](&lt;drive&gt;:\support\tools\suptools.msi)</td>
</tr>
<tr>
<td><em>(adsiedit.msc)</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Application Deployment Wizard</strong></td>
<td>Use to package and deploy Exchange store applications on the Exchange store.</td>
<td>Start ➤ All Programs ➤ Exchange SDK ➤ Exchange SDK Development Tools ➤ Application Deployment Wizard</td>
<td><a href="http://go.microsoft.com/fwlink/?LinkId=18614">http://go.microsoft.com/fwlink/?LinkId=18614</a></td>
</tr>
<tr>
<td><em>(exapppacker.exe)</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Application Security Module</strong></td>
<td>Use to access and modify XML content provided by the security descriptor.</td>
<td><code>&lt;drive&gt;:\Program Files\Exchange SDK\SDK\Samples\Security</code></td>
<td><a href="http://msdn.microsoft.com/exchange">http://msdn.microsoft.com/exchange</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Download Exchange 2003 SDK Documentation and Samples</td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>(archivesink_setup.vbs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Authoritative Restore</strong></td>
<td>Use to force a restored directory database to replicate to other servers after restoring from a backup. This tool should only be used when instructed by Microsoft Product Support Services.</td>
<td>Command prompt; Must be installed to \exchsrvr\bin</td>
<td><a href="http://www.microsoft.com/exchange/2003/updates">http://www.microsoft.com/exchange/2003/updates</a></td>
</tr>
<tr>
<td>(Authrest.exe)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **Cluster Administrator** | Use to configure, control, and monitor clusters.                             | Start ➤ All Programs ➤ Administrative Tools ➤ Cluster Administrator | In Windows Server 2003, installed by default.  
In Windows 2000 Server, installed when Cluster Service component is selected during setup. |
| (cluadmin.exe)             |                                                                              |                               |                                                   |
| (Certchk.exe)              |                                                                              |                               |                                                   |

Not recommended for production environments.
<table>
<thead>
<tr>
<th>Tool name</th>
<th>Description</th>
<th>Run from</th>
<th>Install from</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(DNSDiag)</strong></td>
<td>Simple Mail Transfer Protocol (SMTP) service's internal code-path and prints</td>
<td>Must be installed to</td>
<td></td>
</tr>
<tr>
<td><strong>(Dnsdiag.exe)</strong></td>
<td>diagnostic messages that indicate how the DNS resolution is proceeding.</td>
<td><code>&lt;drive&gt;</code>:\windows\system32\inetsrv</td>
<td></td>
</tr>
<tr>
<td><strong>(Err.exe)</strong></td>
<td>Windows products.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Event Viewer</strong></td>
<td>Use this MMC snap-in to view logged events, such as errors and warnings.</td>
<td>Start ➤ All Programs ➤ Administrative Tools ➤ Event Viewer</td>
<td>Installed during Windows setup.</td>
</tr>
<tr>
<td><strong>(eventvwr.msc)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Exchange Explorer</strong> <em>(ExchExplorer.exe)</em></td>
<td>Use to explore Exchange store folders, items, and their property values. Create property and content class definitions and configure their schema scope.</td>
<td>Start › All Programs › Exchange SDK › Exchange SDK Development Tools › Exchange Explorer</td>
<td><a href="http://go.microsoft.com/fwlink/?LinkId=18614">http://go.microsoft.com/fwlink/?LinkId=18614</a></td>
</tr>
<tr>
<td><strong>Exchange Server Database Utilities</strong> <em>(eseutil.exe)</em></td>
<td>Use to perform offline database procedures, such as defragmentation and integrity checking.</td>
<td>&lt;drive&gt;\Program Files\Exchsrvr\bin</td>
<td>Installed during Exchange setup.</td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Exchange Deployment Tools**         | Use this guide to review the recommended steps and tools that help you successfully install Exchange Server 2003. | Run from Exchange CD                         | Exchange CD  
<drive>:\support\ExDeploy  
—or—  
| **Exchange Server Migration Wizard** | Use to migrate user accounts to Exchange 2003.                              | Start ➔ All Programs ➔ Microsoft Exchange ➔ Migration Wizard | Installed during Exchange setup.                                             |
| **Exchange Store Event Sink Wizard** | Use to create a Microsoft Visual Basic® project for a Component Object Model (COM) class of correctly implemented event interfaces, and a module of functions and routines that use event sink support interfaces. | Microsoft Visual Basic                         | [http://go.microsoft.com/fwlink/?LinkId=18614](http://go.microsoft.com/fwlink/?LinkId=18614)  
(Use the Add-In Manager in Visual Basic to make the Event Sink Wizard available on the Visual Basic Add-Ins menu.) |
| **Exchange Store TreeView Control**  | Use to display a hierarchical list of node objects that corresponds to folders in the Exchange store. | <drive>:\Program Files\Exchange SDK\Tools\ExchExplorer | [http://go.microsoft.com/fwlink/?LinkId=18614](http://go.microsoft.com/fwlink/?LinkId=18614)  
Run ExchTools.msi after downloading. |
<table>
<thead>
<tr>
<th>Tool name</th>
<th>Description</th>
<th>Run from</th>
<th>Install from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Stress and Performance 2003</td>
<td>Use to test stress and performance. This tool simulates large numbers of client sessions, by concurrently accessing one or more protocol servers.</td>
<td>Command prompt</td>
<td>2003 version: <a href="http://www.microsoft.com/exchange/2003/updates">http://www.microsoft.com/exchange/2003/updates</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2000 version: <a href="http://go.microsoft.com/fwlink/?LinkId=1709">http://go.microsoft.com/fwlink/?LinkId=1709</a></td>
</tr>
<tr>
<td>Exchange System Manager</td>
<td>Use this MMC snap-in to provide a graphical view of an Exchange organization where you can perform many administrative tasks.</td>
<td>Start ▶ All Programs ▶ Microsoft Exchange ▶ System Manager</td>
<td>Installed during Exchange setup.</td>
</tr>
<tr>
<td>(exchange system manager.msc)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange Workflow Configuration Scripts</td>
<td>Use wfssetup.vbs to configure the server for correct workflow functionality. Use addwfrole.vbs to add users to workflow event sink security roles.</td>
<td>Command prompt</td>
<td><a href="http://go.microsoft.com/fwlink/?LinkId=18614">http://go.microsoft.com/fwlink/?LinkId=18614</a></td>
</tr>
<tr>
<td>(wfssetup.vbs; addwfrole.vbs)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Information Store Integrity Checker (isinteg.exe)</td>
<td>Use to find and eliminate errors in the public and private information store databases. Intended for disaster recovery situations and not for routine maintenance.</td>
<td>Command prompt</td>
<td>Exchange CD &lt;drive&gt;:\setup\i386\exchange\bin</td>
</tr>
<tr>
<td>Information Store Viewer (MDBVU32) (mdbvu32.exe)</td>
<td>Use to view or set details about a user's message storage files. These files are the private information store, the personal folder file (.pst file), and the offline folder file (.ost file).</td>
<td>Command prompt</td>
<td><a href="http://www.microsoft.com/exchange/2003/updates">http://www.microsoft.com/exchange/2003/updates</a></td>
</tr>
<tr>
<td>Internet Information Services (IIS) Manager (iis.msc)</td>
<td>Use to configure Outlook Web Access settings.</td>
<td>Start ➤ All Programs ➤ Administrative Tools ➤ Internet Information Services (IIS) Manager</td>
<td>Add/Remove Programs ➤ Add/Remove Windows Components</td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>LDP (ldp.exe)</td>
<td>Use to perform Lightweight Directory Access Protocol (LDAP) searches against Active Directory.</td>
<td>&lt;drive&gt;:\Program Files\Support Tools</td>
<td>Windows Server 2003 CD &lt;drive&gt;:\support\tools</td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Managed Exchange TreeView Control</strong></td>
<td>Use in managed Windows applications to display a hierarchical list of nodes that correspond to a mail or public folder hierarchy. Add, delete, and move folders in the Exchange store.</td>
<td>&lt;drive&gt;:\Program Files\Exchange SDK\Tools\ExchangeTreeViewControl</td>
<td></td>
</tr>
<tr>
<td><strong>Microsoft Baseline Security Analyzer (MBSA)</strong></td>
<td>Use to scan local or remote systems for common misconfigurations and to check for security best practices.</td>
<td>Command prompt</td>
<td><a href="http://go.microsoft.com/fwlink/?LinkId=18614">http://go.microsoft.com/fwlink/?LinkId=18614</a></td>
</tr>
<tr>
<td><em>GUI:</em> (MBSA.exe)</td>
<td></td>
<td></td>
<td>To use this tool, you must add a reference to it in a Microsoft Visual Studio® .NET project, and then add it to the toolbox in the project.</td>
</tr>
<tr>
<td><em>Command Line:</em> (mbsacli.exe)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Tool name</th>
<th>Description</th>
<th>Run from</th>
<th>Install from</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MTA Check</strong> (Mtacheck.exe)</td>
<td>Use when MTA will not start, due to corruption or suspected corruption in the MTA database. This tool provides a soft recovery of a corrupted MTA database.</td>
<td>Command prompt</td>
<td><a href="http://www.microsoft.com/exchange/2003/updates">http://www.microsoft.com/exchange/2003/updates</a></td>
</tr>
<tr>
<td><strong>Network Monitor</strong> (netmon.exe)</td>
<td>Use to diagnose issues with server connectivity.</td>
<td>Start ‣ All Programs ‣ Administrative Tools ‣ Network Monitor</td>
<td><a href="http://www.microsoft.com/exchange/2003/updates">Add/Remove Programs ‣ Add/Remove Windows Components</a></td>
</tr>
<tr>
<td><strong>Performance Monitor</strong> (perfmon.msc)</td>
<td>Use for establishing a baseline of performance and for troubleshooting performance issues.</td>
<td>Start ‣ All Programs ‣ Administrative Tools ‣ Performance</td>
<td>Installed during Windows setup.</td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>PFMigrate</td>
<td>Use to migrate public folders from Exchange 5.5 to Exchange 2003. Can also be used to move the offline address book, Schedule+, Free/Busy folder, and organization forms.</td>
<td>Command prompt</td>
<td>Exchange CD &lt;drive&gt;:\support\ExDeploy</td>
</tr>
<tr>
<td>RPC Ping utility</td>
<td>Use to confirm the RPC connectivity between the computer running Microsoft Exchange Server and any of the client workstations on the network.</td>
<td>Command prompt</td>
<td><a href="http://go.microsoft.com/fwlink/?Linkid=18615">http://go.microsoft.com/fwlink/?Linkid=18615</a></td>
</tr>
<tr>
<td>Tool name</td>
<td>Description</td>
<td>Run from</td>
<td>Install from</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol Accept/Deny List</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration (ExIpsec.dll)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>Use to troubleshoot Exchange mail flow.</td>
<td>Command prompt</td>
<td>Installed during Windows setup.</td>
</tr>
<tr>
<td>(telnet.exe)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WinRoute</td>
<td>Use to connect to the link state port (TCP/IP 691) on an Exchange server and extract the link state information for an organization.</td>
<td>Command prompt</td>
<td><a href="http://www.microsoft.com/exchange/2003/updates">http://www.microsoft.com/exchange/2003/updates</a></td>
</tr>
<tr>
<td>(winroute.exe)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B

Services Used by Exchange

Services are application types that run in the system background. Services provide core operating system features, such as Web serving, event logging, file serving, help and support, printing, cryptography, and error reporting. To provide core system features to its users, Microsoft® Exchange Server 2003 provides a number of services (see Table B.1) that run on an Exchange server.

**Note**
To manage services on local or remote computers, use the Microsoft Management Console (MMC) Services snap-in (see Figure B.1).

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messenger</td>
<td>Transmits send and Ack</td>
</tr>
<tr>
<td>Microsoft Exchange Event</td>
<td>Monitors folders and files</td>
</tr>
<tr>
<td>Microsoft Exchange IMAP</td>
<td>Provides Internet Message Access Protocol (IMAP)</td>
</tr>
<tr>
<td>Microsoft Exchange Information Store</td>
<td>Manages the Microsoft Information Store</td>
</tr>
<tr>
<td>Microsoft Exchange Management</td>
<td>Provides Exchange management</td>
</tr>
<tr>
<td>Microsoft Exchange MTA Backends</td>
<td>Provides Microsoft Exchange MTA Backends</td>
</tr>
<tr>
<td>Microsoft Exchange POP3</td>
<td>Provides Post Office Protocol</td>
</tr>
<tr>
<td>Microsoft Exchange Routing Engine</td>
<td>Provides topology and routing</td>
</tr>
<tr>
<td>Microsoft Exchange Site Replication Service</td>
<td>Provides monitoring, monitoring, and site replication</td>
</tr>
<tr>
<td>Microsoft Exchange System Administrator</td>
<td>Manages Exchange System Administrator</td>
</tr>
<tr>
<td>Microsoft Search</td>
<td>Creates full-text indexes</td>
</tr>
<tr>
<td>Microsoft Shadow Copy Provider</td>
<td>Manages software backups</td>
</tr>
</tbody>
</table>

**Figure B.1** Services snap-in
<table>
<thead>
<tr>
<th>Service display name/abbreviation</th>
<th>Default startup type</th>
<th>Description and dependencies</th>
</tr>
</thead>
</table>
| Microsoft Exchange Calendar Connector (MSExchangeCalCon) | Manual | Allows sharing of Lotus Notes and Novell GroupWise Free/Busy Information.  
*Dependencies:*  
Event Log, Microsoft Exchange Information Store, Microsoft Exchange Connectivity Controller |
| Microsoft Exchange Connectivity Controller (MSExchangeCoCo) | Manual | Provides support services for Microsoft Exchange connectors.  
*Dependencies:*  
Event Log |
| Microsoft Exchange Connector for Lotus Notes (LME-NOTES) | Manual | Allows sharing of mail traffic with Lotus Notes systems.  
*Dependencies:*  
Event Log, Microsoft Exchange Connectivity Controller |
| Microsoft Exchange Connector for Novell GroupWise (LME-GWISE) | Manual | Allows sharing of mail traffic with Novell GroupWise systems.  
*Dependencies:*  
Event Log, Microsoft Exchange Connectivity Controller, Microsoft Exchange Router for Novell GroupWise |
| Microsoft Exchange Event (MSExchangeES) | Manual | Monitors folders and triggers events for server applications compatible with Exchange Server 5.5.  
*Dependencies:*  
Microsoft Exchange Information Store |
| Microsoft Exchange IMAP4 (IMAP4Svc) | Disabled | Provides Internet Message Access Protocol version 4 (IMAP4) services to clients. If this service is stopped, clients are unable to connect to this computer using IMAP4.  
*Dependencies:*  
IIS Admin Service |
<table>
<thead>
<tr>
<th>Service display name/abbreviation</th>
<th>Default startup type</th>
<th>Description and dependencies</th>
</tr>
</thead>
</table>
| Microsoft Exchange Information Store (MSExchangeIS) | Automatic | Manages the Exchange store. The service makes mailbox stores and public folder stores available. If this service is stopped, mailbox stores and public folder stores on this computer are unavailable. If this service is disabled, any services that explicitly depend on it will fail to start. *Dependencies:*  
Microsoft Exchange System Attendant |
| Microsoft Exchange Management (MSExchangeMGMT) | Automatic | Provides Exchange management information using Windows Management Instrumentation (WMI). If this service is stopped, WMI providers implemented to work in Microsoft Exchange Management, like message tracking and Directory Access, will not work. *Dependencies:*  
Remote procedure call (RPC), WMI |
| Microsoft Exchange MTA Stacks (MSExchangeMTA) | Automatic | Provides Exchange X.400 services. You use Exchange X.400 services to connect to Exchange 5.5 servers and other connectors (custom gateways). If this service is stopped, Exchange X.400 services are unavailable. *Dependencies:*  
Microsoft Exchange System Attendant |
| Microsoft Exchange POP3 (POP3Svc) | Disabled | Provides Post Office Protocol version 3 (POP3) services to clients. If this service is stopped, clients are unable to connect to this computer using POP3. *Dependencies:*  
IIS Admin Service |
None |
<table>
<thead>
<tr>
<th>Service display name/abbreviation</th>
<th>Default startup type</th>
<th>Description and dependencies</th>
</tr>
</thead>
</table>
| Microsoft Exchange Routing Engine (RESvc) | Automatic | Provides topology and routing information to servers running Exchange 2003. If this service is stopped, optimal routing of messages will not be available.  
**Dependencies:**  
IIS Admin Service |
| Microsoft Exchange Site Replication Service (MSExchangeSRS) | Disabled | Provides directory interoperability between Exchange 5.5 and Exchange 2000 Server or Exchange 2003. Site Replication Service (SRS) acts as a directory replication bridgehead server for an Exchange site. SRS runs on Exchange 2000 and serves as a modified Exchange 5.5 directory. SRS uses Lightweight Directory Access Protocol (LDAP) to communicate to both the Active Directory® directory service and the Exchange 5.5 directory. To Exchange 5.5, SRS looks like another Exchange 5.5 configuration/recipients replication partner.  
**Note**  
Enabled by default on computers that have Active Directory Connector (ADC).  
**Dependencies:**  
Microsoft Exchange System Attendant |
<table>
<thead>
<tr>
<th>Service display name/abbreviation</th>
<th>Default startup type</th>
<th>Description and dependencies</th>
</tr>
</thead>
</table>
| Microsoft Exchange System Attendant (MSExchangeSA) | Automatic | Provides monitoring, maintenance, and Active Directory lookup services (for example, monitoring of services and connectors, proxy generation, Active Directory to metabase replication, publication of free/busy information, offline address book generation, mailbox maintenance, and forwarding Active Directory lookups to a global catalog server). If this service is stopped, monitoring, maintenance, and lookup services are unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.  
**Dependencies:**  
Event Log, NTLM Security Support Provider, Remote Procedure Call (RPC), Server, Workstation |

**Note**
The following Exchange services are set to manual, if installed on a cluster: IMAP4Svc, MSExchangeMTA, MSExchangeSA, MSExchangeIS, SMTPsvc, NNTPsvc, REsvc, MSExchangeMGMT.

You must enable the following Microsoft Windows® services before you run Exchange Setup:

- World Wide Web service
- Simple Mail Transfer Protocol (SMTP) service
- Network News Transfer Protocol (NNTP) service

For more information about these services, see the book *Exchange Server 2003 Deployment Guide* (http://www.microsoft.com/exchange/library).
APPENDIX C

Configuration Settings for a Four-Node Cluster

As shown in Figure C.1, the recommended configuration for a four-node Microsoft® Exchange Server 2003 cluster contains three active nodes and one passive node, where each of the active nodes contains one Exchange Virtual Server (EVS). This configuration is advantageous because it provides you with the capacity of running three active Exchange servers, while maintaining the failover security provided by one passive server.

![Diagram of a four-node Exchange cluster]

**Figure C.1** Recommended configuration of a four-node Exchange cluster

**Note**

The recommended four-node cluster can handle a single node failure at a time and maintain 100 percent availability after the failover has occurred. A second failure during this period leaves the cluster in a partially up state. To illustrate this concept, here is an example:

- **First failure** If Node 1 fails, Node 2 still owns EVS2, Node 3 still owns EVS3, and Node 4 takes ownership of EVS1 with all the storage groups mounted after the failover.

- **Second failure** If another node fails while Node 1 is still recovering from the failure, the Exchange Virtual Server on the second failed node attempts to fail over to a node not hosting an Exchange Virtual Server. Because failover is not possible, the second Exchange Virtual Server remains in a failed state.

Tables C.1 and C.2 list the recommended configuration settings for this four-node cluster.

### Table C.1  Exchange Virtual Server settings

<table>
<thead>
<tr>
<th>Properties dialog box</th>
<th>Tab</th>
<th>Recommended settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS1</td>
<td>General</td>
<td>Preferred Owners Node 1</td>
</tr>
<tr>
<td>EVS2</td>
<td>General</td>
<td>Preferred Owners Node 2</td>
</tr>
<tr>
<td>EVS3</td>
<td>General</td>
<td>Preferred Owners Node 3</td>
</tr>
<tr>
<td>EVS1, EVS2, EVS3</td>
<td>Failback</td>
<td>Prevent Failback</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This default option disables failback on each ESV. The administrator can move the server back at an appropriate time.</td>
</tr>
</tbody>
</table>

### Table C.2  Exchange resource settings

<table>
<thead>
<tr>
<th>Properties dialog box</th>
<th>Tab</th>
<th>Recommended settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Resource</td>
<td>General</td>
<td>Possible Owners All nodes are possible owners.</td>
</tr>
<tr>
<td>Exchange Resource</td>
<td>Advanced</td>
<td>Restart</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This default option enables Cluster Service to attempt to restart the resource after the initial failure of the resources. To enable Restart, select the Affect the group check box with a threshold of 3 and a period of 900 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pending Timeout 3 minutes (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>As mentioned in &quot;Setting Pending States&quot; in Chapter 8, &quot;Managing Exchange Clusters,&quot; the Exchange store instance is not restricted by this setting when coming online.</td>
</tr>
</tbody>
</table>
APPENDIX D

Identifying and Accessing Exchange Store Components

The Exchange store has multiple components. Some components can reside on many separate servers, and others are specific to an administrative group but not to a particular server. Figure D.1 shows where these components reside in Exchange System Manager. Storage groups, mailbox stores, and public folder stores on a specific server reside under the node for the server. Public folders reside under the Folders node.

Figure D.1   Store information in Exchange System Manager, found under both the server's node and the Folders node
Table D.1 lists the types of Exchange store components, their relationship to other components, and ways to administer them. All of these components must work together for the Exchange store to function correctly.

**Table D.1  Identifying the components of the Exchange store**

<table>
<thead>
<tr>
<th>Component</th>
<th>Relationship to other components</th>
<th>Administrative approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage group</td>
<td>A grouping of mailbox stores and public folder stores. Stores in a storage group share a single backup schedule and a single set of transaction logs. There can be as many as four storage groups per server.</td>
<td>Configure a storage group on a particular server in Exchange System Manager.</td>
</tr>
<tr>
<td>Mailbox store</td>
<td>A storage device for mailboxes. There can be as many as five stores per storage group, and any number of the five may be mailbox stores.</td>
<td>Configure a mailbox store on a particular server, or by setting system policies.</td>
</tr>
<tr>
<td>Mailbox</td>
<td>Associated with a user in the Microsoft Active Directory® directory service. There can be many mailboxes per mailbox store.</td>
<td>Create a mailbox using Active Directory Users and Computers. Use Active Directory Users and Computers for most tasks. Use either Exchange System Manager or Active Directory Users and Computers to move or delete mailboxes.</td>
</tr>
<tr>
<td>Public folder store</td>
<td>A storage device for public folders and public folder tree information. A public folder store must be associated with one public folder tree. There can be as many as five stores per storage group, and any number of the five may be public folder stores. Each server has one default public folder store (called <strong>Public Folder Store</strong>) that supports the <strong>Public Folders</strong> tree.</td>
<td>Configure a public folder store on a particular server, or by setting system policies.</td>
</tr>
<tr>
<td>Component</td>
<td>Relationship to other components</td>
<td>Administrative approach</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Public folder</td>
<td>A group of public folders in a hierarchical structure. Also called a public folder hierarchy. One tree can have multiple public folder stores, if each public folder store is located on a separate server. These stores replicate tree information among themselves. Each organization has one default tree called <strong>Public Folders</strong> (also called the MAPI public folder tree) that is compatible with the Microsoft® Exchange Server 5.5 public folder tree and is accessible using Microsoft Outlook® or Outlook Web Access. You can create new public folder trees (called general-purpose public folder trees) that users can access using Outlook Web Access.</td>
<td>Configure a public folder tree in the <strong>Folders</strong> container of the administrative group where the tree was created.</td>
</tr>
<tr>
<td>Public folder</td>
<td>Stored in public folder stores. Each public folder belongs to a public folder tree. A tree can have many folders. If the tree has many stores, you can configure which stores hold a copy of a particular folder's content.</td>
<td>Configure a public folder in the <strong>Folders</strong> container of the administrative group where the tree was created.  You can also access properties from the public folder store.</td>
</tr>
</tbody>
</table>
APPENDIX E

Controlling Public Folder Replication

This appendix presents an overview of how Microsoft® Exchange public folder replication works, how you can configure replicas, and how you can tune the replication process. Understanding the basic replication processes will help you to troubleshoot replication issues that are specific to your Exchange topology. (For information about common problems that may arise during public folder replication, see Appendix G, "Troubleshooting and Repairing Store Problems."

This appendix also provides recommendations for configuring public folder replication when you have a mixed-mode topology (a topology that includes servers running Microsoft Exchange Server 5.5), and describes how to use the Inter-Organizational Replication Tool to replicate information between two Exchange organizations.
How Replication Works

When multiple public folder stores—each located on a separate server—support a single public folder tree, Exchange uses public folder replication to keep the stores synchronized.

Public folder content exists only in stores that are configured to have a replica of a specific folder. Content and hierarchy information are replicated separately. Each store keeps a copy of the hierarchy, which includes lists of which other stores hold content replicas of each folder. Content replicas exist only on the stores that you specify.

For each content replica in a public folder store, the store maintains a Replication State Table. A replica's Replication State Table stores the following information:

- Basic information that is required to construct updates to the replica.
- Information about the last update to the replica that originated in the local store, including the change number of the update.
- Groups of updates that have been applied to all other known replicas of the folder. The updates in each group are identified by change numbers; the set of change numbers of all of the updates in a group is called a CNSet. Update information is passed from one store to another as part of the replication process.

By combining the lists of stores that hold content replicas and the information in the Replication State Tables, each public folder store can determine how up-to-date it is compared to the other stores that support the public folder tree. For information about how public folder stores use this information, see "Status and Backfill Messages" later in this section.
When a folder or its contents are modified, the store that is hosting the replica that was changed e-mails the change to the other stores in the form of a replication message. Exchange routes the replication message the same way that it routes normal e-mail messages. For replication to work properly:

- The Recipient Update Service must be able to stamp e-mail attributes on the store objects in the Microsoft Active Directory® directory service (mail, proxyAddresses, and so on). Normally, Exchange automatically creates the recipient policies that the Recipient Update Service follows to update the store objects.

- Exchange must be able to route e-mail between the replicating servers. Replication messages can be routed through different types of e-mail links (routing group connectors, X.400 connectors, and so on).

**Note**
The replication process uses the Active Directory attributes of the public folder stores, not of individual public folders. The Active Directory entries for individual public folders are only used to send regular e-mail to or from the folders. Figure E.1 shows a public folder store object in Active Directory. A public folder store object is configured and maintained automatically, and resides in the Configuration container in Active Directory.

![Figure E.1 Public folder store objects in Active Directory](image-url)
However, replication messages differ from normal e-mail messages in that Exchange treats replication messages as system messages. This means that replication messages are not bound by the normal restrictions that are applied to user e-mail messages, such as size and delivery restrictions. In the Exchange 5.5 Directory, replication messages were also system messages.

Table E.1 lists the different types of replication messages that Exchange uses.

### Table E.1  Types of public folder replication messages and when they are used

<table>
<thead>
<tr>
<th>Message type*</th>
<th>When used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy (0x2)</td>
<td>Replicates hierarchy changes from the local public folder store to all other public folder stores that support the same hierarchy.</td>
</tr>
<tr>
<td>Content (0x4)</td>
<td>Replicates content changes from one replica to all other content replicas of that folder.</td>
</tr>
<tr>
<td>Backfill request (0x8)</td>
<td>Requests missing data (in CNSets) from another store (both hierarchy and content change numbers).</td>
</tr>
<tr>
<td>Backfill response (0x80000002 or 0x80000004)</td>
<td>Sends missing data (in CNSets) to a store that requested missed updates.</td>
</tr>
<tr>
<td>Status (0x10)</td>
<td>Sends the current CNSets of a folder to one or more replicas of that folder (both hierarchy and content change numbers).</td>
</tr>
<tr>
<td>Status request (0x20)</td>
<td>Requests CNSets to be replicated, or status messages to be returned (both hierarchy and content change numbers).</td>
</tr>
</tbody>
</table>

* The value in parentheses is the hexadecimal notation of the message type, which is used in events and logs. Use the hexadecimal value when you are troubleshooting replication issues. For more information about troubleshooting replication issues, see Appendix G, "Troubleshooting and Repairing Store Problems."
The Basic Hierarchy and Content Replication Process

When a user modifies a public folder, the following process occurs on the server that holds the replica of the folder to which the user is connected:

1. The public folder store records the change, and checks the folder properties to determine which other servers hold a replica of that folder. If other replicas exist, the store determines what information needs to be replicated to them. This information becomes the "update" to the replicas.

   Public folder replication is object-based: if one property of an object is modified, the entire object must be replicated. The store that is replicating the change cannot assume that all of the receiving replicas are up-to-date, so it must send the whole object. The implications for the different types of replication are as follows:
   - **Hierarchy replication** If a new folder is created or if a folder property (such as its display name) is changed, the update includes all of the folder's properties.
   - **Content replication** If a new message is posted or an existing message is modified, the update includes the entire message and its properties.

2. The public folder store assigns a change number to the update.

   When a folder replicates an update to another server, the change number is included with the update. The change number is then used by the receiving server to determine whether the update represents a new change, and also whether it is missing any data.

   Change numbers are similar to the Update Sequence Numbers (USNs) used in Active Directory replication. However, in most other aspects, public folder replication is very different from Active Directory replication.

3. The public folder store "packs" updates into a replication message. As indicated earlier, the change numbers of all of the updates in the message are referred to as a CNSet.

   Along with the updates, the public folder store packs information from the Replication State Table of each folder, including the CNSets that were applied to the replica previously.

   To reduce mail traffic, multiple hierarchy updates can be packed into a single replication message. Likewise, multiple content updates for the same folder can be packed into a single replication message. However, hierarchy updates cannot be packed into the same replication message as content updates.
4. The public folder store addresses the replication message to the other public folder stores that host replicas that are affected by the updates.

5. At the next scheduled replication cycle (which is determined by the replication interval set for the public folder store), the public folder store sends the message, along with any other messages that have been packed since the previous replication cycle.

   The public folder store relies on Exchange's internal routing components to deliver replication messages. The store makes no attempt to split replication messages based on topology details. If the content of a folder is modified and it has five other replicas, a single replication message is generated and addressed to all five other stores. It is up to the routing components within Exchange to determine how to route and deliver the message.

When a public folder store receives a replication message, the following process occurs:

1. The public folder store "unpacks" the updates from the replication message.

2. The store compares the change numbers to the list of change numbers that it already has and identifies the updates that have not been received previously.

3. The store applies the new updates to the appropriate folder replicas.

4. For each updated replica, the store updates the replica's Replication State Table with the change numbers of the current updates.

   If the replication message indicates that other CNSets have been applied to other replicas of the folder but not to this store's replica, the store records that information as well and prepares to send a backfill request (as described in the next section).
Status and Backfill Messages

A store sends a status message to another store to indicate the current state of a particular folder on the sending store. "Backfilling" occurs when a public folder store determines that it has not received all of the updates for a replicated folder and must retrieve the missing updates from another store.

If a public folder store receives a status message regarding a folder that indicates that the sending store has more recent information about the folder, the receiving store creates a backfill request. If the change numbers are shown to be equal (or the change numbers on the receiving server are more recent), no action is taken.

A store sends a status request under the following circumstances:

- It receives a hierarchy update that includes a change to the list of stores that hold replicas of a folder. For example, you used Exchange System Manager to add a store to the list or remove a store from the list.
- A new store has started for the first time. This status request requires every known replica of the folder to respond. When all of the stores hosting these replicas have responded, the new store sends a backfill request to the "best" of the known stores.

A store sends a status message under two circumstances:

- In response to a status request sent by another store, as described previously. The status message is sent only to the requesting store.
- Twenty-four hours after the most recent update to a folder was received, if there have been no subsequent updates. Each time the store receives an update for a specific folder, the timer is reset to 24 hours. This status message goes to the other public folder stores that have replicas of the updated folder.

The store follows a set schedule for checking whether status messages need to be sent. By default, this check runs at 00:15 and 12:15 Coordinated Universal Time (Greenwich Mean Time). As a result, after a folder has been updated, a status message may be sent as many as 36 hours later.
Figure E.2 depicts the basic sequence of events that is triggered when you add a content replica to a public folder store (adding the public folder store to the folder's replica list) in a simplified two-server scenario. Note that the sequence of steps depends on factors such as the timing of the replication intervals and the routing topology.

Figure E.2  The sequence of events when you add a replica to a public folder store
The details of the process are as follows:

1. Working on ExServ01, an Administrator adds ExServ01 to a folder's replica list.
2. ExServ01 sends out a hierarchy message.
3. ExServ01 sends a status request to ExServ02.
4. ExServ02 adds ExServ01 to the local copy of the folder's replica list.
5. ExServ02 sends a status message to ExServ01 that includes the full CNSet of the folder.
6. ExServ01 determines that all of the folder content is missing and creates a backfill request.
7. If the content is still missing when the backfill time-out elapses, ExServ01 sends a backfill request to ExServ02.
8. ExServ02 compiles the content messages and sends them to ExServ01.
9. ExServ01 uses the incoming content messages to update the folder content and related tracking information.
10. If change numbers still appear to be missing, ExServ01 waits 24 hours and then sends an updated backfill request. If a server other than ExServ02 is available, ExServ01 may send the request to that server.
Figure E.3 shows the sequence of events that is triggered when you remove a replica from a public folder store (removing the public folder store from the folder's replica list) in a simplified two-server scenario. Note that the sequence of steps would become more complex in topologies with more than two servers, and depending on how the delete command originates.

The details of the process are as follows:

1. Working on ExServ01, an Administrator removes ExServ01 from a folder's replica list.
2. ExServ01 marks its replica (the copy of the folder on ExServ01) as "delete pending". Clients can no longer access the folder using this store.
3. ExServ01 sends out a hierarchy message.
4. ExServ02 updates its copy of the folder's replica list to show that the folder is in the "delete pending" state on ExServ01.
   ExServ02 will no longer refer clients that are looking for this folder to ExServ01.

5. ExServ01 sends a status request to ExServ02.

6. ExServ02 sends a status message to ExServ01.

7. ExServ01 checks that the folder replica on ExServ02 contains all of the information that the "delete pending" replica does. If it does not, ExServ01 returns to Step 5. Otherwise, ExServ01 continues with Step 8.

8. ExServ01 marks its replica as "delete now". The next maintenance cycle will remove the replica from ExServ01.

9. ExServ01 sends out a hierarchy message.

10. ExServ02 removes ExServ01 from its copy of the folder's replica list.

The following events may alert a public folder store to missing updates that need to be backfilled:

- An incoming replication message contains CNSets for a specific folder, and the incoming CNSets are out of sequence with the CNSets that are listed in that folder's Replication State Table. The public folder store identifies the missing change numbers and packs them into a backfill request.

- A public folder store starts for the first time. As described above, the new store sends out status requests to get information about the other stores in the hierarchy, and then prepares a backfill request.

- An incoming hierarchy message indicates that a new content replica is to be placed in the public folder store. The store prepares a backfill request to get the content for the new replica.

To select a server (or servers) to use as a backfill source, Exchange first creates a list of all of the servers that have some portion of the necessary content, and then it sorts the list as follows:

1. According to the lowest transport cost. Servers in the same site have priority over servers in remote sites.

2. For servers with the same transport cost, sorts again according to newest Exchange version.
   In Microsoft Exchange Server 2003, transport cost has greater importance in the selection criteria. This is a change from earlier versions of Exchange. In Microsoft Exchange 2000 Server and Exchange 5.5, servers running newer Exchange versions are selected over servers running older versions, regardless of the transport cost. For example, a server in a remote site running Exchange 2000 would be selected over a local server running Exchange 5.5.
3. For servers with the same transport cost and Exchange version, sort again according to the largest number of necessary changes that are available on the server. The backfill request will go to this server.

In previous versions of Exchange, a server that holds all of the necessary updates is chosen over a server that holds only some of the updates, regardless of transport cost. In Exchange 2003, this preference has been changed so that if some updates are available on a server with a lower transport cost, that server is selected to backfill those updates, even if the rest of the updates must be obtained from other (higher-cost) servers.

4. If one server does not have all of the needed changes, Exchange runs through this process again to select the server with the next largest number of changes. This process is repeated until all of the changes have been requested.

In previous versions of Exchange, if no single server could satisfy a backfill request, each separate backfill request would be held 24 to 48 hours before being sent. Using the new process, requests can be sent simultaneously to different servers after the initial 6-hour time-out (12 hours for sending requests to servers in remote sites). For more information about backfill time-outs, see Table E.2.

This process is faster and more efficient than that used by all versions of Exchange 2000 Server. Consider an Exchange 5.5 deployment of several sites (with multiple servers per site, all replicating public folders) that must be upgraded to Exchange 2003. Add one Exchange 2003 server to each site. In each site, the Exchange 2003 server backfills its public folders from the local Exchange 5.5 servers, rather than searching for a newer server in one of the remote sites.

After the store has created a backfill request, it holds the request for a specified length of time before sending it. If, in the meantime, the store receives an update that fills in the missing information, the request is discarded without being sent. Table E.2 lists the default backfill time-out values, which depend on where the request is to be sent and whether the request has been sent before.

<table>
<thead>
<tr>
<th>Type of request</th>
<th>Addressed to a store in the local site</th>
<th>Addressed to a store in a remote site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial backfill</td>
<td>6 hours</td>
<td>12 hours</td>
</tr>
<tr>
<td>First backfill retry</td>
<td>12 hours</td>
<td>24 hours</td>
</tr>
<tr>
<td>Subsequent backfill retries</td>
<td>24 hours</td>
<td>48 hours</td>
</tr>
</tbody>
</table>
Configuring the Default Replication Schedule

If the majority of folders in a specific public folder store contain information that rarely changes, you can schedule less frequent replication for all of the folders in the public folder store. However, if one folder contains time-critical information that is updated more often, you can set up more frequent replication intervals for that folder to ensure that all replicas remain current. You can also schedule replication during non-peak hours to reduce message traffic.

If all public folders are used with the same frequency, you can create one replication schedule for all of the folders by setting the schedule on the public folder store. After you set the store's schedule, all folders that are set to Default Schedule replicate according to the store's schedule.

To set a default replication schedule for a public folder store, use the Replication tab of the public folder store's Properties dialog box, as shown in Figure E.4.

![Figure E.4 The Replication tab for a public folder store](image)
Use the following options to set the replication schedule:

- **Replication interval**  Select a replication interval, or click Customize to display the Schedule dialog box, in which you can define the desired replication interval.

- **Replication interval for always (minutes)**  Use this setting if you use the Always Run setting for Replication interval. This interval is the number of minutes between replication cycles.

- **Replication message size limit (KB)**  Specify a size limit for the messages that Exchange uses to pass replication information from one server to another.

---

### Configuring Replicas

**Important**

Before you configure replication settings, you must first create public folder stores on the servers to which you want to replicate. Associate those stores with the public folder tree that contains the folder that you want to replicate.

After you create multiple public folder stores for a public folder tree, you need to identify the folders to replicate to the stores. Folders are not replicated automatically. Use a public folder's Replication property tab (shown in Figure E.5) to configure which stores will have replicas of the folder, and how often replication will occur.

![Figure E.5 The Replication tab for a public folder](image)
Adding or Removing Content Replicas

In the `Replicate content to these public stores` section of the `Replication` tab, use the `Add` or `Remove` buttons to specify the public folder stores that should hold content replicas for this folder. The group of public folder stores that you specify is the folder's replica list.

Setting a Folder-Specific Replication Schedule

By default, folders in a specific public folder store replicate according to the store's schedule. If you have a few folders that should replicate more often or less often than others, you can set a specific replication schedule for those folders. On the folder's `Replication` tab, you can use the `Public folder replication interval` drop-down list to set a replication interval of 2 hours or 4 hours, or you can click `Customize` to create a different schedule.

Setting Replication Message Priority

The `Replication message priority` setting determines the order in which replication messages for the specific folder are delivered to the target store (relative to replication messages that the target store receives from other sources). See Table E.3 for explanations of the settings that are available.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not urgent</td>
<td>Messages with this priority are delivered last.</td>
</tr>
<tr>
<td>Normal</td>
<td>Messages with this priority are sent before non-urgent messages; however, all urgent messages are delivered first.</td>
</tr>
<tr>
<td>Urgent</td>
<td>Messages with this priority are sent before messages with a priority of normal or not urgent.</td>
</tr>
</tbody>
</table>
Checking Replication Status

For actively updated information about a specific public folder's replication status, use the Replication tab in the left pane of Exchange System Manager (shown in Figure E.6). The Replication tab lists the servers that hold content replicas of the specific public folder, the replication status of each server, the last time a replication message was received, and the average transmission time. Use this information for performance monitoring.

![Exchange System Manager](image)

Figure E.6  Replication tab of a public folder

You can also view this information by clicking Details on the Replication tab of the folder's Properties dialog box.

Table E.4 lists a number of additional time-outs and settings that control public folder replication. Values that you can modify are noted in the table; other values are for reference only. This information is provided to help you troubleshoot replication issues, especially if replication seems to take an unusual length of time.
### Table E.4  Default time-outs and intervals that Exchange uses during replication

<table>
<thead>
<tr>
<th>Replication event</th>
<th>Default time-out</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication Expiry</td>
<td>24 hours</td>
<td>The frequency with which the store checks folders for expired information.</td>
</tr>
<tr>
<td>Replication Send Always</td>
<td>15 minutes</td>
<td>The default &quot;Replicate Always&quot; value, indicating how often the store checks to see whether it needs to replicate content. Can be adjusted using Exchange System Manager.</td>
</tr>
<tr>
<td>Replication Send Folder Tree</td>
<td>5 minutes</td>
<td>The frequency with which the store checks to determine whether a hierarchy replication message needs to be sent.</td>
</tr>
<tr>
<td>Replication Send Status Timeout</td>
<td>24 hours</td>
<td>The frequency with which the store checks to determine whether a status message for a folder should be sent.</td>
</tr>
<tr>
<td>Replication Timeout</td>
<td>5 minutes</td>
<td>The frequency with which the store checks to determine whether any backfill time-outs have expired.</td>
</tr>
<tr>
<td>New Replica Backfill Request Delay</td>
<td>15 minutes</td>
<td>The length of time that the store delays before sending a backfill request for a new folder replica when the data is available in the same Exchange site.</td>
</tr>
<tr>
<td>Short Backfill Request Delay</td>
<td>6 hours</td>
<td>The length of time that a store delays before sending a backfill request when the data is available in the same Exchange site.</td>
</tr>
<tr>
<td>Long Backfill Request Delay</td>
<td>12 hours</td>
<td>The length of time that a store delays before sending a backfill request when the data is not available in the same Exchange site.</td>
</tr>
<tr>
<td>Short Backfill Request Timeout</td>
<td>12 hours</td>
<td>The time-out value that is used when trying to send a backfill request when the data is available in the same Exchange site.</td>
</tr>
<tr>
<td>Long Backfill Request Timeout</td>
<td>24 hours</td>
<td>The time-out value that is used when trying to send a backfill request when the data is not available in the same Exchange site.</td>
</tr>
</tbody>
</table>
### Replication Data Manually

If you want to ensure that changes to public folders replicate without having to wait for the normal replication interval, you can start replication manually.

**Important**

Manual replication only affects changes that should already have replicated at least once. Changes made after the last replication message was sent are not included.

Exchange provides two commands for this purpose:

**Send Hierarchy**

This command is available on the **Action** menu in Exchange System Manager for public folder trees, for individual public folders that have subfolders, or for public folder stores. This command replicates hierarchy changes (including changes in the tree structure or changes in folder properties).

**Send Contents**

This command is available on the **Action** menu in Exchange System Manager for individual public folders.

When you use these commands, Exchange prompts you to select one or more source and target servers, and to specify a range of changes to replicate. The range of changes to replicate starts the number of days in the past that you specify and ends at the last replication cycle. For example, you can replicate all changes made over the past two days, except for any changes made since the last replication cycle.

<table>
<thead>
<tr>
<th>Replication event</th>
<th>Default time-out</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication Short Backfill Request Timeout Retry</td>
<td>24 hours</td>
<td>The time-out value that is used when sending a backfill request when the data is available in the same Exchange site, and this request is a retry of a previous backfill request.</td>
</tr>
<tr>
<td>Replication Long Backfill Request Timeout Retry</td>
<td>48 hours</td>
<td>The time-out value that is used when sending a backfill request when the data is not available in the same Exchange site, and this request is a retry of a previous backfill request.</td>
</tr>
</tbody>
</table>
Special Considerations for Mixed-Mode Topologies

This section discusses connection agreements only in the context of public folders. For a detailed explanation of mixed-mode topologies (topologies that include both Exchange 2003 and Exchange 5.5 servers), including how to set up Active Directory Connector (ADC) and how to work with connection agreements, see "Migrating from Exchange Server 5.5" and "Upgrading Mixed Exchange 2000 Server and Exchange Server 5.5 Organizations" in the book Exchange Server 2003 Deployment Guide (www.microsoft.com/exchange/library).

The connection agreements that are maintained by Active Directory Connector synchronize user and group information, public folder information, and other configuration information between the Exchange 5.5 Directory and Active Directory. With this information in place, replication messages pass between Exchange 2003 servers and Exchange 5.5 servers in the same way that they do among Exchange 2003 servers.

**Note**
Exchange 5.5 servers can host replicas of folders from the Public Folders tree. They cannot host replicas of folders from general-purpose public folder trees.

Connection Agreements and Public Folder Replication

All three types of connection agreements—configuration connection agreements, user connection agreements, and public folder connection agreements—are important to public folder replication.

**Important**
Exchange 5.5 does not support general-purpose public folder trees. However, you can configure Exchange 5.5 servers to participate in the routing of replication messages for general-purpose trees. To do this, you must add entries to the Exchange 5.5 Directory for the general-purpose public folder stores, in a special container called Exchange 2003 Configuration Objects.

Configuration Connection Agreements

Configuration connection agreements (Config CAs) replicate site and administrative group configuration objects between Exchange 5.5 and Active Directory. They are created automatically by Exchange Setup. Tables E.5 and E.6 list important attributes that are handled by the Config CAs. These attributes play a part in replication of the Public Folders tree between Exchange 5.5 and Exchange 2003 servers.
Table E.5  Attributes that ADC replicates from the Exchange 5.5 Site-MDB-Config object to the Administrative Group object in Active Directory

<table>
<thead>
<tr>
<th>Exchange 5.5</th>
<th>Active Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-Folder-Guid</td>
<td>siteFolderGUID</td>
<td>Identification of the site folders for this site.</td>
</tr>
<tr>
<td>Site-Folder-Server</td>
<td>siteFolderServer</td>
<td>Name of the server that is responsible for hosting the site folders (normally the first server in the site or administrative group).</td>
</tr>
<tr>
<td>Folders-Container</td>
<td>msExchPfCreation</td>
<td>Location in which to create the public folder's directory entries in Exchange 5.5. If this attribute is not present, the Recipients container is used. In Exchange 2003, this attribute is read by the store on startup to determine what LegacyExchangeDN must be used by the store when a folder is created in Exchange 2003. Using this attribute, the public folder connection agreement will replicate the new folder back to the correct container in Exchange 5.5.</td>
</tr>
</tbody>
</table>

Table E.6  Attributes that ADC replicates from the Exchange 5.5 Microsoft Public MDB object to a Public Folder Store object in Active Directory

<table>
<thead>
<tr>
<th>Exchange 5.5</th>
<th>Active Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obj-Dist-Name</td>
<td>LegacyExchangeDN</td>
<td>Tracks the public folder store's Exchange 5.5-compatible name.</td>
</tr>
<tr>
<td>Email Addresses</td>
<td>proxyAddresses</td>
<td>Identifies the e-mail addresses for the public folder store.</td>
</tr>
<tr>
<td>Home-MTA</td>
<td>HomeMTA</td>
<td>Replicates the Home-MTA to Exchange 5.5, so that Exchange 5.5 can route replication messages to Exchange 2003.</td>
</tr>
</tbody>
</table>

As stated previously, Exchange 5.5 servers can route replication messages for general-purpose public folder trees. Table E.7 lists the attributes that make this function possible. These attributes are replicated from Active Directory to the Exchange 2003 Configuration Objects container in the Exchange 5.5 Directory.
Table E.7  Attributes that are replicated from Active Directory to the Exchange 2003 Configuration Objects container in Exchange 5.5

<table>
<thead>
<tr>
<th>Active Directory</th>
<th>Exchange 5.5</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LegacyExchangeDN</td>
<td>Modified Obj-Dist-Name</td>
<td>The LegacyExchangeDN attribute does not map directly to the Obj-Dist-Name attribute (otherwise the general-purpose public folder store object would be in the same container as public folder store objects for the Public Folders tree.) Instead, the object is placed in the Exchange 2003 Configuration Objects container.</td>
</tr>
<tr>
<td>LegacyExchangeDN</td>
<td>X.500 Pilgrim Address</td>
<td>Replicates to an additional X.500, or &quot;pilgrim&quot;, address.</td>
</tr>
<tr>
<td>HomeMTA</td>
<td>Home-MTA</td>
<td>Replicates a HomeMTA value to Exchange 5.5, so that Exchange 5.5 can route replication messages to Exchange 2003.</td>
</tr>
<tr>
<td>proxyAddresses</td>
<td>Email Addresses</td>
<td>Replicates the store's e-mail addresses to the store object in Exchange 5.5.</td>
</tr>
</tbody>
</table>

Important
If you need to be able to use an Exchange 5.5 Internet Mail Connector (IMC) to replicate information for a general-purpose public folder tree, you must configure an additional X.500 proxy address for the general-purpose store object in the Exchange 5.5 Directory. Use the Exchange 5.5 Obj-Dist-Name for the new proxy address.

User Connection Agreement
The user connection agreement replicates Exchange 5.5 mailboxes, custom recipients, and distribution lists to Active Directory users, contacts, and groups. Because these objects are used in public folder access control lists (ACLs), it is crucial that this information be replicated correctly.

Public Folder Connection Agreement
The public folder connection agreement replicates the public folder directory objects between Exchange 5.5 and Active Directory. In Exchange 5.5, all public folders have directory objects. In Exchange 2003, only mail-enabled public folders have directory objects. By default, in mixed mode, folders in the Public Folders tree are mail-enabled automatically.
Setting up public folder connection agreements can prevent future problems in the following ways:

- Folders that are created on Exchange 2003 cannot be administered from Exchange 5.5 if they do not have a directory entry in the Exchange 5.5 Directory. The Exchange 5.5 administrative program requires directory objects for all public folders.

- Folders created on Exchange 5.5 that do not have an object in Active Directory generate errors if you administer them using Exchange System Manager. The folder has properties stating that it is mail-enabled, so Exchange System Manager tries to find the directory object for that folder. The error can be cleared and the folder can still be administered, but you must deal with the error each time you work with the folder. Worse, an administrator may attempt again to mail-enable the folder and create a separate object for the folder in Active Directory. In such a case, if a public folder connection agreement is ever put in place, there will then be two directory objects for the same folder and e-mail sent to the folder will be returned as undeliverable.

- If folder objects are not replicated correctly, an administrator running DS/IS Consistency Adjuster on Exchange 5.5 can create folder objects in the Exchange 5.5 Directory that do not correspond to the folder objects in Active Directory. In such a case, if a public folder connection agreement is ever put in place, there will then be two directory objects for the same folder and e-mail that is sent to the folder will be returned as undeliverable.

- There may be a future need to e-mail a folder. If all of the Exchange 5.5 servers are removed by the time you need this functionality, there is nowhere to replicate the directory objects from anymore, so the folders have to be updated manually (or mail-enabled again by using a script).
Table E.8  Details of how public folder objects replicate between Active Directory and the Exchange 5.5 Directory

<table>
<thead>
<tr>
<th>Exchange 5.5 to Active Directory</th>
<th>Active Directory to Exchange 5.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for public folder objects in the Exchange 5.5 Directory, starting from the Site level. This means that all containers are searched for public folder objects, not just the Recipients container.</td>
<td>Search for public folder objects in the Microsoft Exchange System Objects container in Active Directory. This is the only Active Directory container that holds public folder objects.</td>
</tr>
<tr>
<td>Public folder objects replicate to the <strong>Microsoft Exchange System Objects</strong> container in Active Directory.</td>
<td>Public folder objects replicate into the Exchange 5.5 Directory container that is indicated by the LegacyExchangeDN value (set by the store when the folder is created, based on the value of msExchPfCreation). Unless another container is specified, the object will be placed in the Recipients container.</td>
</tr>
<tr>
<td>The Home-MTA and Home-MDB attributes are not replicated (they are meaningless to Exchange 2003).</td>
<td>The HomeMDB and targetAddress attributes are not replicated (they are meaningless to Exchange 5.5).</td>
</tr>
</tbody>
</table>
Avoiding Common Replication Problems in Mixed Mode

Many common problems with public folder replication in mixed mode can be traced back to two issues:

- Where an ACL on a public folder in Exchange 5.5 contains a distribution list, the ACL on a replica of the folder in Exchange 2003 must contain an Active Directory security group. The conversions of the Exchange 5.5 distribution list to an Active Directory distribution group and then to an Active Directory security group should be automatic if your topology is configured correctly. See "Types of Groups Used in Access Control Lists" later in this appendix.

- Where a public folder ACL contains a user, Exchange 2003 must be able to locate that user in Active Directory. When an ACL that has been replicated from Exchange 5.5 contains a user that no longer exists (or for some other reason Exchange 2003 cannot identify a matching user object in Active Directory), Exchange 2003 cannot process the ACL. Until the problem is resolved, only the folder owner is able to access the folder. See "Unknown Users in Access Control Lists" later in this appendix.

The rest of this section describes how to avoid these issues. For instructions about how to identify and resolve these problems when they occur, see "Problems with Permissions in a Mixed Exchange 5.5-Exchange 2003 Environment" in Appendix G, "Troubleshooting and Repairing Store Problems."

Types of Groups Used in Access Control Lists

Exchange 5.5 uses distribution lists for both message delivery and access control, whereas Exchange 2003 uses them only for message delivery. Exchange 2003 uses Active Directory security groups for access control. ADC replicates Exchange 5.5 distribution lists to Active Directory universal distribution groups (UDGs). When Exchange 2003 processes a public folder ACL and encounters a UDG, it immediately attempts to upgrade the UDG to a universal security group (USG). The USG then replaces the UDG in the ACL.

Important
The UDG must be in a Microsoft Windows® 2000 or Windows Server™ 2003 native mode domain to allow Exchange 2003 to upgrade it to a USG. In a mixed Exchange 2003/Exchange 5.5 environment, ADC displays a warning if you are replicating Exchange 5.5 distribution lists to a non-native-mode domain.
Exchange is not able to convert a UDG to a USG under the following circumstances:

- The UDG resides in a mixed-mode Microsoft Windows 2000 or Windows Server 2003 domain.
- A USG was converted manually to a UDG.
- The membership of the UDG has not been replicated to Active Directory.

**Important**

Avoid using UDGs as members of USGs. Exchange does not check to determine whether group members are groups that need converting. As a result, if a USG in an ACL has members that are UDGs, the UDGs are ignored and the ACL is not enforced correctly.

### Unknown Users in Access Control Lists

An unknown user (sometimes referred to as a zombie user) is a user that is listed in an ACL, but that does not have an account. The most common way that this situation arises is if, sometime while the topology was pure Exchange 5.5, an Exchange 5.5 user was deleted, but the user had been granted permissions on Exchange 5.5 public folders. At some later time, if the public folder replicates to Exchange 2003 with references to that user still in the ACL, Exchange 2003 cannot process the ACL because it cannot locate the user in Active Directory. Until the problem is resolved, only the folder owner will be able to access the folder. This protects the folder from access by users that may have been explicitly denied permissions on the folder. Exchange will also log a 9551 event when it has set folder permissions to "owner only." For more information about the 9551 event, and other events that may arise when you replicate information between Exchange 5.5 and Exchange 2003, see Appendix G, "Troubleshooting and Repairing Store Problems."

For detailed information about how Exchange converts ACLs when folders replicate from Exchange 5.5 to Exchange 2003, see "Anatomy of Object Level Access Control" in the Exchange technical article "Working with Store Permissions in Microsoft Exchange 2000 and 2003" ([http://go.microsoft.com/fwlink/?Linkid=18612](http://go.microsoft.com/fwlink/?LinkId=18612)). In particular, see the subsection "Special Considerations for Coexisting Exchange 2000 and Exchange 5.5 Servers." The information in this technical article applies to both Exchange 2000 and Exchange 2003.

The best way to avoid having unknown users is to run the Exchange 5.5 utility DS/IS Consistency Adjuster before you begin replicating public folders to Exchange 2003. This will clean unknown users from the ACLs.
In some circumstances, Exchange 2003 may deal with unknown users in different ways:

- If the folder has replicated from Exchange 5.5 before without problems but suddenly has an unknown user in the ACL, Exchange ignores the unknown user and processes the rest of the ACL normally. The assumption in this circumstance is that a user has been deleted in Exchange 5.5, or a new user was added in Exchange 5.5 and has not yet been replicated to Active Directory. The problem should rectify itself on the next ADC replication interval.

- If you have removed all of the Exchange 5.5 servers and switched Exchange 2003 to native mode, Exchange assumes that the user has been deleted and removes the unknown user from the ACL.

In some cases, you can set a registry key that tells Exchange to drop unknown users from the ACL while Exchange is in mixed mode. It is recommended that you only set this registry key when it is absolutely necessary (for example, if you have a small subset of unknown users, and they can all be safely eliminated from public folder ACLs). Otherwise, if the user was temporarily unknown because of a replication delay (as described in the first bullet point in the preceding list), you will have lost the permissions information for that user.

**Warning**
Dropping unknown users means that if those users have Access or Deny permissions on public folders, those permissions may be lost. It is not recommended that you drop unknown users on a long-term basis.

**Warning**
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

To temporarily ignore unknown users, on an Exchange 2003 server that holds public folder replicas, set the following registry key and then restart the Microsoft Exchange Information Store service:

```
HKLM\System\CurrentControlSet\Services\MSExchangeIS\Parameters\System\Ignore zombie users = <nonzero value>
```

This is a DWORD value. If the value is zero or if the key is not present, Exchange 2003 handles unknown users normally.

---

**Managing Inter-Organization Replication**

You can share public folder and free and busy information between two or more organizations in different Active Directory forests using the Inter-Organization Replication Tool. You can download the Inter-Organization Replication Tool from the Exchange Server 2003 Tools and
Update Web site (http://www.microsoft.com/exchange/2003/updates). The utility package contains two applications:

- Microsoft Exchange Server Replication Configuration utility (exscfg.exe)
- Microsoft Exchange Server Replication Service (exssrv.exe)

This package also contains documentation that describes how to set up inter-organizational replication. For more information about inter-organizational replication, see the book Exchange Server 2003 Deployment Guide (www.microsoft.com/exchange/library).

After you have configured the Exchange organizations, you can use this utility to coordinate meetings, appointments, and contact information between the members of the two organizations. As shown in Figure E.7, the inter-organizational replication process involves one Exchange server in each forest. One server acts as a publisher and sends information to the second server (the subscriber).

![Figure E.7 Using publisher and subscriber servers to replicate information between forests](image)

Figure E.7 Using publisher and subscriber servers to replicate information between forests
To configure the Inter-Organization Replication Tool, follow the instructions provided in the readme file that accompanies the tool. When you've finished the configuration process, you will have the following:

- At the first level of both the publishing public folder tree and the subscribing public folder tree, a public folder named `ExchsyncSecurityFolder`.
- For each first-level public folder in the publishing tree that you want to replicate, a corresponding target folder in the subscribing tree (subfolders in the subscribing tree will be created automatically).
- A mailbox-enabled account that has the following:
  - Local administrator rights on both the publisher server and the subscriber server.
  - Owner permission on both copies of `ExchsyncSecurityFolder`.
  - Owner permission on the folders to be replicated and the corresponding target folders.
- Session configuration settings for one Free and Busy replication session.
- Session configuration settings for one or more public folder replication sessions. If you need to tune your replication traffic, you can create public folder sessions that replicate at different times and at different intervals.
Using Full-Text Indexing

When you deploy full-text indexing, you select an individual public folder or mailbox store to be indexed. Users can then conduct full-text searches on the messages and attachments contained in the public folder or mailbox store. By default, the index contains the subject and body of a message, along with names of the sender and recipient and any names that appear in the Cc and Bcc fields. The index also includes text from the following types of attachments: .doc, .xls, .ppt, .html, .htm, .asp, .txt, and .eml (embedded Multipurpose Internet Mail Extensions (MIME) messages) files. Binary attachments, such as pictures and sounds, are not indexed.

Search results are only as accurate as the last time the index was updated. As the content of public folders or mailbox stores changes, the index must be updated to reflect the new content. Index updates can be performed manually or automatically on a schedule.

To work with full-text indexes, you must be at least an Exchange Administrator. To move files as described in this appendix, you must have read and write permissions on the appropriate drives and directories.

Verifying Recommended Hardware Configurations

Microsoft recommends the following hardware configurations for servers on which you deploy full-text indexes:

- Use a mirrored redundant array of independent disks (RAID) configuration. Microsoft recommends using a RAID 0+1 configuration (or RAID 1+0). RAID-5 is not recommended for full-text indexing.

- Make sure that the disk containing the index is large enough that it has 15 percent free disk space at all times. Depending on the types of files that you store, the size of your index can range from 10 percent to 30 percent of the size of your database.

- Add an additional 256 megabytes (MB) of RAM to the recommended configuration for a computer running Microsoft® Exchange Server 2003. Microsoft does not recommend running full-text indexing with less than 512 MB.
Preparing Your Exchange 2003 Organization

Before you configure full-text indexing, verify that your Exchange topology is configured and running correctly. If you change your Exchange organization after you configure full-text indexing, the index could require a full repopulation. In addition, verify the following:

- The Simple Mail Transfer Protocol (SMTP) address configuration is stable and functioning. This configuration affects the URL that is used to index objects.
- The server language is set correctly. To verify the language, open Control Panel, double-click **Regional Options**, and then check the language settings for the system. Full-text indexing references the server language that is specified in Control Panel when breaking words and stemming—a process that allows a search for "travel" to return "travels," "traveled," and "traveling." Full-text indexing works best when the query language of the client computer matches the language of the files that are being indexed. The server language is sometimes used for the query language when the client computer language is unknown, so it is best for the server language to match the language of most of the documents on the server.
- All servers are functioning properly, and connectivity throughout the organization is stable. Perform tests to ensure that all servers are configured correctly within the organization.

Deploying Full-Text Indexing

Use Exchange System Manager to deploy full-text indexing. Deployment involves the following tasks:

- Creating a full-text index
- Optimizing full-text indexing
- Performing a full population
- Setting a schedule for incremental populations
- Enabling full-text indexing queries
- Notifying users

Of these tasks, the most server-intensive is the full population process, which can take from a few minutes for a small database to several days for a large database. However, you can run the population process in the background during business hours without significant impact on system response time for users.
Creating a Full-Text Index

Before you can use full-text indexing, you must create an initial index (catalog) for each mailbox or public folder store that you want to index. This process will create the necessary file structure, which you will modify when you are optimizing the index.

To create an initial full-text index

1. In Exchange System Manager, right-click the mailbox store or the public folder store that you want to index, and then click Create Full-Text Index.
2. When a dialog box prompts you to select the location for the index, specify a place for the index on the RAID array.

Optimizing Full-Text Indexing

Use the following steps to optimize full-text indexing on your computer running Exchange 2003. As stated earlier, by distributing frequently accessed files across a RAID array, you can enhance system performance.

There are five major categories of full-text indexing files. By default, these files are installed on the system drive, which typically does not have the input/output (I/O) throughput of the RAID array. Arrange the disk locations of these files (as described in Table F.1) to optimize the performance of full-text indexing. In some cases, this appendix provides separate procedures for moving files in clustered topologies and unclustered topologies.

- **Catalogs** are the main indexes. There is only one catalog for each mailbox store or public folder store in Exchange.
- **Property store** is a database that contains various properties of items indexed in the catalog. There is only one property store per server.
- **Property store logs** are the log files associated with the property store database.
- **Temporary files** are the files that contain temporary information used by the Microsoft Search service.
- **Gather logs** are the log files that contain log information for the indexing service. One set of logs exists for each index.

This section refers to the following tools for moving files:

- **Pstoreutl**, located in Program Files\Common Files\System\MSSearch\Bin.
- **SetTempPath**, located in Program Files\Common Files\System\MSSearch\Bin.
- **Catutil**, located in Program Files\Common Files\System\MSSearch\Bin.
Table F.1  Recommended locations for full-text indexing files

<table>
<thead>
<tr>
<th>File type</th>
<th>Recommended location</th>
<th>How to specify the location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog</td>
<td>RAID array</td>
<td>Specify a location on the RAID array when you create the catalog using Exchange System Manager.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> If the index was already created elsewhere, use the Catutil tool to move it.</td>
</tr>
<tr>
<td>Property store</td>
<td>RAID array</td>
<td>Use the Pstoreutl tool.</td>
</tr>
<tr>
<td>Property store logs</td>
<td>RAID array in the same location as the property store</td>
<td>Use the Pstoreutl tool.</td>
</tr>
<tr>
<td>Temporary files</td>
<td>RAID array</td>
<td>Use the SetTempPath tool.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> On a cluster, place these files on a drive that will not fail over, such as a local drive or a drive on the RAID array or Storage Area Network that is configured to run only on a designated computer.</td>
</tr>
<tr>
<td>Gather logs</td>
<td>Leave in the default location, or move to any location you prefer.</td>
<td>Assign the location in the <strong>StreamLogsDirectory</strong> registry key.</td>
</tr>
</tbody>
</table>

**Warning**
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data. For information about how to restore the registry, view the “Restore the Registry” topic in the Registry Editor (Regedit.exe) Help or the Regedt32.exe Help.

To optimize full-text indexing

1. Move the property store and the property store logs.
2. Move the temporary directory.
3. Move the index (catalog).
4. Move the gather logs.
5. Increase the message size limit.
6. Set up checkpointing.

   The checkpointing feature was provided in Microsoft Exchange 2000 Server Service Pack 2 (SP2) and later to prevent possible indexing problems.

Each of these steps is explained in more detail in the following procedures.

### Moving the Property Store and the Property Store Logs

When the first index is created on your server, Exchange creates a new property store database on your Exchange system drive. To improve performance, move the property store database files to your RAID array. You need to move the property store and the property store logs only one time for each server, because all indexes on a server use the same property store.

**To move the property store in a non-clustered environment**

1. From a command prompt, use the Pstoreutl tool to move the database to the new drive (see the following example).

2. Restart the Microsoft Search service.

**Example** Your Exchange property store database is on drive C and your server name is 01. You want to move the property store to drive D. From a command prompt, run the Pstoreutl tool. Use the –m option to move the database to the specified location and the –l option to change the directory for log files. Enter the following command on the same line; it is shown on separate lines for readability:

```
pstoreutl.exe ExchangeServer_01 –m d:\exchsrvr\ExchangeServer_01\ExchangeServer_myserver.edb –l d:\exchsrvr\ExchangeServer_01
```

**To move the property store in a clustered environment**

1. Leave the Microsoft Search service running in Control Panel. Use Cluster Administrator to take the MSSearch resource (the cluster resource for the Microsoft Search service) offline.

2. Use the Pstoreutl tool to move the database to the new drive.

   The Exchange data directories are located on the shared disk that you specified when you created the Exchange virtual server.

3. Use Cluster Administrator to bring the MSSearch resource online.
Moving the Temporary Directory

By default, the gather and filter temporary files (also known as temp files) are located on the Exchange system drive, which typically does not have the I/O throughput of the RAID array. Use the SetTempPath tool to move the temporary directory to the RAID array. You need to move this directory only one time for each server, because all indexes on a server use the same temporary directory.

To move the Microsoft Search service temporary directory

1. From a command prompt, run the SetTempPath tool. (For syntax, see the following example.)
2. Stop and then restart the Microsoft Search service.

Example Enter the following command on the same line; it is shown on separate lines for readability:

```
cscript "c:\Program Files\Common Files\System\MSSearch\Bin\settemppath.vbs"
d:\temp
```

You can view the current location of the temporary directory at any time by running the preceding SetTempPath script with no parameters.

Note

On a cluster, the full-text index temporary directory must be located on a drive that will not fail over. Make sure that you place the temporary directory on a local drive, or on a drive on the RAID array or Storage Area Network that is configured to run only on a designated computer.
Moving the Index (Catalog)

The index should be located on the RAID array. If you did not specify this location when you created the index, use the Catutil tool to move it.

To move an index

1. Pause any active full- or incremental-index population processes.
2. From a command prompt, run the Catutil tool.

Note
For help using the Catutil tool, go to the command prompt and type `catutil movecat /?`.

Important
When you use the Catutil tool, the index moves successfully and functions correctly, but the index location that is displayed in Exchange System Manager is not updated. This does not affect the normal operation of full-text indexing. You cannot correct the display, but you can check the current location of the index at any time by viewing the following key in the registry:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Search\1.0\Indexer\<application name>\<index name>\ProjectPath
```

Moving the Gather Logs

As mentioned previously, the gather logs are created on the Exchange system drive, which typically does not have the I/O throughput of the RAID array. You can choose to leave the gather logs in the default location, or you can specify a location on a higher-performance drive by editing the `StreamLogsDirectory` registry key. Be sure that you specify a valid directory, because full-text indexing does not function if you specify an invalid directory. The Microsoft Search service does not need to be running when you edit the registry key. However, if you edit the registry key while the Microsoft Search service is running, you must restart the service after you make the change for the change to take effect.

Warning
Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.
To move the gather logs

1. Start Registry Editor.
2. In the Registry Editor, specify the preferred location for gather logs using the following registry key:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Search\1.0\gather\ExchangeServer_<instance>\<index name>\StreamLogsDirectory

   **Note**
   On a cluster, before you change the StreamLogsDirectory registry key, make sure that the MSSearch resource is online. Also, make sure that you are editing the correct node by using Cluster Administrator to verify the node on which the group is running. After you change the registry key, use Cluster Administrator to restart the MSSearch resource by taking it offline, and then bringing it back online.

Increasing the Message Size Limit

By default, the index includes messages (including attachments) that are 16 MB or less in size. Therefore, messages with large attachments may be excluded from the index and from the search results of users. To avoid performance problems, Microsoft recommends that you increase this limit to the maximum setting of 4000 MB so that larger messages and attachments are indexed.

The Microsoft Search service does not need to be running when you edit the registry key. However, if you edit the registry key while the Microsoft Search service is running, you must stop and restart the service after you make the change for it to take effect.

To increase the message size limit

1. Start Registry Editor.
2. In Registry Editor, set the following registry key to 4000 MB:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Search\1.0\Gathering Manager\MaxDownloadSize

   **Note**
   On a cluster, before you change the MaxDownloadSize registry key, make sure the MSSearch resource is online. Also, make sure you are editing the correct node by using Cluster Administrator to verify the node on which the group is running. After you change the registry key, use Cluster Administrator to restart the MSSearch resource by taking it offline, and then bringing it back online.
Setting Up Checkpointing

It is strongly recommended that you use the checkpointing script provided with Microsoft Exchange 2000 Server SP2 to prevent possible indexing problems. If the Microsoft Search service terminates abnormally during an incremental population of the index, some folders and messages may not be indexed properly. (An incremental population is a process that updates an existing index with data that has changed since the previous population.) Checkpointing remedies this problem by maintaining the following backup files in the catalog directory:

- Two checkpoint record files: <catalog>.chk1.gthr and <catalog>.chk2.gthr.
- Approximately 13 files consisting of the last known complete and uncorrupted set of catalog files stored in a Save subdirectory.

Checkpointing is not turned on by default because it requires a significant amount of additional disk space. The additional file size is approximately 200 bytes for each document in your database. For example, 5,000,000 messages or documents in your database generate checkpointing files totaling 1 gigabyte (GB). The size of these files grows as the number of documents in your database grows. You should ensure that there is sufficient disk space before you run the checkpointing script. It is recommended that at least 15 percent free disk space is available on the disk on which you keep full-text indexing catalogs.

To set up checkpointing

1. Ensure that there is sufficient disk space. If necessary, increase the size of the volume or move the catalogs to a larger volume.
2. From a command prompt, run the following script:

   `<SystemDrive>:\Program Files\Common Files\System\MSSearch\Bin\EnableCheckPoints.vbs <APPLICATION> [CATALOG]`

Parameter Definitions

 `<APPLICATION>`
This is the name of the full-text indexing application. The naming convention for the application is ExchangeServer_<ServerName>. In a stand-alone configuration, <ServerName> is the name of the server. In a clustered environment, <ServerName> is the name of the virtual server.

 `[CATALOG]`
This parameter refers to the name of the full-text indexing catalog. To find the name of the catalog in Exchange System Manager, double-click the Exchange store for which a full-text index was created, and then double-click Full-Text Indexing. The property is labeled "Index Name" and the value of the property is the name of the catalog.
Usage

- To see information about how to use the script, run the script with no parameters.

- Specifying just the name of the full-text indexing application will enable checkpointing for the entire application. This means that all full-text indexes created from this point on will inherit the property automatically. If you have existing full-text indexes, you will have to enable checkpointing on them one at a time by specifying the name of the catalog as a parameter to the script.

- Specifying both the name of the full-text indexing application and catalog will enable checkpointing for that particular full-text index and no others. This has no effect on future creation of full-text indexes.

  **Note**
  The only way to disable checkpointing on a full-text index (catalog) is to delete it and then re-create it.

Examples

- Set up checkpointing on the server TUNIS01 for all new catalogs:

  ```
  D:\Program Files\Common Files\System\MSSearch\Bin\EnableCheckPoints.vbs ExchangeServer_TUNIS01
  ```

- Enable checkpointing for an existing catalog on a mailbox store:

  ```
  D:\Program Files\Common Files\System\MSSearch\Bin\EnableCheckPoints.vbs ExchangeServer_TUNIS01 privE34F12BB
  ```

Performing a Full Population

After you create the index, you must run a full population (also called a crawl) to fill the index with data. The resource usage setting for full-text indexing is located on the Full-Text Indexing tab of the server's Properties dialog box. By default, it is set to Low. It is recommended that you use the default setting. A higher setting yields little benefit and could slow down user access to the Exchange server.

With a resource usage setting of Low, the population process runs in the background and can be performed during business hours. Population process threads use idle processing time. User activities receive priority on the system. Because full-text indexing uses only cycles that would otherwise be idle, it should not significantly slow down user access to the server. Expect CPU usage to approach 100 percent as a normal effect of the population process.

  **Note**
  If you are experiencing performance issues with the Exchange server while the Microsoft Search service is performing a full or incremental population, you can drop the resource usage to Minimum. By setting the resource usage to Minimum, you further reduce the amount of resources the Microsoft Search service can use. Therefore, full or incremental populations take longer to complete, but there will not be any data loss.
To start a full population

1. Make sure full-text searches are unavailable during full population. Otherwise, users will assume that they can conduct full-text searches, but their searches will not return the expected results. To make full-text searches unavailable:
   a. In Exchange System Manager, right-click the mailbox store or public folder store that you want to index, and then click Properties.
   b. Click Full-Text Indexing, and then clear the This index is currently available for searching by clients check box.

2. In Exchange System Manager, right-click the mailbox store or public folder store that you want to index, and then click Start Full Population.

The initial full population can take a long time. With a typical Exchange Server 2003 configuration, population performance typically ranges from 10 to 20 messages per second. Performance varies based on the hardware configuration, the type and size of messages, and the server resources that are available. As a result, the total time required for a full population can range from a few minutes for a small database, to several days for a large database. The content language of documents on your server also affects the time the population takes. For example, populating an index on a server that contains documents written mostly in East Asian languages can take more than five times longer than for a server containing documents that are written in Western European languages. Folders containing Internet newsfeeds can also significantly lengthen population time if the folders contain messages in uuencode format.

To view the status of the population process

- In Exchange System Manager, expand the public folder or mailbox store, and click Full-Text Indexing.

  During the initial population, the status is Crawling. You can determine that the population has finished by looking at this status or by looking in Event Viewer for Microsoft Search service messages.

  **Note**
  
  Do not stop a full population while it is in progress. If you must stop a full population, but intend to rerun it at another time, choose Pause Population instead of Stop Population.

To pause a full population

1. In Exchange System Manager, right-click the mailbox store or public folder store that you want to pause.

2. Click Pause Population.
Setting a Schedule for Incremental Populations

Determine how often you want to run an incremental population to update the index. Because an incremental population runs in the background the same way a full population does, frequent updates do not significantly affect system response time for users. Although you should schedule incremental population to occur at least once daily, you may want to schedule more frequent updates, because the index is only as current as the last time it was populated. You should also consider the amount of time it takes to complete an incremental population. For example, a typical schedule sets incremental updates at the beginning of each hour. However, if the update lasts more than an hour, the next incremental population begins at the start of the following hour.

The schedule for the incremental population only determines when the population process can begin. It does not place a time limit on the population process. Therefore, it is possible that an incremental population will continue to completion outside of the scheduled time.

**Tip**

Generally, if the mailbox store or public folder store is 6 GB or smaller, you can perform incremental updates hourly. If the store is larger than 6 GB, or the server has high memory usage, you may want to update the index less frequently.
To set the incremental population schedule

1. In Exchange System Manager, right-click the mailbox or public folder store that you want to index, click Properties, and then click the Full-Text Indexing tab (see Figure F.1).

![Figure F.1 The Full-Text Indexing tab for a mailbox store](image)

2. In the Update Interval list, select an interval schedule.
Enabling Full-Text Indexing Queries

After the initial population and at least one incremental population are complete, enable the use of the index so that users can begin conducting full-text searches against the index.

To enable the use of the index

1. In Exchange System Manager, right-click the mailbox store or public folder store that you want to enable, and then click Properties.
2. Click Full-Text Indexing, and then select the **This index is currently available for searching by clients** check box.

Notifying and Educating Users

After you have enabled queries (as described earlier), notify users that the indexes are available for searching, and educate them about what they can expect when they run full-text index searches. For example, to notify users, you can send out an e-mail announcement to your users.

Managing Full-Text Indexing

Use the following information to help you manage full-text indexing after deployment. Included are guidelines for determining when to repopulate the index to keep the information current.

Checking the Size of the Index

You can check the size of the index file in the following folder:

```
<driveletter>:\Exchsrvr\ExchangeServer_<servername>\Projects\<indexname>\Build\Indexer\CiFiles
```

Adding Users to an Indexed Server

When you add users to an indexed server, perform an incremental population to add the new mailbox to the index immediately.
Deciding When a New Full Population Is Required
You must fully populate the index in the following cases:

- When a word-breaker is changed. (A word-breaker is used by full-text indexing to identify where individual words begin and end in a given text.)
- When new document format filters are added.
- When the schema file is changed.
- When the SMTP address of the store changes.
- When performing disaster recovery.

During the population process, the index is still available for full-text queries. The index is unavailable for queries only when you must delete an old index, before you re-create it and perform a new full population. This process should be necessary only if the old index is corrupted.
APPENDIX G

Troubleshooting and Repairing Store Problems

This appendix has four main parts:

- Problems with Full-Text Indexing
- Problems with Permissions in a Mixed Exchange 5.5-Exchange 2003 Environment
- Problems with Public Folder Replication
- Other Problems

Problems with Full-Text Indexing

This section contains information about how to resolve problems that you may encounter with full-text indexing. It contains the following topics:

- Safe Event Viewer Messages
- Population Process Is Slow
- Population Process Is Found in a Paused State
- Deleted Message Is Still Visible in Search Results
- Wrong Location Is Displayed After Moving the Index
- Using Gather Log Entries to Identify Problems
- Language Settings Problems
- Queries Fail During Server Startup
- Restoring Missing Performance Counters
- Avoiding Disk Bottlenecks
- High Paging

If you encounter problems with full-text indexing, Event Viewer and Performance Logs and Alerts are useful troubleshooting tools.
Safe Event Viewer Messages

Although Event Viewer is useful for troubleshooting full-text indexing problems, there are certain events (as described in the following sections) that do not necessarily indicate problems.

Event ID 7000: The Indexer Started Successfully

After you use Exchange System Manager to stop an index population, the Microsoft® Search service may incorrectly log several copies of the following event message in the Event Viewer application event log:

```
Event Type: Information
Event Source: Microsoft Search
Event Category: Indexer
Event ID: 7000
Date: date
Time: time
User: N/A
Computer: server_name
Description:
The Indexer started successfully for project <ExchangeServer_SERVERNAME priv78F2DC76>
```

This message does not indicate a problem, and you can ignore it.

Event ID 10006: Catastrophic Failure (Cluster Environment)

When you shut down the Microsoft Search service in a clustered environment, you may see the following error:

```
Event Type: Error
Event Source: Microsoft Search
Event Category: Gatherer
Event ID: 10006
Date: 2/11/2000
Time: 9:44:25 AM
User: N/A
Computer: <servername>
Description:
An error occurred during the online operation for instance <your instance>: 8000ffff - Catastrophic failure
```
This error is not actually a catastrophic failure. Wait for all services to shut down successfully, and then restart services, if necessary. To prevent this error from occurring, use Cluster Administrator to stop clustered resources, not the Services application in Control Panel. When you stop the service using Services in Control Panel, the cluster resource manager assumes that the resource failed, and it either attempts to restart the service or fails over the group.

SMTP and System Attendant Logged as Errors

When the Microsoft Search service is running, you may receive error messages similar to the following in the gather logs:

```
2b3b1b8 1bed2fc
file:\.\BackOfficeStorage\server.microsoft.com\MBX\SMTP
(SERVER-{E2E63C70-4129-43F6-9363-6B501433C952}) 8000000c 0
80800005
```

```
2cdeb96 1bed2fc
file:\.\BackOfficeStorage\server.extest.microsoft.com\MBX\System Attendant
8000000c 0 80800005
```

You can ignore these error messages. For more information about the gather logs, see "Using Gather Log Entries to Identify Problems" later in this appendix.

Population Process Is Slow

If the population process is slow, Internet newsfeeds may be the cause. Internet newsfeeds may contain uuencoded binaries, which are indexed at a much slower rate than normal messages. When you run a population on a public folder that contains Internet newsfeeds, population time lengthens significantly.

Messages with large attachments may also cause performance problems if you have not optimized the maximum download size. The recommended setting is 4,000 megabytes (MB). Changing this setting requires editing the registry.

**Warning**

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

For information about how to edit the registry, see "Change Keys and Values" in the Registry Editor (Regedit.exe) Help, or "Add and Delete Information in the Registry" and "Edit Registry Information" in the Regedt32.exe Help. If you are running Microsoft Windows NT® or Microsoft Windows® 2000, you should also update your Emergency Repair Disk (ERD).
To change the maximum download size

1. Start Registry Editor.
2. In Registry Editor, set the following DWORD registry key to 4000 MB:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Search\1.0\GatheringManager\MaxDownloadSize
```

For more information about the setting the download size, see "Optimizing Full-Text Indexing" in Appendix F, "Using Full-Text Indexing."

---

**Population Process Is Found in a Paused State**

The Microsoft Search service pauses a population process if it cannot continue. To verify whether the Microsoft Search service, rather than an administrator, paused the population, check the event log. The Microsoft Search service logs an event when it must pause or stop the population. For example, the Microsoft Search service pauses a population if the disks are too full to add new information to the indexes or the log files. Usually, you can fix the problem (for example, by freeing space on a full drive), and resume the population. New documents added during the pause are not added to the index until the next population.

**Note**

Lack of space on the disk is often the problem, even when it appears that there is plenty of free disk space. The Microsoft Search service uses disk space liberally to temporarily unpack large sections of the index to merge new results before recompressing.

---

**Deleted Message Is Still Visible in Search Results**

You can delete a message from a search results folder. The message is deleted, but the message remains visible in the search result window until you refresh the search.

---

**Wrong Location Is Displayed After Moving the Index**

If you use the Catutil tool to move the index, as described in Appendix F, "Using Full-Text Indexing," the index location displayed in Exchange System Manager is not updated. The index is moved successfully and functions correctly, but Exchange System Manager incorrectly displays the original location of the index. This is only a display error and does not affect the normal operation of full-text indexing. You cannot correct the display, but you can check the current location of the index at any time by checking the registry.
To check the current location of the index after using Catutil

- In Registry Editor, view the following registry key:

```
HKEY_LOCAL_MACHINE \Software\Microsoft\Search\1.0\Indexer\<application name>\<index name>\ProjectPath.
```

Using Gather Log Entries to Identify Problems

Gather log files are generated during a population. These files contain log information for the Microsoft Search service. The files are located in the Program Files\Exchsrvr\ExchangeServer_<servername>\GatherLogs directory. The files have a .gthr extension.

If a particular document fails to be indexed for any reason, an entry is logged in the gather log file. Each entry lists the file name and the error number. To decode this error number, use the Gthrlog tool found in the Program Files\Common Files\System\MSSearch\Bin directory.

To use the Gthrlog tool to decode an error number from the gather log file

- From the command prompt, type the following command, where `<filename>` is the name of the .gthr file:

```
cscript gthrlog.vbs <filename>
```

Results from the tool are displayed at the command prompt.

Language Settings Problems

The language settings of individual messages, attachments, the server, and the client computer affect indexing behaviors. This section provides guidelines for these behaviors and scenarios that illustrate the results of mixed language settings.

Full-Text Indexing Guidelines for Mixed Language Settings

The guidelines that govern full-text indexing in mixed-language scenarios are complex. The following topics explain how various language settings affect indexing behaviors. Administrators can use this information to help determine the cause of user-reported search problems.
Language Setting of Individual Messages

The language setting of individual messages affects indexing behavior in the following ways:

- If a message is a MAPI message, it has a **Locale ID** property, and full-text indexing uses this value to determine which word-breaker (identifies where individual words begin and end in a given text) to use. This property value comes from the Language setting in Microsoft Office on the client computer. If full-text indexing cannot find a word-breaker to match the **Locale ID** property, it uses the **Neutral <0>** property. For more information about how full-text indexing uses word-breakers, see Appendix F, "Using Full-Text Indexing."

- If a message is created with Distributed Authoring and Versioning (DAV), it uses the "Accept-Language" header to determine the correct locale.

- If a message has no locale identified (which is often the case with messages from the Internet), the **System Locale** setting of the computer running Microsoft Exchange Server 2003 where full-text indexing is performed is used to determine the word-breaker.

Language Setting of Attachments

The language setting of an attachment affects indexing behavior in the following way:

- If an attachment is a Microsoft Office document, full-text indexing uses the language setting that was used to generate the document.

Language Setting of the Server Running Microsoft Windows Server 2003 or Windows 2000 Server

The language setting of the server affects indexing behavior in the following way:

- If the message is non-MAPI (in other words, from the Internet), its **Locale ID** property is not set, and full-text indexing uses the **System Locale** setting of the server to determine which word-breaker to use.

Language Setting of the Client Computer

The language setting of the client computer affects indexing behavior in the following way:

- When a query is sent from Microsoft Office Outlook®, the **Locale ID** of the client computer is also sent. If the **Locale ID** of the message does not match the **Locale ID** of the query, the search results are unpredictable.

**Note**
The language of the computer running Exchange Server is irrelevant in this scenario. The client computer setting takes priority.
Full-Text Indexing Behavior in Mixed-Language Scenarios

The following scenarios describe query behavior of content indexing with various language settings.

All U.S. Language Settings

If you use U.S. language settings in Outlook, running on a client computer with U.S. language settings, to compose and submit a message to Exchange 2003, running on a server running Windows Server 2003 or Windows 2000 Server with U.S. language settings, the following process occurs:

1. Full-text indexing indexes the message using the U.S. language setting word-breaker.
2. Queries from the client computer with U.S. language settings are processed as expected.


In this example, the client computer is configured as follows:

- The client computer has Hebrew language settings.
- Office has U.S. language settings.
- Outlook has Hebrew language settings.

If you compose a message on the client computer described in this example and submit the message to Exchange 2003 with the System Locale setting set to U.S., the following process occurs:

1. Full-text indexing uses the U.S. word-breaker to index the message. The Locale ID property of the message defaults to U.S. because of the Office settings.
2. Queries from the Hebrew client computer fail because the Hebrew document does not have the proper word-breaker applied.


In this example, the client computer is configured as follows:

- The client computer has Japanese language settings.
- Office has Japanese language settings.
- Outlook has Japanese language settings.
If you compose a message on the client computer described in this example and submit the message to Exchange 2003 with the **System Locale** setting set to **U.S.**, the following process occurs:

1. Full-text indexing uses the Japanese word-breaker to index the message.
2. Queries from the Japanese client computer succeed because the message was indexed and queried with the same **Locale ID** property.

### Queries Fail During Server Startup

During initialization, in the first few minutes after starting a computer running Exchange Server with full-text indexing, users might receive their mail but not receive results from queries. This failure to receive query results occurs because the Microsoft Search service is loading the index, and Exchange is loading the property store. Queries do not return results until these processes are complete.

### Restoring Missing Performance Counters

Event messages similar to the following indicate that the counters used by the Performance Logs and Alerts service and the Performance application (also called System Monitor) are missing. If you receive one of these messages, restore the counters by restarting the Microsoft Search service. For more information about these monitoring applications, see the Windows Resource Kit.

<table>
<thead>
<tr>
<th>Performance monitoring for the Gatherer service cannot be initialized because the counters are not loaded or the shared memory object cannot be opened. This only affects availability of the performance counters. Rebooting the system may fix the problem.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance monitoring cannot be initialized for the Gatherer object because the counters are not loaded or the shared memory object cannot be opened. This only affects availability of the performance counters. Rebooting the system may fix the problem.</td>
</tr>
<tr>
<td>Performance monitoring for the Indexer object cannot be initialized because the counters are not loaded or the shared memory object cannot be opened. Stop and restart the Search service. If this error continues, reinstall the application.</td>
</tr>
</tbody>
</table>
Avoiding Disk Bottlenecks

To avoid disk read and write bottlenecks, use the following guidelines:

- Disk queue length should be monitored.
- The queue length is expected to average more than the number of spindles in the redundant array of independent disks (RAID) array.
- The length should drop to zero occasionally.
- The queue should be empty occasionally. Having something always in the queue indicates a problem.
- The average time per disk write and per disk read should be close to the expected latency. The system should take roughly 10 milliseconds for a disk write or read. If the configuration has a hardware cache or a RAID controller, the time could be even less.

High Paging

High memory-to-disk paging can indicate a memory bottleneck. Check your performance counters and monitor them for warning signs. In particular, check the Memory: Page writes/sec and Memory: Page reads/sec counters.

Problems with Permissions in a Mixed Exchange 5.5-Exchange 2003 Environment

A user's inability to see public folders in Outlook is often the first sign of a permissions problem. This section describes ways that you can determine whether the problem is caused by permissions replication, and how you can track the source of the problem.
Determine What is Preventing a User from Seeing the Public Folder in Outlook

Determine which of the following situations is preventing a user from seeing the public folder in Outlook:

- The public folder was not replicated to the server.
- The public folder permissions were not converted successfully.

The best way to determine the cause of the problem is to view the folder tree in Exchange System Manager. If the public folder appears in the tree when Exchange System Manager is connected to a particular public folder store, but a user with a mailbox on the same server as the public folder store cannot see the public folder, the problem has to do with permissions, not replication. However, if the public folder does not exist in the tree, you may have a replication problem.

View Access Control Lists in Exchange System Manager

In mixed-mode environments where permissions in access control lists (ACLs) were not successfully converted to ptagNTSD data, users may not be able to access the folder, even though the permissions appear to be correct in Exchange System Manager. For more information about the conversion process and the properties involved, see "Working with Permissions for Public Folders and Mailboxes" in Chapter 7, "Managing Mailbox Stores and Public Folder Stores."

When you use Exchange System Manager to view the permissions for a public folder in the default Public Folders tree (also called the MAPI tree), Exchange System Manager displays the permissions that are contained in the ptagACLData property (if one exists) rather than recalculating the permissions from the ptagNTsd property. In other words, Exchange System Manager displays permissions from the "replicated in" property (which Exchange normally discards) rather than the permissions that are calculated from the ptagNTSD property, which actually control access to the folder. Use the following procedure to view the ptagNTSD permissions.
To view the ptagNTSD permissions on a folder in Exchange System Manager

1. In Exchange System Manager, in the console tree, right-click the public folder for which you want to view the properties, and then click Properties.

2. Click the Permissions tab in the public folder's properties.

3. To display the ptagNTSD ACL data, which controls access to the folder, hold down the CTRL key and click Client Permissions, and then click Advanced.

   **Important**
   Do not set permissions in Exchange System Manager while viewing the ptagNTSD permissions. If you change permissions while they are displayed in this format, you will no longer be able to set permissions using MAPI tools.

   **Note**
   When you use Exchange System Manager to view permissions for general-purpose (non-MAPI) public folders, Exchange System Manager always displays the ptagNTSD permissions.

Monitor Permissions Events in Event Viewer

You can use diagnostic logging to record permissions events to the application event log in Event Viewer. By default, the public folder logging level is set to None, which logs only critical errors.

You can use the Diagnostics Logging tab in the Properties of a server running Exchange 2003 to increase the logging level on a public folder. This increased logging level allows you to obtain more detailed permissions information.

To view the attempts of individual users to access folders and show the permissions that are granted to users when they try to access folders, set the Logons and Access Control diagnostics to maximum.

To set the Logons and Access Control diagnostics to maximum

1. In Exchange System Manager, double-click Servers, right-click a server, and then click Properties.

2. Click the Diagnostics Logging tab.

3. Under Services, double-click MSExchangeIS, and then click Public Folder.


For more information about diagnostics logging, see "Use Diagnostic Logging and Event Viewer" in the Exchange Server 2003 Help.
Event ID 9548: Disabled user <user> does not have a master account SID

When users other than folder owners are not able to access a folder, look for events 9548 and 9551 in the application event log. (Event 9551 is discussed in the following section.)

<table>
<thead>
<tr>
<th>Event ID: 9548</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date: 2/11/2000</td>
</tr>
<tr>
<td>Time: 9:44:25 AM</td>
</tr>
<tr>
<td>User: &lt;user&gt;</td>
</tr>
<tr>
<td>Computer: &lt;servername&gt;</td>
</tr>
<tr>
<td>Description:</td>
</tr>
<tr>
<td>disabled user &lt;user&gt; does not have a master account SID. Please use Active Directory MMC to set an active account as this user's master account.</td>
</tr>
</tbody>
</table>

If you view the client permissions for the folder using Exchange System Manager, initially they look correct. However, viewing the permissions using the Advanced dialog box (these are the raw permissions that are stored in the ptagNTSD property) reveals that only the owner has been converted successfully from the Microsoft Exchange Server 5.5 version of the permissions to the Exchange 2003 version.

There are two potential causes for this problem:

- The Microsoft Active Directory® directory service does not have a trust set up to the Microsoft Windows NT® version 4.0 domain that holds the user's account.
- The user has been disabled manually and does not have an external account.

You should be able to fix the problem using the following approaches:

- Remove the disabled accounts from the ACL.
- Give the disabled accounts associated external accounts.
- Create a trust between the Windows NT 4.0 (or external Windows) domain and Active Directory. This trust gives the disabled accounts associated external accounts (and master account security identifiers (SIDs)).
Event ID 9551: An error occurred while upgrading the ACL on folder `<folder>` located on database `<database>`

When users other than folder owners are not able to access a folder, look for events 9548 and 9551 in the application event log (event 9548 is discussed in the previous section). When event 9551 occurs, it is logged each time a user attempts to access the folder.

---

**Note**

If the folder has been replicated from an Exchange 5.5 server to the Exchange 2003 server, the ACL shows the name in uppercase letters because distinguished names are always uppercase. However, remember that to view permissions, Exchange System Manager connects to a store that holds an actual content replica of the folder. If Exchange System Manager connects to an Exchange 5.5 server, the ACL appears to be correct. Do not be misled by the appearance of the ACL. If the store is logging 9551 events, the cause of these events must be fixed before Exchange 2003 users can access the folder.

There are three potential causes for upgrade problems:

- No user connection agreement is in place to replicate the Exchange 5.5 mailboxes into Active Directory.
- The user has been deleted from Active Directory.
- There is replication latency.

When Exchange 2003 receives the replication message, Exchange will attempt to upgrade the data stored in `ptagACLData` to Windows NT SIDs. If the upgrade process fails, only owners are stored in `ptagNTSD`. No one else will be able to access the folder.
You should be able to fix the problem using the following approaches:

- Remove the bad entry.
- Replicate the missing user to Active Directory.

**Event IDs 9552 or 9556: Cannot Convert Distribution List to Security Group**

When users that belong to a specific distribution list or group cannot access a folder, look for events 9552 or 9556 in the application event log. Following are the event descriptions for Events 9552 and 9556:

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9552</td>
<td>While processing public folder replication, moving user, or copying folders on database &lt;database&gt;, DL &lt;distribution list&gt; could not be converted to a security group. Please grant or deny permissions to this DL on Folder &lt;folder&gt; again. This most likely is because your system is in a mixed domain.</td>
</tr>
<tr>
<td>9556</td>
<td>Unable to set permission for DL &lt;distribution list&gt; because it could not be converted to a security group. This most likely is because your system is in a mixed domain.</td>
</tr>
</tbody>
</table>

In addition, Outlook users that attempt to set permissions involving users that do not have access may see the following error:

- The modified permissions could not be saved. The client operation failed.

Administrators using Exchange System Manager who attempt to set permissions involving users that do not have access may see the following error:

- The operation failed. ID no 8004005 Exchange System Manager.

The most likely cause for these errors is that the Exchange 5.5 distribution list to which the users belong was replicated into an Active Directory mixed-mode domain rather than into an Active Directory native-mode domain. As a result, the universal distribution group that corresponds to the distribution list was created in an Active Directory mixed-mode domain. The domain into which groups are replicated is configured in the user connection agreement that governs the migration of Exchange 5.5 distribution lists to Active Directory.

To be used in setting permissions, the universal distribution group must be converted to a universal security group. This conversion can only take place if the universal distribution group has been created in a native-mode domain. For more information about this conversion process, see "Working with Permissions for Public Folders and Mailboxes" in Chapter 7, "Managing Mailbox Stores and Public Folder Stores."
To fix the conversion problem, do the following:

1. Create a native-mode domain in Active Directory.
2. Configure the user connection agreement to use the new domain for groups that it migrates from Exchange 5.5.

---

**Problems with Public Folder Replication**

If you think there is a problem with folder replication (especially replication of the hierarchy), use Exchange System Manager to check whether folders have replicated. Do not rely on the view provided by Outlook to determine whether folders have replicated. The problem might relate to permissions, not replication.

To help identify replication issues, set diagnostic logging to **Maximum** for the **MSExchangeIS: Public Folder** categories **Replication Incoming**, **Replication Outgoing**, and **Non-delivery Reports**.

If replication messages are not being sent or received, check that normal e-mail routing between the servers works.

---

**Replication Messages Not Being Received**

This problem could have one of the following causes, each of which has its own solutions:

- Public folder stores do not have e-mail addresses.
  - Check that the Recipient Update Service has stamped the mail attributes onto the public folder store's directory objects correctly.
  - In mixed Exchange 5.5/Exchange 2003 organizations, check that Exchange 5.5 can access the directory entries for the Exchange 2003 public folder stores, and that Exchange 2003 can access the directory entries for the Exchange 5.5 public folder stores.
- There is no route for mail to follow.
  - Check that normal mail traffic can flow between the servers.
  - If the replication message goes over an Exchange 5.5 Internet Mail Connector (IMC), check that the **ResolveP2** registry key is set to \-1\. This registry key is located at:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeTransport\Parameters\<VSID>
```

Check also that the Exchange 5.5 Public Information Store object exists in the Active Directory **Configuration** container and has a valid X.400 proxy address (you can use ADSI Edit or the LDP utility to check attribute values).
Transport links are restricted to disallow system messages.

- Check that there is a route for system messages between the servers. Winroute.exe indicates whether there are restrictions on the links.

**Backfill Takes a Long Time**

The backfill can take a long time when a new server is installed and the initial status request gets lost or goes to a server that also has no knowledge of the hierarchy. To remedy this, make a change to the hierarchy on another server and check that it replicates through correctly. The server should backfill within 24 to 48 hours.

**Server Does Not Appear to Backfill**

If a server does not appear to be backfilling, check whether new folders that have been added to other servers replicate as part of hierarchy replication to the backfilling public folder store. If they do replicate correctly to the backfilling public folder store, the server determines that it's not synchronized and writes an entry into the backfill array. Backfilling could take two or three days to complete.

**Other Problems**

This section contains information about how to resolve problems that do not fit into the other categories in this appendix. These issues include the following:

- Unable to Access Permissions on a Public Folder (Invalid Windows Handle Error)
- One or More Users Could Not Be Added to the Folder Access List
- Mail Messages to Public Folder Were Not Delivered
- Outlook Web Access Cannot View a Public Folder After the Tree Has Been Renamed
- Message "Operation Failed" When Attempting to Access a Tree Using Exchange System Manager
- Exchange 5.5 Servers See Multiple Public Folder Stores on an Exchange 2003 Server
- In a Mixed Exchange 5.5-Exchange 2003 Environment, Users Cannot Access a Public Folder Using Outlook Web Access
- Attachment Exceeds Storage Limit on Public Folder
Unable to Access Permissions on a Public Folder (Invalid Windows Handle Error)

The most frequent cause of the Invalid Windows Handle Error in Microsoft Exchange Server 2003 is an administrator's use of the M:\ drive (the Exchange Installable File System) to modify permissions on a public folder. Servers running clean installations of Exchange 2003 do not have an M:\ drive, although it may still be accessible on upgraded servers that previously ran Exchange 2000.

This error can also arise if you use the wrong dialog box in Exchange System Manager to modify client permissions on a public folder, although this is unlikely to occur. For more information about the correct way to modify permissions on a public folder, see "Special Considerations for Working with Client Permissions" in Chapter 7, "Managing Mailbox Stores and Public Folder Stores."

The underlying cause of this error is that, if you use the Windows user interface to modify client permissions for a public folder, the permissions are stored in such a way that Exchange is no longer able to convert the permissions to their MAPI form. If this happens, you will no longer be able to use the dialog boxes in Outlook or Exchange System Manager to edit the permissions.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you use this procedure, the affected public folders will have permissions for only the folder owner (an administrative account), Default users, and Anonymous users.</td>
</tr>
</tbody>
</table>

To reset permissions on public folders

1. In Exchange System Manager, under the Public Folders node, create a new top-level folder.
2. Move the affected folder and subfolders (those with the wrong permissions settings) into this new folder.
3. Set the permissions on the new top-level folder so that an account with administrator permissions in Active Directory is the owner.
4. Right-click the new top-level folder, point to All Tasks, click Propagate Settings, and then select the Administrative Rights and Folder Rights check boxes.
   After you click OK, the changes to the permissions are applied to all subfolders of the new top-level folder.
5. Move the affected folder and subfolders back to their original locations in the Public Folders tree.
6. Verify that, in Exchange System Manager, you can now modify the permissions.
One or More Users Could Not Be Added to the Folder Access List

Either Outlook users or administrators using Exchange System Manager could see this message when trying to grant users permissions to a folder in the Public Folders tree. When this error occurs, Default and Anonymous permissions on the affected folder do not work. Only users that were previously granted permissions to the folder are able to access it. However, if you try to use the Properties button to view the properties of one or more of those users in the folder's Client Permissions dialog box, you will get a MAPI error message. This user (or users) is the root of the permissions problem.

This permissions problem occurs when a user who does not have an Exchange mailbox creates or administers a folder in such a way that they user is granted explicit permissions to the folder (this can happen using Exchange System Manager or the Exchange Installable File System). The most likely cause is that someone used an account that has permissions to administer folders (for example, an account that belongs to the Enterprise Admins group), but no mailbox was ever created for that account.

To fix this problem, in the folder's Client Permissions dialog box, identify the user whose properties you cannot access. Remove the user from the folder's access control list, or go to the Active Directory Users and Computers snap-in and create a mailbox for that user.

Mail Messages to Public Folder Were Not Delivered

If you have a mixed-mode Exchange organization, check that the public folder connection agreement has replicated the folder's directory objects correctly. Remember that you cannot e-mail general-purpose hierarchy folders from Exchange 2003 if the e-mail message travels by way of an Exchange 5.5 server.

In any Exchange organization, an e-mail to a folder first needs to go to a public folder store that supports the correct public folder tree to find the replica list for the destination folder. It may be that the public folder store that was chosen has not received the updated replica list of the destination folder yet.
Outlook Web Access Cannot View a Public Folder After the Tree Has Been Renamed

When you rename a public folder tree, you have to update all of the virtual directories that point to that tree. The changes will not finish propagating from Exchange to Internet Information Services (IIS) until after the public folder store has been remounted.

Therefore, if you rename a tree, you need to:

1. Update the virtual directories on the servers that hold public folder stores for this tree, so that they point to the new tree.
2. To propagate the change through Exchange and IIS, remount all of the public folder stores that support the tree.

Message "Operation Failed" When Attempting to Access a Tree Using Exchange System Manager

To access the public folder trees, Exchange System Manager uses an OLEDB service that depends on the World Wide Web Publishing Service (W3SVC). If you have problems accessing a tree using Exchange System Manager, check the following:

- Check that the Microsoft Internet Explorer settings do not have a non-existent proxy server configured.

Exchange 5.5 Servers See Multiple Public Folder Stores on an Exchange 2003 Server

This problem can occur if a new configuration connection agreement (Config CA) replaces an existing Config CA. This replacement can occur, for instance, if servers running Site Replication Service (SRS) are removed from the organization incorrectly.

The problem starts when the new Config CA replicates the Active Directory object for a default public folder store from an Exchange 2003 server in an Exchange 2003 administration group to the Exchange 5.5 Directory of an Exchange 5.5 server. The new Config CA does not "see" that the Exchange 2003 default public folder store's object already exists in the Exchange 5.5 Directory because the object has the old Config CA's replication signature.
As a result of the replication cycle, a second default public folder store appears in the Exchange 5.5 Directory for the Exchange 2003 server. Because the server's container already has an object called Microsoft Public MDB, the new object is named Microsoft Public MDB – 1. However, this name is too long for a public folder store object in Exchange 5.5, and, as a result, the replication engines on Exchange 5.5 servers will fail to start throughout the organization.

The following errors will be logged:

```
Error 0x3f0 occured while performing a site folder teardown check
Event 3079 MSExchangeIS Public
Unexpected replication thread error 0x3f0
EcGetReplMsg
EcReplStartup
FreplAgent
```

The "site folder teardown check" referred to in the error message is performed each time an Exchange 5.5 server starts, to determine whether any sites have been removed, in which case the list of site folders (SCHEDULE + FREE BUSY and so forth) needs to be cleaned up. You can do this clean-up by comparing details about all of the site folders with details about all of the public folder stores in the organization.

Because the string Microsoft Public MDB – 1 is too long, the replication thread fails with an Out Of Memory error (0x3f0) when it tries to get site details of the store with that name. This failure in turn causes the replication engine to fail to start. The only way to fix this problem is to remove both the incorrect directory object and the original correct directory object for the 2003 public folder store from the Exchange 5.5 Directory, and replicate the directory entry again.

**Note**

Before you remove the Exchange 2003 default public folder store objects from the Exchange 5.5 Directory and allow the correct object to replicate back in, contact Microsoft Product Support Services to ensure that you do it correctly.

---

**In a Mixed Exchange 5.5-Exchange 2003 Environment, Users Cannot Access a Public Folder Using Outlook Web Access**

Microsoft Outlook Web Access users cannot access folders that exist only on Exchange 5.5 servers. Check your public folder connection agreements to make sure that the folders are being replicated to at least one Exchange 2003 server.
Attachment Exceeds Storage Limit on Public Folder

After you install Exchange 2003 (or Exchange 2000 Server Service Pack 1 (SP1) or later), when you post a new item with an attachment that is larger than 1 megabyte (MB) to a public folder, you receive the following error message:

This item exceeds the maximum size defined for this folder and cannot be saved. Contact your administrator to have the folder limits increased.

Attachments that are smaller than 1 MB are not affected. This issue occurs even if no limits are set on the public folder store.

This issue occurs because a system folder called OWAScratchPad{GUID} is created when a user adds an attachment to a public folder post. This system folder has a limit of 1,024 kilobytes (KB).

To work around this issue, use Exchange System Manager to either increase or remove the limit on the OWAScratchPad{GUID} folder.

To change or remove the size limit for attachments in public folders

1. In Exchange System Manager, right-click Public Folders, and then click View System Folders.

2. Expand Public Folders, then right-click the OWAScratchPad folder. Click Properties, and then click Limits.

3. Under Storage Limits, the Maximum item size (KB) is set to 1,024, or 1 MB, by default. To change the limit:
   • Under Storage Limits, change the limit in the Maximum item size (KB) box.
   —or—
   • Click Use public store defaults. When this check box is selected, the limit settings are controlled by the Maximum items size (KB) setting and the Prohibit post at (KB) setting on the Limits tab of the public folder store Properties dialog box. However, if the store is configured by a system policy, the settings are located on the Limits tab of the policy's Properties dialog box.
For information about Microsoft® Exchange Server, see http://www.microsoft.com/exchange. Additionally, the following Web sites, Exchange books, technical articles, tools, resource kits, and Microsoft Knowledge Base articles provide valuable information relevant to administering Exchange Server 2003.

**Web Sites**

- Download or view online the Exchange Software Development Kit. (http://msdn.microsoft.com/exchange)
- Microsoft Online Crash Analysis (http://go.microsoft.com/fwlink/?LinkId=18428)
- Microsoft Product Support Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=18175)
- Exchange 2000 Server Third-party Solutions (http://go.microsoft.com/fwlink/?LinkId=5225)
- Microsoft Operations Manager (http://www.microsoft.com/mom/)
- RFC 2798, "Definition of the inetOrgPerson LDAP Object Class" (http://go.microsoft.com/fwlink/?LinkId=18610)

**Exchange Server 2003 Books**

Exchange 2000 Server Books

Configuring SMTP in Exchange 2000 Server
(http://go.microsoft.com/fwlink/?LinkId=15084)

Disaster Recovery for Microsoft Exchange 2000 Server
(http://go.microsoft.com/fwlink/?LinkID=18350)

Monitoring Exchange 2000 with Microsoft Operations Manager 2000
(http://go.microsoft.com/fwlink/?LinkId=18177)

Technical Articles

"Working with Store Permissions in Microsoft Exchange 2000 and 2003"
(http://go.microsoft.com/fwlink/?LinkId=18612)

"Public Folder Permissions in a Mixed Mode Microsoft Exchange Organization"
(http://go.microsoft.com/fwlink/?LinkID=10228)

"Better Together: Microsoft Operations Manager and Exchange Server 2003"
(http://go.microsoft.com/fwlink/?LinkId=18176)

"Checklist: Preparation for installing a cluster"
(http://go.microsoft.com/fwlink/?LinkId=16302)

"Best practices for securing server clusters"
(http://go.microsoft.com/fwlink/?LinkId=18173)

Tools

Exchange SDK Development Tools June 2003
(http://go.microsoft.com/fwlink/?LinkId=18614)

Exchange Stress and Performance Tool (ESP)—Build 5531.0
(http://go.microsoft.com/fwlink/?LinkId=1709)

Load Simulator
(http://go.microsoft.com/fwlink/?LinkId=1710)

Microsoft Baseline Security Analyzer
(http://go.microsoft.com/fwlink/?LinkId=17809)

RPC Ping: RPC Connectivity Verification Tool
(http://go.microsoft.com/fwlink/?LinkId=18615)
Resource Kits

Microsoft Windows Server 2003 Resource Kit
(http://go.microsoft.com/fwlink/?LinkId=18860)

Microsoft Knowledge Base Articles

The following Microsoft Knowledge Base articles are available at http://support.microsoft.com/:

324745, "HOW TO: Install the Active Directory Administrative Tools to Windows XP Professional in Windows Server™ 2003"
(http://support.microsoft.com/?kbid=324745)

313992, "How To Add an Attribute to the Global Catalog in Windows 2000"
(http://support.microsoft.com/?kbid=313992)

316047, "XADM: Addressing Problems That Are Created When You Enable ADC-Generated Accounts"
(http://support.microsoft.com/?kbid=316047)

257891, "XWEB: 'The Page Could Not Be Found' Error Message When You Use OWA"
(http://support.microsoft.com/?kbid=257891)

328970, "Cumulative Patch for Internet Explorer"
(http://support.microsoft.com/?kbid=328970)

279681, "How to Force SSL Encryption for an Outlook Web Access 2000 Client"
(http://support.microsoft.com/?kbid=279681)

297393, "HOWTO: Programmatically Move an Exchange 2000 Mailbox Using CDOEXM in Visual C++"
(http://support.microsoft.com/?kbid=297393)

288150, "XADM: How to Rehome Public Folders in Exchange 2000"
(http://support.microsoft.com/?kbid=288150)

266096, "XGEN: Exchange 2000 Requires /3GB Switch with More Than 1 Gigabyte of Physical RAM"
(http://support.microsoft.com/?kbid=266096)

810371, "XADM: Using the /Userva Switch on Windows 2003 Server-Based Exchange Servers"
(http://support.microsoft.com/?kbid=810371)

168801, "How to Turn On Cluster Logging in Microsoft Cluster Server"
(http://support.microsoft.com/?kbid=168801)
access control entry
(ACE) An individual item in an access control list (ACL). Access permissions for each user or group object for an Exchange store resource are listed as an ACE in the ACL for the resource.

ACE
See definition for: access control entry

access control list
(ACL) A list of Microsoft® Windows Server™ 2003 or Windows® 2000 Server security principles, user accounts, and groups associated with the object. This list is used to determine whether a user or process has been granted access to an object. Individual entries in the list are known as access control entries (ACEs).

ACL
See definition for: access control list

Active Directory
The directory service for Windows Server 2003 or Windows 2000. The directory contains information about objects on the network and makes this information available for authorized administrators and users. Microsoft Active Directory® directory service gives network users access to permitted resources anywhere on the network using a single logon process. It provides administrators with a hierarchical view of the network and a single point of administration for all network objects.

Active Directory Connector
(ADC) A Windows Server 2003 or Windows 2000 service that replicates the Exchange Server 5.5 directory with Active Directory. This allows administration of a directory from either Active Directory or the Exchange 5.5 directory service.

Active Directory Replication Bridgehead Server
An Exchange 5.5 computer that acts as the endpoint of a directory replication connection between its site and a Windows Server 2003 or Windows 2000 Server domain controller. See also: bridgehead server
Active Directory Service Interface
(ADSI) A dual-interfaced model that allows programmatic access to underlying directory
services through a common command set.

Active Directory Users and Computers
A Microsoft Management Console (MMC) snap-in that allows administrators to manage
objects in the domain.
See also: Microsoft Management Console

ADC
See definition for: Active Directory Connector

address
A recipient address is a collection of information that identifies a specific message recipient.
It must be unique and complete to properly identify an e-mail recipient.

Address Book
A directory of address lists available to Exchange users that allows them to address e-mail
messages, and select conferencing resources. Exchange administrators determine which
address lists are available to their e-mail users.

address list
A collection of recipient and other Active Directory objects. Each address list can contain
one or more types of objects (for example, users, contacts, groups, public folders,
conferencing, and other resources). Microsoft Exchange Server 2003 and Exchange 2000
Server address lists also provide a mechanism to partition mail-enabled objects in Active
Directory for the benefit of specific groups of users.

address space
A set of address information associated with a connector or gateway that identifies certain
types of messages. An address space is typically a subset of a complete address.

ADMD
See definition for: Administrative Management Domain

administrative group
A collection of Active Directory objects that are grouped together for the purpose of
permissions management. An administrative group can contain policies, routing groups,
public folder hierarchies, servers, and chat networks. The content of an administrative group
depends on choices you make during installation.

Administrative Management Domain
(ADMD) Part of a management domain that is a set of messaging systems managed by an
organization that contains at least one message transfer agent (MTA). An ADMD is
managed by a public service provider and is the highest level management domain that
transmits third-party message traffic.
See also: message transfer agent

ADSI
See definition for: Active Directory Service Interface
advanced security
A feature that enables you to digitally sign and/or seal (encrypt) a message. When you sign a message, you must provide your advanced security password. This password guarantees to recipients that a digitally signed message is from you. When you encrypt a message, recipients must provide their advanced security password to decrypt it.

alias
A short name used to look up recipients in the directory. For example, Ben Miller may have the alias of BenM. This alias is used to automatically generate the recipient's e-mail address, such as benm@contoso.com. In Active Directory, the alias is stored in the mailNickname attribute.

anonymous user
A non-validated user who is not recognized by the server, and who can only access published folders and address lists.

attribute
A characteristic of an object; for example, a network printer is an object and its attributes include its location, whether it can print in color, and its print job capacity.

authentication
In a multiuser or network operating system, the process by which the system validates the user's logon information. A user's name and address are compared against an authorized list, and if the system detects a match, access is granted to the network.

See also: trust relationship

authentication certificate
A certificate provided by a remote host. To ensure a secure data connection, the certificate establishes trustworthiness when a connection is attempted by an application.

back-end server
A server that hosts at least one database that front-end servers connect to when relaying requests from clients.

See also: front-end server

bridgehead server
A computer that connects servers using the same communications protocols so information can be passed from one server to another. In Exchange 2003 and Exchange 2000, a bridgehead server is a connection point from a routing group to another routing group, remote system, or other external system.
CA
See definition for: certification authority

certificate
An electronic credential that authenticates a user on the Internet and on intranets. Certificates ensure the legitimate online transfer of confidential information or other sensitive material by means of public encryption technology. In Exchange, certificates contain information used for digital signatures and encryption that binds the user's public key to the mailbox.

Certificate Trust List
(CCTL) A signed list of root certification authority certificates that an administrator considers reputable for designated purposes, such as client authentication or secure e-mail.

certification authority
(CA) An entity with a server that issues certificates to clients and servers. A certification authority attests to the identification of a user of a public key. The CA can also revoke certificates when the private key associated with the certificate is compromised, or when the subject of the certificate leaves an organization.

code page
A means of providing support for character sets and keyboard layouts for different countries/regions. A code page is a table that relates the binary character codes used by a program to keys on the keyboard or to characters on the display.

coexistence
When you connect Exchange 2003 to another messaging system, including a previous version of Exchange, the two systems coexist. A coexistence period can be short-term (for example, enough time to migrate users from an existing messaging system to Exchange 2003), or it can be long-term (for example, a permanent connection to the messaging system of another department that is not moving to Exchange 2003).

connector
A component that enables information to flow between two systems. For example, connectors support message transfer, directory synchronization, and calendar querying between Exchange and other messaging systems. When connectors are in place, the basic user experience is maintained on both messaging systems. The exchange of mail and other information between Exchange and other messaging systems is transparent to the user, even if the two systems function differently.

contact
An Active Directory object that represents a user who is outside of the Exchange organization. For example, a contact may represent a user at another company. A contact in Windows Server 2003 or Windows 2000 is equivalent to a custom recipient in Exchange 5.5 and earlier versions.

See also: custom recipient
**custom address lists**  
An address list created to help users who need a custom view of recipients within an Exchange organization. For example, you can create an address list that includes only employees in North America, or you can create an address list that includes only employees in the marketing department.  
*See also:* default address list

**custom recipient**  
In Exchange 5.5 and earlier, a custom recipient is a user who is not hosted by Exchange. In Exchange 2003, such users can be added to Active Directory as contacts, Windows users, or users whose Windows accounts are disabled. In any case, they are mail-enabled, but not mailbox-enabled, because their mailboxes are hosted on another messaging system.  
*See also:* contact, mail-enabled

**DACL**  
See definition for: discretionary access control lists

**DAV**  
See definition for: Distributed Authoring and Versioning

**default address list**  
An address list that is automatically created based on the values of specific attributes of Active Directory objects. These address lists are available to Exchange users without any administrator action.  
*See also:* custom address lists

**delegate**  
A representative with permissions to manage e-mail for another user, send e-mail for another user, or both. The user or administrator grants these permissions.

**Delegate Access**  
A feature that allows you to grant a representative permission to manage your e-mail, send e-mail for you, or both.

**delivery receipt**  
A notification indicating the date and time a message that you sent was delivered. You can request a delivery receipt for all messages that you send or for individual messages.

**destination queue**  
A queue containing messages that are addressed to the same final destination server.

**directory replication**  
The process of updating the directories of all servers within and between sites.
directory synchronization
The process of synchronizing directory information about Exchange users from Active Directory with the directory of another messaging system. With directory synchronization, users can send e-mail to users on a different messaging system using an alias or short name. In addition, address or other directory changes are updated automatically between systems.

discretionary access control list
(DACL) A Windows Server 2003 or Windows 2000 access control list (ACL) that identifies which users and groups are granted or denied which permissions. DACLs may be explicit to the object in that permissions may have been granted or denied specifically for that object. However, DACLs may also be implicit in that they are inherited from a parent object.

Distributed Authoring and Versioning
(DAV) An extension to the HTTP/1.1 protocol that allows for manipulation of objects and attributes. Although not specifically designed for the purpose, DAV allows for the control of a filing system using HTTP protocol.

distribution group
A group of recipients created to expedite mass mailing of messages and other information. When e-mail is sent to a distribution list, all members of that list receive a copy of the e-mail.
See also: group

DNS
See definition for: Domain Name System

domain
A group of computers that are part of a network and share a common directory database.

domain controller
A computer running Windows Server 2003 or Windows 2000 Server that manages user access to a network, which includes logging on, authentication, and access to Active Directory and shared resources.

Domain Name System
(DNS) A TCP/IP standard name service that allows clients and servers to resolve names into Internet Protocol (IP) addresses and vice versa. The Dynamic Domain Name Services in Windows Server 2003 and Windows 2000 enables clients and servers to register themselves automatically without the need for administrators to define records manually.

DSAccess
An Exchange 2003 component that provides directory lookup services for components such as Simple Mail Transfer Protocol (SMTP), message transfer agent (MTA), and the Exchange store. Client requests use the DSProxy service for directory access.
E

encryption
An advanced security feature that provides confidentiality by allowing users to conceal data. Data is encrypted as it resides on disk and travels over a network.

ESMTP
See definition for: Extended Simple Mail Transfer Protocol

Exchange store
A storage platform that provides a single repository for managing multiple types of unstructured information within one infrastructure. The Exchange store combines the features and functionality of the file system, the Web, and a collaboration server (such as Exchange Server) through a single, URL-addressable location for storing, accessing, and managing information, as well as for building and running applications. There are two kinds of stores: mailbox stores and public folder stores. The Exchange store was previously known as Web Storage System.

extended permission
A permission that is specific to an object added to the standard Active Directory object schema by Exchange.

Extended Simple Mail Transfer Protocol
(ESMTP) An extension of the basic Simple Mail Transfer Protocol (SMTP) that provides additional commands for server communication. An ESMTP server initiates a session with an EHLO command. If the receiving server supports ESMTP, it responds to this command with a list of ESMTP extensions that it supports. If the receiving server does not support ESMTP, the sending receiver reverts to basic SMTP.

Extensible Storage Engine
Formerly known as JET, Extensible Storage Engine is a method that defines a low-level application programming interface (API) to the underlying database structures in Exchange. Extensible Storage Engine is also used by other databases, such as the Active Directory database.

F

firewall
A combination of hardware and software that function as a security system intended to protect an organization's network against external threats coming from another network, such as the Internet. A firewall prevents direct communication between a network and external computers by routing communication through a proxy server that exists outside the network.
forest
One or more domain trees that do not form a contiguous namespace. Forests allow organizations to group divisions that operate independently, but still need to communicate with one another.

FQDN
See definition for: fully qualified domain name

front-end server
A server that receives requests from clients and relays them to the appropriate back-end server.
See also: back-end server

front-end/back-end architecture
An Exchange configuration where clients access a bank of protocol servers (the front-end) for collaboration information, and then these servers communicate with the data stores on separate servers (the back-end) to retrieve the physical data. A front-end/back-end configuration allows for a scalable, single point-of-contact for all Exchange-related data.
See also: protocol farm

fully qualified domain name
(FDQN) A Domain Name System (DNS) domain name that has been stated unambiguously to indicate with certainty its location in the domain namespace tree. Fully qualified domain names differ from relative names in that they typically are stated with a trailing period (.), for example, "host.contoso.com.", to qualify their position to the root of the namespace.
See also: Domain Name System

G

gateway
A device that connects networks using different communications protocols, so information can be passed from one network to the other. A gateway transfers information and converts it to a form compatible with the protocols used by the receiving network.

GID
See definition for: global domain identifier
**global address list**
A list containing all Exchange users, contacts, groups, conferencing resources, and public folders in an organization. This list is retrieved from the global catalog servers in Active Directory and is used by Microsoft Outlook® clients to address messages or find information about recipients within the organization.

**global catalog**
A server that holds a complete replica of the configuration and schema naming contexts for the forest, a complete replica of the domain naming context in which the server is installed, and a partial replica of all other domains in the forest. The global catalog is the central repository for information about objects in the forest.

**global domain identifier**
(GID) Exchange uses the X.400 global domain identifier in a relay environment. The global domain identifier consists of the country/region, Administrative Management Domain (ADMD), and Private Messaging Domain (PRMD) name of the remote message transfer agent (MTA). It is used for inserting trace elements and can be used for troubleshooting an unsuccessful relay attempt. It is also used to prevent message looping in wide-area messaging environments.

**globally unique identifier**
(GUID) A value that uniquely identifies some entity and never changes. In Active Directory, GUIDs are automatically generated for every object (for example, user, group, computer, and so on), and that value is guaranteed to never change. In Exchange, the Recipient Update Service automatically generates GUIDs for every mailbox. Also referred to as a Universally Unique Identifier (UUID).

**group**
A collection of users, groups, and contacts. There are two types of groups: distribution groups and security groups. Distribution groups are used only for e-mail. Security groups are used to grant access to resources.

*See also:* distribution list

**GUID**
See definition for: globally unique identifier

**home server**
The Exchange server that contains a user's mailbox.

**Hypertext Transfer Protocol**
(HTTP) A client/server protocol used on the Internet for sending and receiving HTML documents. HTTP is based on the TCP/IP protocol.
IFS
See definition for: installable file system

IIS
See definition for: Internet Information Services

IMAP
See definition for: Internet Message Access Protocol

IMAP4
See definition for: Internet Message Access Protocol

IMAP4rev1
See definition for: Internet Message Access Protocol

InetOrgPerson
An Active Directory object that is similar to the Windows user object, but has extended attributes to improve compatibility with directory services that use the InetOrgPerson object.

Installable file system
(IFS) A storage technology that functions as a filing system. It makes mailboxes and public folders available as traditional folders and files through standard Microsoft Win32® application programming interface processes, such as Microsoft Internet Explorer and the command prompt.

Internet Information Services
(IIS) The Microsoft Web service for publishing information on an intranet or the Internet and for building server-based Web applications. Upon installation, Exchange 2003 extends the messaging capabilities of IIS and incorporates it into the Exchange message routing architecture.

Internet Message Access Protocol
(IMAP) An Internet messaging protocol that enables a client to access mail on a server rather than downloading it to the user's computer. IMAP is designed for an environment where users log on to the server from a variety of different workstations.

IP address/TCP port combination
A combination of attributes that uniquely identifies Simple Mail Transfer Protocol (SMTP), Network News Transfer Protocol (NNTP), Internet Message Access Protocol (IMAP), and Post Office Protocol (POP) virtual servers in Exchange 2003. Virtual servers may share an Internet Protocol (IP) address, provided their TCP ports are different; if they share a TCP port, their IP addresses must be different. The combination must be unique on all virtual servers. This is also true for HTTP virtual servers, except that they have a third unique identifying characteristic: a host name.
J
No glossary entries.

K
No glossary entries.

L
LDAP
See definition for: Lightweight Directory Access Protocol

Lightweight Directory Access Protocol
(LDAP) A network protocol designed to work on TCP/IP stacks to extract information from a hierarchical directory such as X.500. It is useful for searching through data to find a particular piece of information.

link state information
Information about the state of messaging routes (links) in an Exchange 2003 messaging system that is determined using the link state algorithm to quickly and frequently calculate the state of system links for up-to-date status about routes. Exchange 2003 servers use link state information to make the best routing choice at the source rather than sending a message down a path where a downstream link may be unavailable. Choosing the best route at the source eliminates message bounce and looping.

link state table
The database used on each Exchange 2003 server to store link state information propagated by the link state algorithm. The link state table is used to evaluate the most suitable route for a message given cost and availability information.

local bridgehead server
A server within a routing group that handles e-mail flow to and from a connector in that routing group. Routing group connectors can have multiple local bridgehead servers or no local bridgehead server, which means every server in the routing group acts as a local bridgehead server. Simple Mail Transfer Protocol (SMTP) and X.400 connectors must have one, and only one, local bridgehead server.
See also: remote bridgehead server

local delivery message
A message sent between recipients that share the same home server.
mail exchange (MX)

MX records specify a host running a Simple Mail Transfer Protocol (SMTP) server along with a priority number; lower numbers take precedence over higher numbers. There should be one MX record for each SMTP server in the Domain Name System (DNS) zone. SMTP servers query a DNS server to determine the preferred SMTP server for receiving e-mail in a given domain. Servers with higher priority are tried first. If multiple servers have the same priority, a server is chosen randomly.

mail gateway

A server in your organization that stands between your internal intranet and the Internet. All Internet e-mail will pass through the mail gateway before it reaches users in your organization.

mail-enabled

An Active Directory object that has at least one e-mail address defined. If the user is mail-enabled, the user has an associated e-mail address, but does not have an associated Exchange mailbox.

See also: custom recipient

mailbox

The location where e-mail is delivered. The administrator sets up a mailbox for each user. If a set of personal folders is designated as the e-mail delivery location, e-mail is routed from the mailbox to this location.

mailbox store

The part of the Exchange store that maintains information in user mailboxes. A mailbox store consists of a rich-text .edb file, plus a streaming native Internet content .stm file.

mailbox-enabled

An Active Directory object that has an Exchange mailbox associated with it; therefore, it can both send and receive messages within the Exchange system.

MAPI

See definition for: Messaging Application Programming Interface

MAPI profiles

The set of MAPI configuration settings, stored in the registry, that allow MAPI clients, such as Microsoft Outlook, to connect to various messaging services, such as Exchange.

MDB

See definition for: message database

message database

(MDB) An instance of a database implemented in Exchange. A single MDB is identified as a mailbox store or public folder store, depending on the type of data that it stores.
**message queue**
An ordered list of messages awaiting transmission from which the messages are taken on a first-in, first-out basis.

**message transfer agent**
(MTA) An Exchange component that routes messages to other Exchange MTAs, information stores, connectors, and third-party gateways. Also referred to as X.400 protocol in Exchange 2003 System Manager.

**Messaging Application Programming Interface**
(MAPI) A messaging architecture enabling multiple applications to interact with multiple messaging systems across a variety of hardware platforms. MAPI is built on the Component Object Model (COM) foundation.

**metabase**
A store that contains metadata, such as that used by Internet Information Services (IIS). The metabase can be viewed through utilities such as Metaedit.

**metabase update service**
A component in Exchange 2003 that reads data from Active Directory and transposes it into the local Internet Information Services (IIS) metabase. The metabase update service allows the administrator to make remote configuration changes to virtual servers without a permanent connection to each system.

**Microsoft Exchange Information Store service**
A Microsoft Exchange service that manages the Exchange store.
*See also:* Exchange store

**Microsoft Management Console**
(MMC) A management display framework that hosts administration tools and applications. Using MMC, you can create, save, and open collections of tools and applications.

**migration**
The process of moving an existing messaging system to another system by copying the existing mailboxes, messages, and other data, and importing that information into a new messaging system.

**MIME**
See definition for: Multipurpose Internet Mail Extensions

**mixed mode**
The default operating mode of Exchange when it is installed. Mixed mode allows Exchange 2003 and Exchange 2000 servers and servers running earlier versions of Exchange to coexist in the same organization. Mixed mode allows interoperability between versions by limiting functionality to features both products share.

**mixed-mode site**
An Exchange 5.x site that also contains Exchange 2003 or Exchange 2000 servers.

**MMC**
See definition for: Microsoft Management Console
MTA  
See definition for: message transfer agent

**Multipurpose Internet Mail Extensions**  
(MIME) A standard that enables binary data to be published and read on the Internet. The header of a file with binary data contains the MIME type of the data; this informs client programs (such as Web browsers and mail packages) that they process the data as straight text.

**MX**  
See definition for: mail exchange (MX)

Native mode  
An operating mode of Exchange 2003 when the Exchange organization consists of only Exchange 2003 or Exchange 2000 servers. Servers running Exchange 5.5 and earlier versions cannot join an organization running in native mode.

**NDR**  
See definition for: non-delivery report

Nested address list  
An address list located under another address list for organizational purposes. A nested address list does not inherit the filter rules of its parent address list.

**Network News Transfer Protocol**  
(NNTP) An application protocol used in TCP/IP networks. Enables clients to read and post information to USENET newsgroups.  
See also: newsgroup

Newsfeed  
The flow of items from one USENET site to another.

Newsgroup  
An Internet discussion group that focuses on a particular category of interest.  
See also: Network News Transfer Protocol

**NNTP**  
See definition for: Network News Transfer Protocol

**Non-delivery report**  
(NDR) A notice that a message was not delivered to the recipient.
object
The basic unit of Active Directory. It is a distinct, named set of attributes that represents something concrete, such as a user, a printer, a computer, or an application.

offline address list
A collection of address lists available to Exchange 2003 users either when they are working offline, or when they are working remotely over a dial-up connection. Exchange administrators can choose which address lists are available for their users that work offline.

offline folder
Offline folders allow a user to copy a folder from a server location, work with the contents of the folder when they are not connected to the network, and then synchronize the folders when they are online again. Offline folders are stored in the offline folder (.ost) file.

organization
A set of computers running Exchange Server that provide messaging and collaboration services within a business, an association, or a group.

Organizational Forms Library
A system folder on an Exchange computer that stores forms commonly accessed by users within an organization. These forms are available to all Exchange users.

organizational unit
An Active Directory container into which you can place objects such as user accounts, groups, computers, printers, applications, file shares, and other organizational units. Organizational units can be used to contain and assign specific permissions to groups of objects, such as users and printers. An organizational unit cannot contain objects from other domains. An organizational unit is the smallest unit to which you can assign or delegate administrative authority.

outbox
A built-in folder that holds e-mail that you send until it is delivered.

Outlook Web Access
Outlook Web Access for Exchange 2003 provides users access to e-mail, personal calendars, group scheduling, contacts, and collaboration applications using a Web browser. It can be used for UNIX and Macintosh users, users without access to an Outlook client, or users connecting from the Internet. Outlook Web Access offers cross-platform client access for roaming users, users with limited hardware resources, and users who do not have access to their own computers.
P

PAB
See definition for: Personal Address Book

PDL
See definition for: personal distribution list

perimeter network
One or more computers that have a connection to the Internet through an external screening router and a connection to the internal network through an interior screening router. Computers that are linked to the perimeter network have limited access to both the Internet and the internal network. This architecture is convenient if multiple hosts require direct Internet access.

permission
Authorization for a user or computer to perform an action, such as sending e-mail for another user or posting items in a public folder.

Personal Address Book
(PAB) A customizable address list in which a user can add and delete names of users and personal distribution lists to which messages frequently are addressed. A user can either create the entries or copy them from another address list. Personal Address Book files have a .PAB extension and can be copied easily to a disk.

personal distribution list
(PDL) A distribution list that a user creates and adds to their Personal Address Book (PAB). A distribution list is a name assigned to a group of recipients. When a user addresses a message or form to a PDL, each user in the list receives the message. The administrator creates and maintains distribution lists in the global address list; users create and maintain their PDLs.

policy
A collection of configuration settings that are applied to one or more Exchange configuration objects. Policies simplify the administration of Exchange. You can define a policy that controls the configuration of some or all settings across a server or other objects in an Exchange organization. After policies are defined and implemented, editing the policy and applying it changes the configuration of all servers and objects covered by the policy.

POP3
See definition for: Post Office Protocol version 3

port
Generally, a connection point on your computer where you can connect devices that pass data into and out of a computer. For example, a printer is typically connected to a parallel port (also called a Lightweight Directory Access Protocol (LDAP) port), and a modem is typically connected to a serial port (also called a COM port).
Post Office Protocol version 3

A user right that is assigned to a user and that specifies allowable actions on the network. An example of a privilege is the right to shut down a system.

Protocol

An Internet protocol that allows a user to download mail from their inbox on a server to the client computer where messages are managed. This protocol works well for computers that are unable to maintain a continuous connection to a server.

Protocol farm

A collection of virtual servers that function as the primary connection point for users in an organization. The unified namespace allows users to access information without having to know a server's physical location.

See also: front-end/back-end architecture

Proxy server

A firewall component that manages Internet traffic to and from a LAN and can provide other features, such as document caching and access control.

Public folder

A folder that co-workers can use to share a wide range of information, such as project and work information, discussions about a general subject, and classified ads. Access permissions determine who can view and use the folder. Public folders are stored on computers running Exchange.

Public folder hierarchy

A tree or hierarchy of public folders with a single public folder store.

Public folder replication

The process of keeping copies of public folders on other servers up-to-date and synchronized with each other.

Public folder store

The part of the Exchange store that maintains information in public folders. A public folder store consists of a rich-text .edb file, plus a streaming native Internet content .stm file.
queue
A temporary location for a set of messages that will be transported to the same next-destination server. All messages within a queue have a common next hop on the path to their respective final destinations.

query-based distribution groups
A distribution group that uses a Lightweight Directory Access Protocol (LDAP) query to derive its membership at the time the message is sent.

See also: distribution group

RAID
See definition for: redundant array of independent disks

recipient
An Active Directory object that is mail-enabled, mailbox-enabled, or that can receive e-mail. A recipient is an object within Active Directory that can take advantage of Exchange functionality.

recipient policy
Policies that are applied to mail-enabled objects to generate e-mail addresses. They can be defined to apply to thousands of users, groups, and contacts in Active Directory using a Lightweight Directory Access Protocol (LDAP) query interface in a single operation.

Recipient Update Service
An Exchange 2003 service that updates the recipient objects within a domain with specific types of information. You can schedule appropriate intervals to update the recipient objects. For example, this service updates recipient objects with address list membership and e-mail addresses at intervals scheduled by the administrator.

redundant array of independent disks
(RAID) A mechanism for storing identical data on multiple disks for redundancy, improved performance, and increased mean time between failures (MTBF). RAID provides fault tolerance and appears to the operating system as a single logical drive.

relay host
See definition for: smart host

remote bridgehead server
A server that handles e-mail flow to and from a routing group connector in a different routing group.

See also: local bridgehead server
remote procedure call
   (RPC) A routine that transfers functions and data among computers on a network.
replicas
   A copy of a public folder that contains all of the folder's contents, permissions, and design
elements, such as forms behavior and views. Replicas are useful for distributing user load on
servers, distributing public folders geographically, and for backing up public folder data.
   See also: public folder
replication
   See definition for: directory replication
reverse proxy server
   A reverse proxy server is similar to a proxy server used for outbound network traffic except
   that it relays connection requests for inbound network traffic.
routing engine
   A Component Object Model (COM) component that relates to Exchange Server Routing and
   runs on Event Service on Exchange 5.5. It acts as a simple state engine that executes and
   tracks multiple process instances within an Exchange folder. The state is advanced when
   events occur within the folder. The routing engine supports the execution of flow-control
   activities directly, and it can call VBScript functions for other activities. Exchange Server
   Routing also works with the Microsoft Transaction Server (MTS).
routing group
   A collection of Exchange servers that have full-time, reliable connections. Messages sent
   between any two servers within a routing group go directly from source to destination.
   Routing groups are optional and are not visible in Exchange System Manager unless they are
   enabled.
routing group connector
   A connector that specifies the connection of a local routing group to a server in a remote
   routing group. It also specifies the local bridgehead server, if any, and the connection cost,
   schedule, and other configuration properties.
   See also: local bridgehead server

S

S/MIME
   See definition for: Secure Multipurpose Internet Mail Extensions
SACL
   See definition for: system access control list
schema
   The data design of a system, often represented as a complete set of properties on the system's
   objects, together with their possible values and rules for their interaction.
Secure Multipurpose Internet Mail Extensions
(S/MIME) A standardized message format for secure e-mail over the Internet. Outlook 98 or later clients can send and receive S/MIME version 2 secure messages without being enrolled in Exchange Advanced Security. Outlook 2000 Service Pack 1 and later versions support S/MIME version 3.

Secure Sockets Layer
(SSL) A communications protocol that provides public key cryptography services to ensure privacy over public networks. It was designed to establish a secure communications channel to prevent the interception of critical information, such as credit card numbers. SSL was developed by Netscape, and the Internet Engineering Task Force (IETF) has now combined SSL with other protocols and authentication methods into a new protocol known as Transport Layer Security (TLS).
See also: Transport Layer Security

security context
An aspect of Windows Server 2003 and Windows 2000 that controls the kind of access a user, process, or service has to system services.

security descriptor
In Windows Server 2003 and Windows 2000, it is possible to set security for objects because every object has a security descriptor. The security descriptor is where the security settings for the object are stored. A security descriptor consists of the security identifier (SID) of the object owner, a group SID used by the Portable Operating System Interface (POSIX) subsystem and Services for Macintosh, a Discretionary Access Control List (DACL), and a System Access Control List (SACL).

security identifier
(SID) A statistically unique number that identifies all users and groups. When a new user or group is created, Windows Server 2003 or Windows 2000 generates a SID for the account. The operating system uses the identifier to verify access permissions when a user requests access to an object, instead of using the user name. Because SIDs are unique, if a user account is deleted and then recreated, the SID is different for the new account. As a result, when the user attempts to access an object they were able to access with their old account, they are denied access. This occurs even if the user name is the same, because the SID that is used to identify the user is different.

server cluster
A group of independent computers that work together to run a common set of applications. The computers are physically connected by cables and programatically connected by cluster software. These connections allow the computers to use problem-solving features, such as load balancing, while appearing to the user and applications as a single system.

service account
A Server 2003 or Windows 2000 user account that is used to run some Exchange services.

SID
See definition for: security identifier
Simple Mail Transfer Protocol
(SMTP) An Internet standard for transporting and delivering electronic messages. Based on specifications in RFC 2821 and RFC 2822, Microsoft SMTP service is included in the Windows Server 2003 and Windows 2000 operating systems. SMTP is the default transport for Exchange 2003.

Site
A Windows Server 2003 or Windows 2000 site consists of one or more reliable and fast TCP/IP subnets. Setting up Windows Server 2003 or Windows 2000 sites allows you to configure Active Directory access and a replication topology to take advantage of the physical network.

Site Replication Service
(SRS) A directory service (similar to the directory used in Exchange 5.5) implemented in Exchange 2003 to allow the integration with downstream Exchange 5.x sites using both remote procedure call (RPC) and mail-based replication. SRS works in conjunction with Active Directory Connector to provide replication services from Active Directory to the Exchange 5.x Directory Service.

Smart host
A designated server through which Exchange routes all outgoing messages. The smart host then makes the remote connection. If a smart host is designated, the Exchange server only needs to transmit to the smart host, instead of repeatedly contacting the domain until a connection is made. Also known as a relay host.

SMTP
See definition for: Simple Mail Transfer Protocol

SRS
See definition for: Site Replication Service

SSL
See definition for: Secure Sockets Layer

Storage group
A collection of mailbox stores and public folder stores that share a set of transaction log files. Exchange manages each storage group with a separate server process.

Synchronization
In networking, a communications transmission in which multibyte packets of data are sent and received at a fixed rate.

System access control list
(SACL) Access control lists in Windows Server 2003 or Windows 2000 that control which events will be audited for the object.

See also: access control list

System Attendant
A core maintenance service included with Exchange.
**system policies**

Policies that apply to server-side objects, such as mailbox stores, public folder stores, and servers.

---

**T**

**TLS**

See definition for: Transport Layer Security

**transaction log file**

A file that maintains a record of every message stored in a storage group and provides fault tolerance in the event that a database must be restored.

**Transport Layer Security**

(TLS) A communications protocol that uses a combination of public key and bulk encryption to provide privacy, authentication, and data integrity.

**trust relationship**

The relationship between two domains that makes it possible for a user in one domain to access resources in another domain.

*See also:* authentication

---

**U**

**Universally Unique Identifier**

See definition for: globally unique identifier

**user**

An Active Directory object that has a Windows security account and a password.

**user class**

A logical collection of chat users whose membership is based on one or more criteria, such as their chat client protocol (for example, Internet Relay Chat or IRC) or their Internet Protocol (IP) address. User classes allow you to protect your chat server and its users from flooding and other types of attacks.
**V**

**virtual directory**
A directory name, used in an address, that corresponds to a physical directory on the server.

**virtual root**
A mapping between a specific path or name and a physical storage location, be it a local file directory network share or redirection to another URL. For HTTP, a virtual root defines a mapping between a URL path and a physical storage location. For NNTP, a virtual root defines a mapping between a newsgroup name and a physical storage location.

**virtual server**
A collection of services that appears to clients as a physical server. It is an instance of a protocol service (for example, Simple Mail Transfer Protocol (SMTP)) with a defined set of Internet Protocol (IP) address/port combinations and an independent collection of configuration properties. A virtual server typically includes all of the resources necessary to run a particular application, including a network name resource and an IP address resource.

**W**

**WebDAV**
An extension of HTTP/1.1 that allows clients to perform remote Web content authoring. Content that is stored on a server can be accessed by a client through the HTTP protocol using WebDAV extensions. The client can perform tasks provided by HTTP, including reading e-mail and documents. If the client also supports WebDAV, the client can manipulate mail, change calendar appointments, modify and create new documents on the Exchange 2003 server, and create Web-based forms. WebDAV uses XML as the format for transmitting data elements.

**Web Storage System**
See definition for: Exchange store
**X**

**X.400 Connector**
An Exchange Server component that is integrated with the message transfer agent (MTA) and can be configured to connect routing groups within Exchange, or to route messages to foreign X.400 systems. When handling communication between Exchange and foreign X.400 systems, it maps addresses and converts Exchange messages to native X.400 messages and vice versa.

*See also:* message transfer agent

---

**Y**

No glossary entries.

---

**Z**

No glossary entries.
Does this book help you? Give us your feedback. On a scale of 1 (poor) to 5 (excellent), how do you rate this book?

Mail feedback to exchdocs@microsoft.com.

For the latest information about Exchange, see the following Web pages:

- Exchange Product Team technical articles and books
  http://www.microsoft.com/exchange/library

- Exchange Tools and Updates

- Self-extracting executable containing all Exchange Product Team technical articles and books