

Maintenance and Troubleshooting

Microsoft Exchange Server

Version 5.5

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Microsoft Corporation. If, however, your only means of access is electronic, permission to print one copy is hereby granted.

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.

© 1997 Microsoft Corporation. All rights reserved.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the USA and other countries.

Macintosh is a registered trademark of Apple Computer, Inc.

Other products and company names mentioned herein may be the trademarks of their respective owners.

Contents

Before You Begin xi

Microsoft Exchange Server Documentation xi

About This Guide xiii

Document Conventions xiii

Chapter 1 Understanding System Maintenance Concepts 1

System Maintenance 1

Planning Maintenance 2

Performing Maintenance 2

Monitoring Performance 2

Performing Trend Analysis 3

Diagnosing and Correcting Problems 3

Evaluating the Organization's Changing Needs 3

Disaster Recovery Strategies 4

Performing Backups 4

Implementing a Disaster Recovery Plan 4

Using a Dedicated Recovery System and Recovery Toolkit 5

Using a Dedicated Recovery System 5

Creating a Recovery Toolkit 6

Training Administrators 6

Considering Server Design and Configuration to Prevent Disasters 6

Chapter 2 Maintaining Your Organization 7

Backup and Restore 7

Implementing a Backup Plan 8

Understanding Transaction Log Files 8

Using Circular Logging 9

Choosing Backup Devices 9

Choosing a Backup Routine 10

Performing Timely Backups 11

Verifying and Validating Backups	12
Documenting and Archiving Backups	12
Backing Up a Server	12
Starting an Online Backup	13
Performing an Offline Backup	14
Automating a Backup	14
Using Command-line Batch Files	14
Validating an Information Store Backup	15
Restoring a Server	15
Restoring an Information Store to the Same Server	16
Restoring an Information Store to a Different Server	17
Restoring Data for a User	18
Restoring from an Offline Backup	18
Restoring Information After a Catastrophe	18
Starting Services Using Backup	19
Message Transfer Agent (MTA)	19
MTA Routing Table	20
Rebuilding the Routing Table	21
MTA Queues and Message Information	21
MTA Diagnostics Logging	21
Microsoft Mail Connector	22
Information Store	22
Status Information	22
Modifying Columns for Information Store Status Items	23
Viewing Logons	24
Viewing Mailbox Resources	25
Viewing Folder Replication Status	27
Viewing Public Folder Resources	28
Viewing Server Replication Status	29
Maintenance Schedule	31
Setting the Maintenance Schedule	32
Directory	33
Directory Consistency	33
Verifying Directory Consistency	34
Resynchronizing Replicated Directory Information	35
Directory Diagnostics Logging	35
Mailbox Maintenance	35
Setting Age Limits	36
Setting the Sensitivity Level	37

Specifying Read Items	37
Deleting Other Information	38
Setting the Action Level	38
Administrator Window Contents	38
Saving the Window Contents	39
File Content Options	39
Selecting Separators and Character Sets	40
Directory Export and Import	41
Using Directory Export	42
Using the Directory Export Command	42
Using Command-line Directory Export Options	43
Using Directory Import	44
Using the Directory Import Command	44
Using Command-line Directory Import Options	45
Selecting a Separator	47
Quoting Behavior for Multivalued Properties	47
Chapter 3 Monitoring Your Organization	49
Link Monitor	49
Link Monitor Configuration	50
General Properties	50
Defining the Directory Name and the Display Name	51
Creating Log Files	51
Setting Polling Intervals	52
Permissions	52
Warning and Alert Durations	52
Specifying a Warning State Duration	53
Specifying an Alert State Duration	53
Notification Process	54
Using Notification Applications	55
Using Mail Messages	57
Using Network Alerts	58
Modifying a Notification	59
Removing a Notification	59
Link Monitoring Within an Organization	59
Specifying Servers for Link Monitoring	60
Removing Servers from Link Monitoring	60
Link Monitoring Outside an Organization	61
Specifying Recipients That Return Subjects	63

Specifying Recipients That Return the Subject or Message Body	63
Link Status	63
Viewing the Last Received Bounce Mail Details	64
Link Notification	65
Link Maintenance Status	66
Viewing the Maintenance Status Details	67
Server Monitor	67
Server Monitor Configuration	68
General Properties	69
Defining the Directory Name and the Display Name	69
Creating Log Files	69
Setting Polling Intervals	70
Permissions	70
Notification Process	70
Using Notification Applications	72
Using Mail Messages	73
Using Network Alerts	74
Modifying a Notification	74
Removing a Notification	75
Server Monitoring Within an Organization	75
Specifying Servers for Monitoring	76
Removing Servers from Monitoring	76
Escalation Actions	76
Specifying Escalation Actions	77
Specifying the Restart Delay	77
Clock Synchronization	78
Setting Up Alerts	78
Setting Up Clock Synchronization	79
Server Status	80
Changing the Component Status	81
Server Clock Synchronization	81
Server Notification	83
Server Maintenance Status	84
Services to Monitor	84
Adding a Service	85
Removing a Service	85
Manual Monitor Startup and Shutdown	86
Starting Monitors Manually	86
Pausing Monitors	87

Windows NT Performance Monitor	88
Windows NT Performance Monitor Counters	88
Windows NT General Performance Monitor Counters	89
Microsoft Exchange Server Performance Monitor Counters	89
Monitoring the Message Transfer Agent	90
Monitoring the Directory	90
Monitoring the Information Store	91
Monitoring the Microsoft Mail Connector	92
Monitoring the Internet Mail Service	92
Monitoring the Microsoft Exchange Connector for Lotus cc:Mail	94
Automatic Logon and Startup	95
Logging On to Windows NT Server Automatically	95
Starting Link and Server Monitors Automatically	96
Starting Performance Monitor Automatically	97

Chapter 4 Troubleshooting Tools and Resources 99

Link Monitor	99
Connection Status	100
Interpreting a Link Monitor Display	100
Link Monitor Logs	101
Connection Problems	102
Troubleshooting Your Link Monitor	103
Server Monitor	104
Server Status	1024
Interpreting a Server Monitor Display	105
Server Monitor Logs	106
Windows NT Performance Monitor	106
Windows NT Event Viewer	107
Searching Event Logs	108
Diagnostics Logging	108
Microsoft Exchange Server Components	109
Microsoft Exchange Server Connectors	110
Diagnostics Logging Categories	111
Understanding the Diagnostics Logging Property Page	111
Changing the Diagnostics Logging Level	112
MTA	112
Changing MTA Diagnostics Logging Levels	113
Creating Interoperability Logs	113
Creating APDU Logs	114

Information Store Events	115
Changing Information Store Logging Levels	116
Using Diagnostics Logging of the Information Store	117
Internet Mail Service	117
Changing Internet Mail Service Logging Levels	118
Logging SMTP Information	119
Interpreting an SMTP Protocol Log	119
Creating a Message Archive	120
Microsoft Mail Connector	120
Changing Microsoft Mail Connector Logging Levels	122
Microsoft Schedule+ Free/Busy Connector	122
Changing Schedule+ Free/Busy Connector Logging Levels	123
Microsoft Exchange Connector for Lotus cc:Mail	124
Microsoft Exchange Server Computer	124
Changing Logging Levels	125
Message Tracking	125
Enabling Message Tracking	126
Enabling Message Tracking on MTAs or the Information Store	126
Enabling Message Tracking on a Microsoft Mail Connector	127
Enabling Message Tracking on the Internet Mail Service	127
Performing Message Tracking	128
Starting Message Tracking	128
Displaying Message Detail	130
Using the Message Tracking Center	131
Searching for Microsoft Exchange Server Messages	132
Searching Outside of an Organization	133
Searching by Message ID	136
Interpreting a Message Track	137
Tracking Log	137
Interpreting Tracking Log Fields	138
Interpreting Events	139
Message Queues	141
MTA Queues	142
Viewing Message Detail	143
Refreshing the Queue Property Page	144
Changing Message Order	144
Deleting Messages	145
Using MTA Message Queues for Troubleshooting	145
Internet Mail Service Queues	146

Selecting a Queue	147
Viewing Message Detail	148
Refreshing the Queues Property Page	149
Deleting Messages	149
Forcing a Retry	150
Using Internet Mail Service Queues for Troubleshooting	150
Microsoft Mail Connector Queues	151
Selecting a Queue	152
Refreshing the Queue	153
Returning Messages	153
Deleting Messages	154
Using Microsoft Mail Queues for Troubleshooting	154
Troubleshooting Utilities	154
MTACHECK	154
Running MTACHECK	155
Interpreting MTACHECK Output	155
Searching Message Logs by Message ID	156
ISINTEG	157
Checking the Tables	157
Patching the Information Store	158
SNMP Monitoring Agents	159
MIB Installation for Microsoft Exchange Server	160
Using the Batch File	160
Using Perf2mib.exe and Mibcc.exe	160
MIB Viewing	161
Understanding Microsoft Exchange Server Object IDs	161
Using the Snmputil Utility	162
Performance Monitor Counters	163
Other Tools and Resources	165
Other Tools	165
Other Resources	166

Chapter 5 Troubleshooting Your System 167

Addressing	167
Administrator Program	169
Clients	171
Connections Between Microsoft Exchange Servers	173
Directory	174
Directory Synchronization	175

Internet Mail Service	177
Microsoft Exchange Server Performance	181
Microsoft Exchange Server Setup	182
Microsoft Mail Connector	182
Non-Delivery Reports	185
Public Folders	187
Internet News Service	189
Sending Mail	189
X.400 Connections	192
Appendix A Diagnostics Logging	195
Directory Service	196
Directory Synchronization	197
Information Store	197
Critical Event Categories	202
Internet Mail Service	202
KM Server	203
MTA	203
Microsoft Exchange Connector for Lotus cc:Mail	204
Microsoft Mail Connector	205
Microsoft Schedule+ Free/Busy Connector	206
IMAP4	206
NNTP	207
POP3	207
Index	209

Before You Begin

After you set up Microsoft® Exchange Server, it is important to maintain your system to ensure optimal performance and reliability. *Microsoft Exchange Server Maintenance and Troubleshooting* provides comprehensive information about monitoring and troubleshooting Microsoft Exchange Server. It includes instructions for using Microsoft Exchange Server tools and Windows NT® tools, as well as those from other sources that you can use to resolve problems with Microsoft Exchange Server.

This book is accessible from the **Help** menu in the Administrator program. It is also available separately as a printed book from Microsoft.

Microsoft Exchange Server Documentation

Microsoft Exchange Server provides comprehensive print and online product documentation. You can install the online books described in this section from the Microsoft Exchange Server compact disc during Setup. You can also order printed versions of many of the books by using the coupon provided in *Microsoft Exchange Server Getting Started*. The following documentation is available for Microsoft Exchange Server.

Microsoft Exchange Server Concepts and Planning Presents an overview of the product features and concepts needed for planning a Microsoft Exchange Server organization. Administrators should read this book before setting up Microsoft Exchange Server.

This book is accessible from the **Help** menu in the Administrator program. It is also available separately as a printed book from Microsoft.

Microsoft Exchange Server Getting Started Presents the basic information needed to get a Microsoft Exchange Server system running in a typical organization. It provides a brief overview of the product and instructions for installing the server component of Microsoft Exchange Server. The guide also describes how to perform basic Microsoft Exchange Server tasks, such as creating mailboxes and using public folders, and provides product support information.

This book is provided with Microsoft Exchange Server as a printed document. It is also accessible from the **Help** menu in the Administrator program.

Microsoft Exchange Server Operations Provides step-by-step instructions for administering Microsoft Exchange Server, including how to set up and configure Microsoft Exchange Server sites, servers, mailboxes, and connectors. It also provides comprehensive information about using the Microsoft Exchange Server Administrator program.

This book is accessible from the **Help** menu in the Administrator program. It is also available separately as a printed document from Microsoft.

Microsoft Exchange Server Migration Describes concepts for migrating from foreign systems to Microsoft Exchange Server. It also provides instructions for using migration tools to move users from systems such as Microsoft Mail for PC Networks and Microsoft Mail for AppleTalk Networks (also known as Quarterdeck Mail) to Microsoft Exchange Server.

This book is accessible from the **Help** menu in the Administrator program.

What's New: Microsoft Exchange Chat Service Describes the new features available with Microsoft Exchange Chat Service. These new features include new administrative commands, extensions to the Internet Relay Chat (IRC) protocol, security enhancements, and improved server performance and scalability.

This book is accessible from the **Help** menu in the Administrator program.

Microsoft Exchange Chat Service Operations Provides instructions for installing, configuring, and administering Microsoft Exchange Chat Service. It explains how Chat Service works and offers guidelines for automating server operation and improving performance. This guide also describes the administrative tools available in Chat Service and includes a comprehensive command reference for the **chatcmd** utility.

This book is accessible from the **Help** menu in the Administrator program.

Online Help Provides online information for the Microsoft Exchange Server Administrator program. You can access Help from the **Help** menu or by pressing F1.

Online Documentation Set Provides Microsoft Exchange Server books online as a Hypertext Markup Language (HTML) file. They are automatically installed during Microsoft Exchange Server Setup and can be accessed from the **Help** menu in the Microsoft Exchange Server Administrator program. You can also access these books from the **Start** menu by choosing **Programs, Microsoft Exchange**, and **Books Online**.

Technical Support Information For technical support information, see *Microsoft Exchange Server Getting Started*.

About This Guide

This book is organized into the following chapters and appendix.

Chapter 1 “Understanding System Maintenance Concepts” Provides an overview of creating a backup plan, maintenance plan, and disaster recovery plan to ensure the optimal performance of your Microsoft Exchange Server system.

Chapter 2 “Maintaining Your Organization” Describes maintenance tasks you need to perform to keep Microsoft Exchange Server message and information transfer running smoothly.

Chapter 3 “Monitoring Your Organization” Explains how to check for problems with services, servers, connections, and gateways.

Chapter 4 “Troubleshooting Tools and Resources” Describes Microsoft Exchange Server and Windows NT tools you can use to diagnose and troubleshoot problems in your Microsoft Exchange Server organization.

Chapter 5 “Troubleshooting Your System” Explains how to use the available tools and resources to narrow down a problem in a specific Microsoft Exchange Server component, find the cause, and then solve the problem.

Appendix A “Diagnostics Logging” Describes events written to the Windows NT application event log by Microsoft Exchange Server services and components.

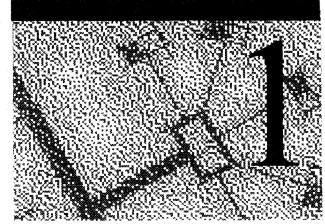
Document Conventions

To help you locate and interpret information easily, *Microsoft Exchange Server Maintenance and Troubleshooting* uses the following conventions.

Convention	Description
ALL CAPITALS	Acronyms and names of certain commands.
Bold	Menus and menu commands, command buttons, property page and dialog box titles and options, command-line commands, options, and portions of syntax that must be typed exactly as shown.
Initial Capitals	Names of applications, programs, files, servers, and named windows; and directory names and paths.
<i>Italic</i>	Information you provide, terms that are being introduced, and book titles.
Monospace	Examples, sample command lines, program code, and program output.
SMALL CAPITALS	Names of keys on the keyboard.

CHAPTER 1

Understanding System Maintenance Concepts



Microsoft Exchange Server provides a way for your organization to manage business-critical and day-to-day information flow and communications. Maintenance is essential to the high-quality performance of your messaging system. Failure to perform system maintenance can cause performance degradation and increase the risk of disasters, such as server failures and the loss of critical data.

The best way to ensure optimal performance of your system is to develop a backup plan, a maintenance plan, and a disaster recovery plan.

System Maintenance

The reliability of your messaging system depends on keeping it maintained. Proper maintenance ensures that problems don't result in downtime. Designing a process to maintain a high-quality system includes:

- Planning maintenance.
- Performing maintenance.
- Monitoring performance.
- Performing trend analysis.
- Diagnosing and correcting problems.
- Evaluating the organization's changing needs.

Planning Maintenance

Putting together an effective maintenance plan includes:

- Developing maintenance guidelines and procedures.
- Scheduling and tracking maintenance to ensure all requirements are met.
- Documenting completed maintenance to create a historical record.
- Developing topology maps to identify all the major components in your messaging environment.
- Designing and configuring the system so that duplicate components can continue to operate during maintenance downtime.
- Training administrators on maintenance guidelines and procedures.

Performing Maintenance

Tasks you should routinely complete to ensure reliability of your Microsoft Exchange Server include:

- Maintain the information store.
- Verify replicated directory information.
- Allocate information store resources.
- Perform backups.
- Move mailboxes and public folders.
- Create, modify, and remove mailboxes.
- Clean mailboxes.
- Create, modify, and remove e-mail addresses.
- Make batch changes to mailboxes, distribution lists, and custom recipients.

Monitoring Performance

Do the following to ensure that Microsoft Exchange Server continues to perform reliably:

- Monitor server performance making sure it is optimized.
- Monitor message transfers by the message transfer agent (MTA), connectors, and gateways to ensure messages are routed appropriately and to eliminate bottlenecks.
- Monitor statistics for Microsoft Exchange Server components to ensure that server resources are being used appropriately.
- Monitor directory and public folder replication to ensure that directories and public folders are replicated and synchronized correctly.

Performing Trend Analysis

Trend analysis is evaluating historical trends in system performance data to identify and diagnose problems as they develop and identify the changing needs of your organization.

You should configure and use Windows NT Performance Monitor to identify trends. Based on these trends, you can add system resources or reconfigure the system to meet the changing needs of your organization.

For information about using Performance Monitor, see Chapter 3, “Monitoring Your Organization,” and your Windows NT documentation.

Diagnosing and Correcting Problems

Microsoft Exchange Server and Windows NT Server provide the following tools and resources to help you diagnose and correct common problems:

- Use Windows NT Performance Monitor and event logs to view system data.
- Use diagnostics logging to gather information about problem areas.
- Use message tracking to help gather information about message transfer problems.
- Use message queue property pages to view queues, change message priorities, and delete messages.

For information about diagnosing and correcting problems, see Chapter 4, “Troubleshooting Tools and Resources,” and Chapter 5, “Troubleshooting Your System.”

Evaluating the Organization’s Changing Needs

As the needs of your organization change, a maintenance process ensures the system is reconfigured and resources are added appropriately. For example, many new users are added to your system each week and message traffic is increasing rapidly. By performing trend analysis, you can anticipate load imbalances and message bottlenecks and then adjust routing costs and add more servers, information stores, and connectors.

Disaster Recovery Strategies

Disasters can occur to your messaging system and cause you to lose key components or critical data. Disasters range from losing the information store because your hard disk failed to losing an entire data center during an earthquake.

The following tasks can help you recover from disasters and minimize downtime and productivity losses:

- Perform timely backups.
- Implement a disaster recovery plan.
- Use dedicated recovery systems and recovery toolkits.
- Train administrators to implement the disaster recovery plan.
- Consider server design and configuration to prevent disasters.

Performing Backups

The most important thing you can do to ensure recovery from disasters is to perform timely backups. Your backup strategy should include choosing a backup program and performing and verifying backups.

For more information about performing backups, see Chapter 2, “Maintaining Your Organization,” and your Windows NT Server documentation.

Implementing a Disaster Recovery Plan

You can develop procedures to recover from common disasters, such as hardware failure or corrupt directories and information stores.

You can also develop contingency plans to recover from major disasters, such as fires, hurricanes, and earthquakes. The plan your organization needs depends on your location. For example, an international organization with facilities in California should develop contingency plans for earthquakes and the potential loss of facilities and services. The plan could require reserve capacity and duplicate services in facilities in Colorado, England, or Japan. As a result, when an earthquake occurs in California, the system continues to operate normally for the rest of the organization.

Using a Dedicated Recovery System and Recovery Toolkit

You can use dedicated recovery systems and disaster recovery kits to increase your organization's ability to recover from disasters and to minimize the recovery time.

Using a Dedicated Recovery System

A dedicated recovery system enables prompt recovery because it is available when a disaster occurs. A dedicated recovery system can be one or more Microsoft Exchange Server computers that are used only when a disaster occurs. Dedicated recovery servers are connected to the network, but are not members of a site until needed.

If your organization does not have a dedicated recovery system, recovery efforts can involve locating the necessary server hardware and software, installing the server, and configuring the server for recovery. Even if you have the equipment on site, installing and configuring the recovery server is time consuming. A small organization may need only one dedicated recovery system, whereas a larger organization may need several.

A dedicated recovery system includes:

- Sufficient capacity for the server file system, directory, and information stores.
- Windows NT Server installed as a primary domain controller (PDC), backup domain controller (BDC), or member server.
- A storage device that is compatible with the storage device used for backing up the production system.
- Microsoft Exchange Server installed but no sites configured.

When a mailbox or information store is corrupted, you can use backups to recover the information store to a dedicated recovery server and then restore the mailbox or information store to the production server. When a server fails, you can use backups to restore the server's information store, directory, and configuration to a recovery server and then place the recovery server in production to replace the failed server.

The requirements and procedures for disaster recovery vary widely depending on your system configurations and the circumstances. For more information, visit <http://www.microsoft.com/exchange>.

Creating a Recovery Toolkit

You can create a recovery toolkit to ensure all needed materials are available when a disaster occurs. A recovery kit can include:

- Operating system configuration sheets.
- EISA/Micro Channel Architecture (MCA) configuration disks.
- Redundant array of inexpensive disks (RAID) configuration sheets.
- Hardware configuration sheets.
- Microsoft Exchange Server computer configuration sheet.
- Windows NT emergency repair disk.
- Microsoft Exchange Server Performance Optimizer settings sheet.

Training Administrators

You should implement a program to train administrators on disaster recovery plans. This program can include qualification training on disaster recovery procedures and periodic drills simulating disaster recovery scenarios.

Considering Server Design and Configuration to Prevent Disasters

The following practices can help reduce the risk and impact of disasters:

- Install servers in adequate, safe, and secure environments.
- Avoid making a Microsoft Exchange Server computer a PDC.
- Maintain transaction log files for the directory and information stores on separate hard disks.
- Use hardware RAID Level 5 and mirroring.
- Protect servers with uninterruptible power supplies (UPS).
- Turn off circular logging.
- Document all server configurations and keep a record of changes.
- Equip servers with sufficient hard disk space to allow for recovery.

For more information about server design and configuration considerations, see *Microsoft Exchange Server Concepts and Planning*, or visit <http://www.microsoft.com/exchange>.

Maintaining Your Organization



Maintaining Microsoft Exchange Server consists of periodically verifying that:

- Messages are being transferred correctly and in a reasonable amount of time by the message transfer agent (MTA), connectors, and gateways.
- The information store is working correctly and providing adequate resources and performance to users.
- The directory is working correctly, and directory replication and synchronization are sharing the correct information.
- You have a recent backup for each server's directory and information store.

The maintenance tasks outlined in this chapter provide basic procedures for keeping message and information transfer running smoothly. You may need to perform additional tasks depending on the design of your organization.

Backup and Restore

You can use Windows NT Backup to back up and restore Microsoft Exchange Server directories and information stores within your organization. The Backup program enables you to protect data from accidental loss or hardware and media failures by using a tape drive to back up and restore information located on any server in any site in your organization locally or over the network.

During backup, users can continue to use the server. When information is being restored, Microsoft Exchange Server services stop and users cannot use the servers until after they have been restored.

For more information about Windows NT Backup, see your Windows NT Server documentation.

Implementing a Backup Plan

It is important to perform backups to protect your organization's information and messaging system. Your backup plan should include:

- Choosing backup devices.
- Choosing a backup routine.
- Performing timely backups.
- Verifying and validating backups.
- Documenting and archiving backups.

Understanding Transaction Log Files

Windows NT Backup backs up the Microsoft Exchange Server directory and information stores differently from normal file system backups. To understand how directory and information store backups work, it is important to understand how transaction log files work.

Microsoft Exchange Server uses write-ahead transaction log files to improve server data write performance and to provide fault tolerance for the directory and information stores. Data for the directory or information store is written synchronously at high speed to a sequential transaction log file and to a memory cache simultaneously. The data in the cache is later written to the directory database or the information store database files as necessary. When a log file has 5 megabytes (MB) of transactions, a new log file is generated. Log files are named with hexadecimal serial numbers.

Note The size of log files is always 5 MB, so you can't determine whether a log file is filled to capacity by checking the file size.

If a power outage or abnormal system shutdown occurs before the data in the cache is written to the database, Microsoft Exchange Server reconstructs the database upon restarting by reading from the transaction log files. If a directory or information store database becomes corrupted, the transaction log files remaining on the hard disk can be used to reconstruct the database from a backup if an uninterrupted sequence of transaction log files exist from the time of the backup.

Normally, transaction log files accumulate sequentially until a full or incremental backup is performed, which deletes log files that have all transactions committed to the database. Differential backups back up the transaction log files but leave the log files on the hard disk.

Using Circular Logging

Circular logging recycles transaction log files by overwriting logs that have been committed to the database with new transactions. This prevents the continuous buildup of transaction log files and reduces the disk space required to store them (typically less than 100 MB). By default, circular logging is turned on in Microsoft Exchange Server. However, you can use the **Advanced** property page on the server object to turn off circular logging for the directory and information store.

When developing your backup plan, you should consider the implications of using circular logging. Because circular logging overwrites transaction log files, it reduces your ability to recover data. In most cases, you should turn off circular logging to increase your backup options and your ability to recover data.

With circular logging turned on, you can restore information only up to the last full backup—not to the last transaction. When circular logging is turned on, you can only perform full backups, not incremental or differential backups. This is because Windows NT Backup relies on having complete transaction log files to perform incremental and differential backups of the directory and information store databases.

You may want to keep circular logging turned on for some configurations. For example, you could keep circular logging turned on because your server computer has limited hard disk space or because the server is being used as a news server that contains only noncritical data.

For more information about circular logging, see *Microsoft Exchange Server Getting Started*.

Choosing Backup Devices

You should choose backup devices and reliable backup media that best meet the needs of your organization. In addition, you should choose reliable backup media that best meets your needs. For example, you should choose a tape drive that is large enough and fast enough to efficiently support the amount of data you need to back up. Most storage device manufacturers publish recommended media brands that have been tested and certified on their storage devices. Media reliability reports are also available from many computer trade publishers.

Choosing a Backup Routine

Backup routines include full (normal), incremental, and differential. Most organizations use a combination of these routines.

A *full (normal) backup* backs up the entire directory or information store. It also backs up the transaction log files and deletes those transaction log files that have all transactions committed to the database. Restoring from a full backup requires only the full backup.

An *incremental backup* backs up data in the directory or information stores that has changed since the last full or incremental backup. It also backs up the transaction log files and then deletes those that have all transactions committed to the database. Restoring from an incremental backup requires the last full backup and each incremental backup that has taken place since then.

A *differential backup* backs up data in the directory or information stores that has changed since the last full backup. It also backs up the transaction log files, but does not delete them. Restoring from a differential backup requires the last full backup and the differential backup.

Backup Type	Advantages	Disadvantages
Full (Normal)	Easy to schedule.	Can affect server performance.
	Easy to restore data.	Consumes more time.
	Removes transaction log files.	Requires the most tape space and frequent tape replacement.
	Allows circular logging.	
Incremental	Minimal effect on server performance.	Requires a more complex restore process.
	Removes transaction log files.	Circular logging must be turned off.
	Requires minimal tape space.	
Differential	Minimal effect on server performance.	Does not remove transaction log files.
	Easy to restore data.	Circular logging must be turned off.
	Requires minimal tape space.	Requires more tape space than an incremental backup but less than a full backup.

Determining Factors You should consider the following factors when choosing a backup routine:

- Time required to perform the backup.
- Performance impact on servers.
- Amount of data to back up.
- Tape drive capability and capacity.
- Personnel resources required to administer and perform backups.
- Value, priority, and security of the data to be saved.

Full daily backups may be feasible if you're backing up a small amount of data, but not if you're backing up a large amount of data.

Backup Rotations Most organizations rotate full backups with differential or incremental backups. A daily rotation requires full backups every day. A weekly rotation requires one full backup followed by either differential or incremental backups on the remaining days of the week. A three-day backup rotation requires a full backup followed by two days of either differential or incremental backups.

Note Mixing differential and incremental backups in the same weekly backup set is not recommended because the rotation and restore process becomes too complicated.

The following chart illustrates several backup rotations.

Sample Backup Rotations

F = Full, I = Incremental, D = Differential							
Rotation	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Daily	F	F	F	F	F	F	F
Weekly	F	I or D	I or D	I or D	I or D	I or D	I or D
3-day	F	I or D	I or D	F	I or D	I or D	Repeat cycle

Performing Timely Backups

Timely backups include:

- Periodic backups of the entire server file system offline (including the Windows NT Registry) to preserve changes to the server's configuration.
- Daily backups of the directory and information store online using the appropriate backup rotation.

Verifying and Validating Backups

Your ability to recover servers and restore data depends on the quality of your backups. Therefore, you should always use the Verify feature of the Backup program when making backups. Also, periodically perform restores from backups to nonproduction servers to ensure that the backup process is working. Routinely review the daily backup logs to ensure that backups have been completed as scheduled. Follow up on any errors or inconsistencies in the backup logs.

Documenting and Archiving Backups

Before you can restore data, you need to know the backup strategy, including the backup types and the rotation. It is important to document the backup strategy and provide guidelines on how backups can be used to restore data. Label backups carefully and store them in a safe and secure location. For maximum reliability, archive full backups to a different location, preferably offsite.

Tip You can use the Windows NT Backup command **Copy** option to create full backups without disturbing the state of ongoing incremental or differential backups. You should consider creating periodic copy backups and adding them to your archives to provide more protection. For example, you could create and archive duplicate copy backups once a month and after changing server configurations significantly.

Backing Up a Server

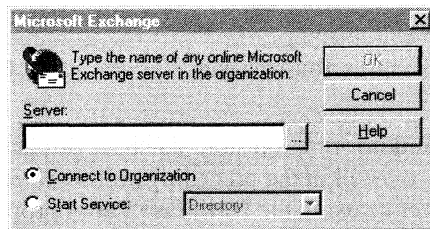
You can back up a server to any tape device compatible with Windows NT Server. The tape drive must be directly connected to the computer running the Backup program, but the server you are backing up can be anywhere on the network.

Note To back up configuration settings that may not be recorded in the directory, you can use the Backup program to back up the registry on the Microsoft Exchange Server computer. For more information, see your Windows NT documentation.

Starting an Online Backup

You can perform an online or offline backup of Microsoft Exchange Server directory and information store databases. However, it is recommended that you perform only online backups to minimize system downtime.

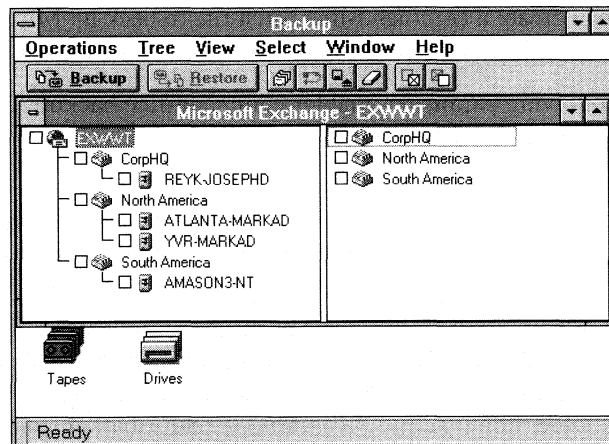
1. From the Start menu, choose Programs, and then choose Administrative Tools.
2. Choose **Backup**.
3. If your Microsoft Exchange Server organization and server are not displayed, from the **Operations** menu, choose **Microsoft Exchange**, and then type the name of any Microsoft Exchange Server computer in the organization.
4. Choose **Connect to Organization**, and then choose **OK**.



5. Select the sites you want to back up.

If the site or server is not displayed in the **Backup** window, double-click the organization and site containers and display their contents.

6. In each site container, select the servers you want to back up.
7. In each server container, select the component to back up.
8. Choose **Backup** to start the backup.



Performing an Offline Backup

To perform an offline backup of a Microsoft Exchange Server database, you must stop the service you're backing up and then back up individual databases.

The following table shows the Microsoft Exchange Server database files and default directories.

Component	File	Directory
Directory	Dir.edb	Exchsrvr\Dsadata
Private information store	Priv.edb	Exchsrvr\Mdbdata
Public information store	Pub.edb	Exchsrvr\Mdbdata
Microsoft Mail directory synchronization	Xdir.edb	Exchsrvr\Dxadata
KM Server	Kmsmdb.edb	Exchsrvr\Kmsdata

Note The directory and information store database directories on your server may be different from those listed in the preceding section if you changed them using Performance Optimizer or using the **Database Paths** property page on the server object.

Automating a Backup

You can use the At.exe utility provided with Windows NT to schedule times when backups are automatically performed. This utility can also be used to schedule a backup on another Microsoft Exchange Server computer.

Using Command-line Batch Files

You can create a command-line batch file to back up Microsoft Exchange Server components. For more information, see your Windows NT documentation.

The following parameter enables command-line backups of the Microsoft Exchange Server databases:

path

If you are backing up Microsoft Exchange Server components, specifies the component and the server using the following format:

{DS *server* | IS *server*}

Where *server* is the name of the server you are backing up preceded by two backslashes (for example, \\berkeley). DS indicates that you are backing up the directory, and IS indicates that you are backing up the information store. For example, to back up the information store, use IS \\berkeley.

The following example would back up the directory and information store on Server_A and the directory on Server_B, validate the backup (/v), using a normal backup type (t:normal).

Ntbackup backup DS \\Server_A IS \\Server_A DS \\Server_B /v /t:normal

Validating an Information Store Backup

To ensure that your information store is being backed up correctly and no information is lost, restore a server from tape backup to another nonproduction server and verify that you can log on to mailboxes and public folders on the restored server.

1. Restore the information store from tape backup to a nonproduction Microsoft Exchange Server computer as described in “Restoring a Server” later in this chapter.
2. In the Administrator program, select a mailbox account to view mail, and give yourself Mailbox Owner permission on that account.
3. Create a client profile and log on to the mailbox. Check to see that mail is there, and send a message to yourself to verify delivery.
4. In the Administrator program, view the **Mailbox Resources** property page on the private information store object to verify the total kilobytes per user.

Restoring a Server

Once you have backed up your Microsoft Exchange Server computer, you can restore it in the event of lost data or a catastrophe or to validate your backup. When restoring information, Microsoft Exchange Server services stop, and users cannot use them until the server is restored.

Restoring an Information Store to the Same Server

Use the following procedure to restore an information store on the same server it was backed up from.

1. From the **Start** menu, choose Programs, and then choose Administrative Tools.
2. Choose **Backup**.
3. In the **Tapes** window, select the sets that you want to restore.
4. Choose **Restore**.

Option	Description
Erase all existing data	Erases all data on the server pertaining to the database being restored. This option must be selected when you want to delete database information currently on the hard disk.
Private	You must select both Private and Public , even if the backup contains only one of these databases.
Public	You must select both Private and Public , even if the backup contains only one of these databases.
Start Service After Restore	Starts the directory or information store service after the restore is finished.
Verify After Restore	Verifies the contents of the files restored to disk from the files on tape, and logs any exceptions.
Destination Server	The server that the backup will be restored to.

Restoring an Information Store to a Different Server

You can restore an information store to a Microsoft Exchange Server computer that is different from the one you backed up. This enables you to recover individual items (messages or folders) from a backup without restoring over a server that is in use. This is a last-resort method for retrieving items from individual mailboxes or public folders. It requires an additional computer that has enough hard drive disk space to restore the entire backup and that meets the hardware requirements to run a Microsoft Exchange Server computer. The alternate server cannot replicate its directory with the existing organization.

Warning If you type your production server name as the destination server name in the **Restore Information** dialog box, you will restore over your production server.

1. Set up Microsoft Exchange Server on the alternate server with the same organization and site name as the tape being restored, but *do not* add this server to an existing site during Setup.
2. Using Windows NT Backup, restore the information store, and type the alternate server name for the destination server in the **Restore Information** dialog box.
3. Select the following check boxes.
 - **Erase all existing data**
 - **Private**
 - **Public**

You must select both **Private** and **Public**, even if the backup contains only one of these databases.

4. Start the services on the alternate server. This can be done automatically by selecting **Start Service after Restore** in step 2.
5. In the Administrator window, locate the **DS/IS consistency adjustment** in the **Advanced** property page of the server object. Choose **All Inconsistencies**, and then choose **Adjust**.

Restoring Data for a User

If you've set a deleted item retention period on a mailbox or private information store, users can easily restore messages after they've been deleted from their mailbox. For more information about setting a deleted item retention period on a user's mailbox, see *Microsoft Exchange Server Getting Started*.

If you haven't set a deleted item retention period, you can recover deleted messages by restoring the information store from tape backup to an alternate server and performing the following steps.

1. Select a mailbox account to view mail, and then give yourself Mailbox Owner permission for that account.
2. Log on to the client, and then move the data to a personal folder (.pst) file. Give the .pst file to the user.

Restoring from an Offline Backup

To restore a directory or information store from a backup that was performed while the server was offline, you must first stop the Microsoft Exchange Server services on the server being restored.

Note After you restore an information store from an offline backup, run **ISINTEG** using the **-patch** switch, restart the services, and then run the DS/IS consistency adjustment tool.

Restoring Information After a Catastrophe

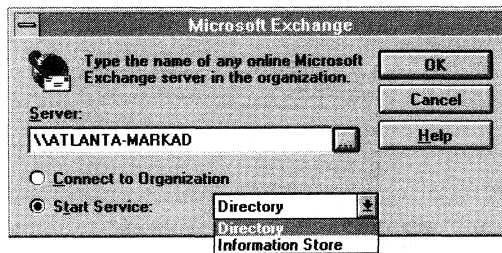
If a server is catastrophically destroyed, the information must be restored from a backup.

1. Install Windows NT on the new or repaired server. It may be necessary to delete the Windows NT computer account for the server and re-create it by using Windows NT Server Manager.
2. Install Microsoft Exchange Server on the new or repaired server by running **Setup /r**. Do not replicate it with the existing organization. Give the server its original organization and site name.
3. Restore the directory from the last backup for that server.
4. Restore the private/public information store from the last backups for that server.
5. Run the DS/IS consistency adjustment tool. For more information, see *Microsoft Exchange Server Getting Started*.

Starting Services Using Backup

You can use the Backup program to start Microsoft Exchange Server services. For example, you can restart services after you've restored a database from tape backup. This feature is useful when restoring remote Microsoft Exchange Server computers.

1. From the **Operations** menu in the **Backup** window, choose **Microsoft Exchange**.
2. In the **Server** box, type the name of the server that you want to start services on.
3. Select **Start Service**.
4. Select **Directory** or **Information Store**.



Option	Description
...	Displays the available Microsoft Exchange Server computers.
Connect to Organization	Opens an organization window so you can select a Microsoft Exchange Server computer in your organization.
Start Service	Starts the specified service on the server.

Message Transfer Agent (MTA)

The MTA submits, routes, and delivers messages to other MTAs, information stores, connectors, and third-party gateways.

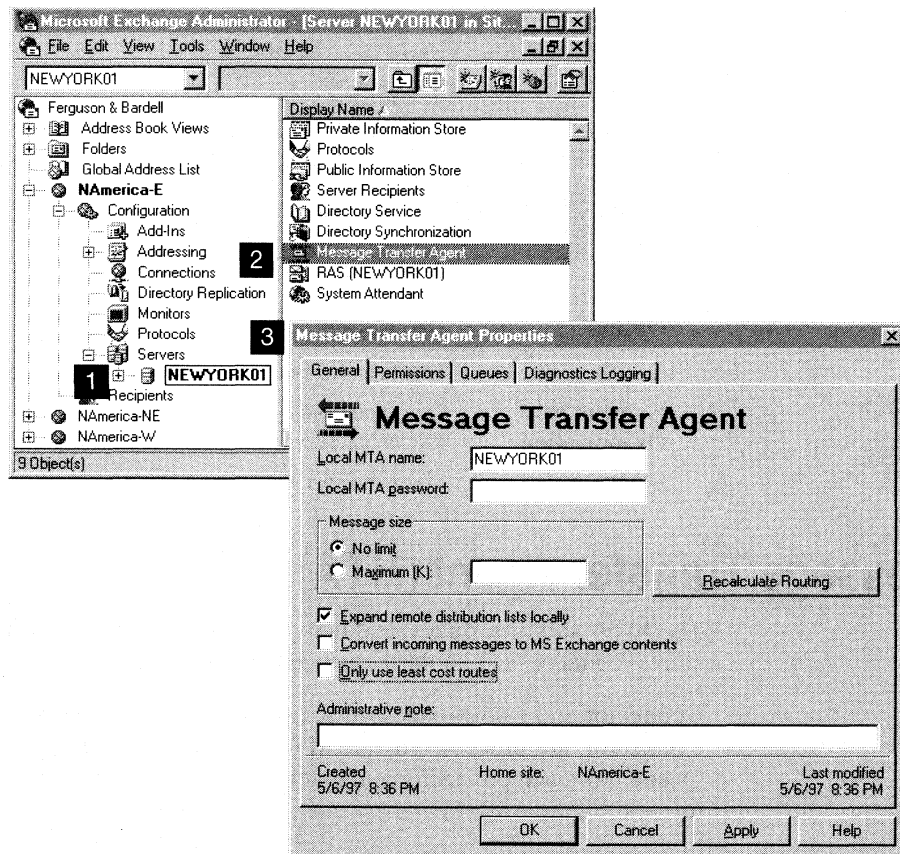
Connector and gateway messages, except messages routed by the Microsoft Mail Connector, are processed by the MTA for security, routing, and other purposes. Queues for each connector and gateway are displayed along with other MTA queues.

MTA Routing Table

The MTA routing table contains information about connectors and gateways that route messages outside the site. You manually rebuild the routing table only if the current routing information does not reflect recent changes to the routing information used by the MTA. Use the **Recalculate Routing** button in the MTA **General** property page to manually rebuild the routing table.

Getting to the MTA General property page

1. In the Administrator window, choose **Servers**, and then choose a server.
2. Double-click **Message Transfer Agent**.
3. Select the **General** tab.



Rebuilding the Routing Table

When you make changes to message routing, they are incorporated into the routing table. This table is automatically rebuilt once a day or after each change is made. For example, if you change the address space information on a connector, the routing table is rebuilt automatically within a few minutes after you save your changes. If you want the changes to take effect sooner, you can rebuild the table immediately.

1. Select the **General** tab.
2. Choose **Recalculate Routing**.

The routing table is rebuilt on the selected server and replicated to other servers in the site. It can take several minutes for the new information to reach all servers in the site.

MTA Queues and Message Information

Microsoft Exchange Server creates different queues for messages waiting to be delivered by the MTA. This applies to each server in a site, as well as to any installed connectors and gateways. Use the MTA **Queues** property page to select the appropriate queue, to view or change the priority of individual messages, or to view detailed information about a message.

For more information, see Chapter 4, “Troubleshooting Tools and Resources.”

MTA Diagnostics Logging

You can control how MTA logging information is written to the Windows NT Event Log. Using the MTA **Diagnostics Logging** property page, you can specify the types of events logged and the level of logging information for each event. Viewing the event log for the MTA is useful for troubleshooting and determining the status of the MTA and message transfers.

For more information, see Chapter 4, “Troubleshooting Tools and Resources.”

Microsoft Mail Connector

The Microsoft Mail Connector is used for message transfer between Microsoft Exchange Server sites and Microsoft Mail for PC Networks (MS Mail [PC]).

A message from Microsoft Exchange Server to MS Mail is picked up by the Connector interchange, converted to MS Mail format, and placed in a temporary information store on the Microsoft Mail Connector. The Microsoft Mail Connector MTA then retrieves the message and delivers it to the MS Mail postoffice.

You can view, return, or delete outbound messages pending transfer, and you can view and clear event logs that contain information about Microsoft Mail Connector components using the **Connections** property page. For more information, see *Microsoft Exchange Server Operations*.

Information Store

The private information store contains all mailboxes for users who have the Microsoft Exchange Server computer as their home server. The public information store is the central repository of all public folders on a server. Folders in the public information store can be replicated to servers in the local site and to servers in other Microsoft Exchange Server sites. This replication enables users in those sites to access information stored in public folders.

Status Information

You can access status information for the public and private information stores quickly by selecting the appropriate name under the public or private information store in the directory hierarchy. You can also view status information by using the status property pages on the public and private information store objects.

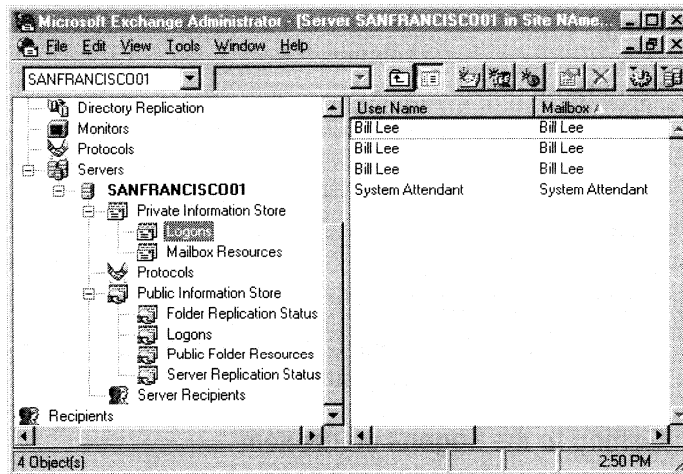
The following status items are available:

- Logons
- Mailbox resources
- Folder replication status
- Public folder resources
- Server replication status

Tip Choosing **Refresh** in an information store status property page displays the most current information about the information store.

Getting to information store status items

1. In the Administrator window, select **Private Information Store** or **Public Information Store** for the server.
2. Select a status item.



Modifying Columns for Information Store Status Items

You can customize the information store status information by changing the columns. Columns list the category name for information displayed in information store status items. You can modify how the information is displayed by adding, removing, or moving a column.

1. In the Administrator window, select **Private Information Store** or **Public Information Store** for the server.
2. Select the appropriate status item.
3. From the **View** menu, choose **Columns**.
4. Choose **Columns** to view all available column titles.

Option	Description
Available columns	Lists the column names displayed in the information store status property pages.
Add	Adds a column to the Show the following columns box.
Remove	Removes a column from the Show the following columns box.
Move Up	Moves a column name up one position in the Show the following columns box.
Move Down	Moves a column name down one position in the Show the following columns box.
Reset	Moves default column names into the Show the following columns box.
Width	Displays the column width in pixels.

Viewing Logons

Use the **Logons** status item to verify information about users who have logged on to the server's information store.

Getting to the Logons status item

1. In the Administrator window, select **Private Information Store** or **Public Information Store** for the server.
2. Select **Logons**.

Option	Description
User Name	The network user name. This is included in the default column view.
Mailbox	The mailbox display name. This is included in the default column view.
Windows NT Account	The Windows NT account name of the user who last logged on to this mailbox or public folder. This is included in the default column view.
Logon Time	The date and time that a user last logged on. This is included in the default column view.
Last Access Time	The date the user last logged on. This is included in the default column view.
Client Version	The version of the client that was used to log on to this mailbox or public folder. This is included in the default column view.
Code Page	The code page that the client is using.
Folder Ops	The total number of folder operations, such as opening or closing a folder, performed in the last minute.

(continued)

Option	Description
Full Mailbox Directory Name	The full e-mail address of the mailbox being accessed. This option is available only for the private information store.
Full User Directory Name	The name of the mailbox that is accessing the information store.
Host Address	The Internet protocol (IP) address of the client.
Locale ID	The locale ID for the language the client is using.
Messaging Ops	The total number of messaging operations, such as opening or closing a message, performed in the last minute.
Open Attachments	The total number of open attachments.
Open Folders	The total number of open folders.
Open Messages	The total number of open messages.
Other Ops	The total number of miscellaneous operations performed in the last minute.
Progress Ops	The total number of progress operations performed in the last minute. Progress operations inform the user about how long it will take to complete a task.
Stream Ops	The total number of stream operations, such as viewing or changing an attachment, performed in the last minute.
Table Ops	The total number of table operations, such as viewing the contents of a folder, performed in the last minute.
Total Ops	The total number of operations performed in the last minute.
Transfer Ops	The total number of transfer operations, such as copying or moving a message, performed in the last minute.

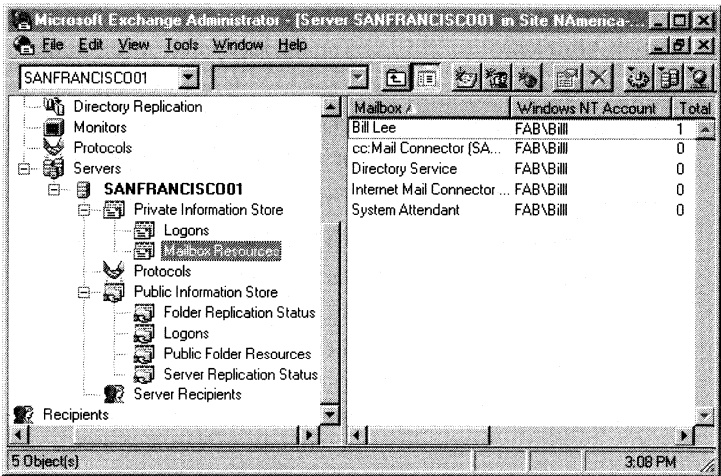
Viewing Mailbox Resources

Use **Mailbox Resources** to view statistics for a private information store. You can determine how mailboxes are being used and whether resources are sufficient.

Note Status on mailbox resources is available only for the private information store.

Getting to the Mailbox Resources status item

- 1. In the Administrator window, select **Private Information Store** for the server.
- 2. Select **Mailbox Resources**.



Option	Description
Mailbox	The name of this mailbox. This is included in the default column view.
Windows NT Account	The Windows NT account name of the user who last logged on to this mailbox. This is included in the default column view.
Total K	The total amount of disk space in kilobytes that this mailbox occupies on the private information store, including space consumed by messages, attachments, and hidden system information in the form of associated messages. This is included in the default column view.
Total no. Items	Total number of non-associated messages that are stored in the mailbox. This is included in the default column view.
Last Logon Time	Time that a user last logged on to this mailbox. This is included in the default column view.
Last Logoff Time	Time that a user last logged off this mailbox. This is included in the default column view.
Deleted Items K	The total amount of disk space in kilobytes occupied by retained deleted items for this mailbox.

(continued)

Option	Description
Full Mailbox Directory Name	The full e-mail address of the mailbox being accessed.
Storage Limits	The status relative to the storage limit.
Total no. Associated Messages	Total number of messages in the mailbox that represent hidden system information, such as forms, views, reply templates, and deferred action messages.

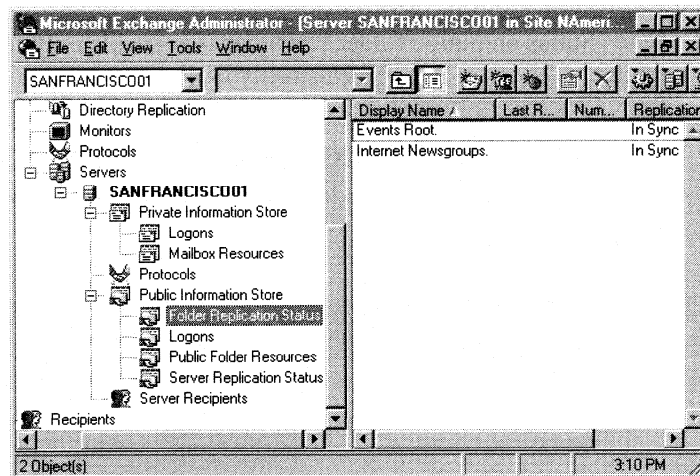
Viewing Folder Replication Status

Use **Folder Replication Status** to view the status of public folder replication within a site.

Note Status on folder replication is available only for the public information store.

Getting to Public Folder Replication Status item

1. In the Administrator window, select **Public Information Store** for the server.
2. Select **Folder Replication Status**.



Option	Description
Display Name	The public folder name as it appears in the Address Book. This is included in the default column view.
Last Received Time	The time the last update was received. This is included in the default column view.
Number of Replicas	The total number of replicas of this folder throughout the site. This is included in the default column view.
Replication Status	In Sync indicates that there have been no changes to this replica since it last sent out its changes. Local Modified indicates that the replica of the public folder on this server has changed and that the changes have not been replicated throughout the site. This is included in the default column view.
Folder	The public folder name.

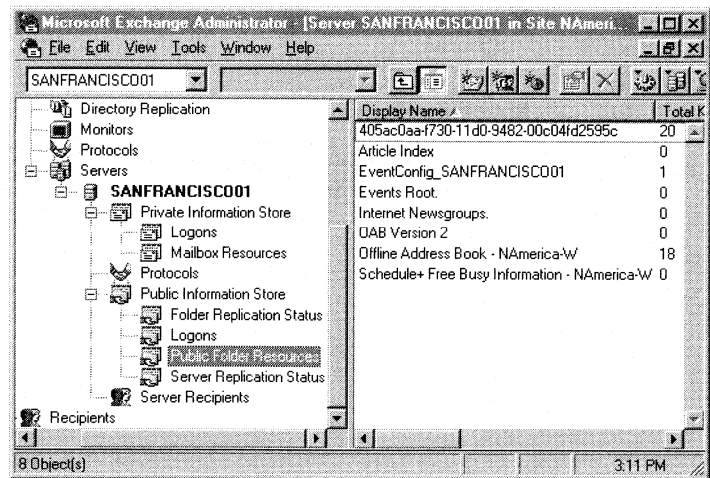
Viewing Public Folder Resources

You can view the resource information of a public folder by selecting the **Public Folder Resources** status item for the public information store object. Use this information to monitor and view the names of folders in the information store, along with other details.

Note Status on public folder resources is available only for the public information store.

Getting to the Public Folder Resources status item

1. In the Administrator window, select **Public Information Store** for the server.
2. Select **Public Folder Resources**.



Option	Description
Display Name	The name of the public folder. This is included in the default column view.
Total K	The total amount of disk space in kilobytes that this folder occupies on the public information store, including space consumed by messages, attachments, and hidden system information in the form of associated messages. This is included in the default column view.
Total no. Items	Total number of items non-associated messages that are stored in the folder. This is included in the default column view.
Created	The date when the folder was created. This is included in the default column view.
Last Access Time	The date when the folder was last accessed. This is included in the default column view.
No. of Owners	The number of users who have Folder Owner permission. This is included in the default column view.
No. of Contacts	The number of users who are designated as folder contacts for this folder. This is included in the default column view.
Folder	The name of the folder where messages are stored.
Folder Path	The name of the path where the folder is located.
Total no. Associated Messages	Total number of messages in the folder that represent hidden system information, such as forms, views, and reply templates.
Deleted Items K	The total amount of disk space in kilobytes occupied by retained deleted items for this public folder.

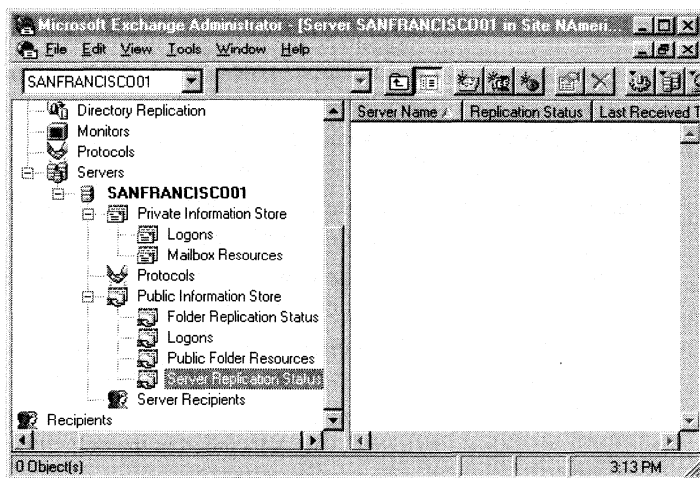
Viewing Server Replication Status

Use **Server Replication Status** to view the status of public folder replication between this server and all other servers in the organization with which it replicates public folders.

Note Status on mailbox resources is available only for the private information store.

Getting to Server Replication Status item

1. In the Administrator window, select **Public Information Store** for the server.
2. Select **Server Replication Status**.



Option	Description
Server Name	The name of the server. This is included in the default column view.
Replication Status	In Sync indicates that there have been no changes to this replica since it last sent out its changes. Local Modified indicates that the replica of the public folder on this server has changed and the changes have not yet been replicated throughout the site. This is included in the default column view.
Last Received Time	The last time the local server received updates from the selected server. This is included in the default column view.
Average Transmission Time	The average time it takes to send updates from the local server to the selected server. This is included in the default column view.
Last Transmission Time (sec)	The amount of time of the last transmission from the local server to the selected server. This is included in the default column view.

Maintenance Schedule

Microsoft Exchange Server performs online maintenance tasks on a scheduled basis. These tasks include:

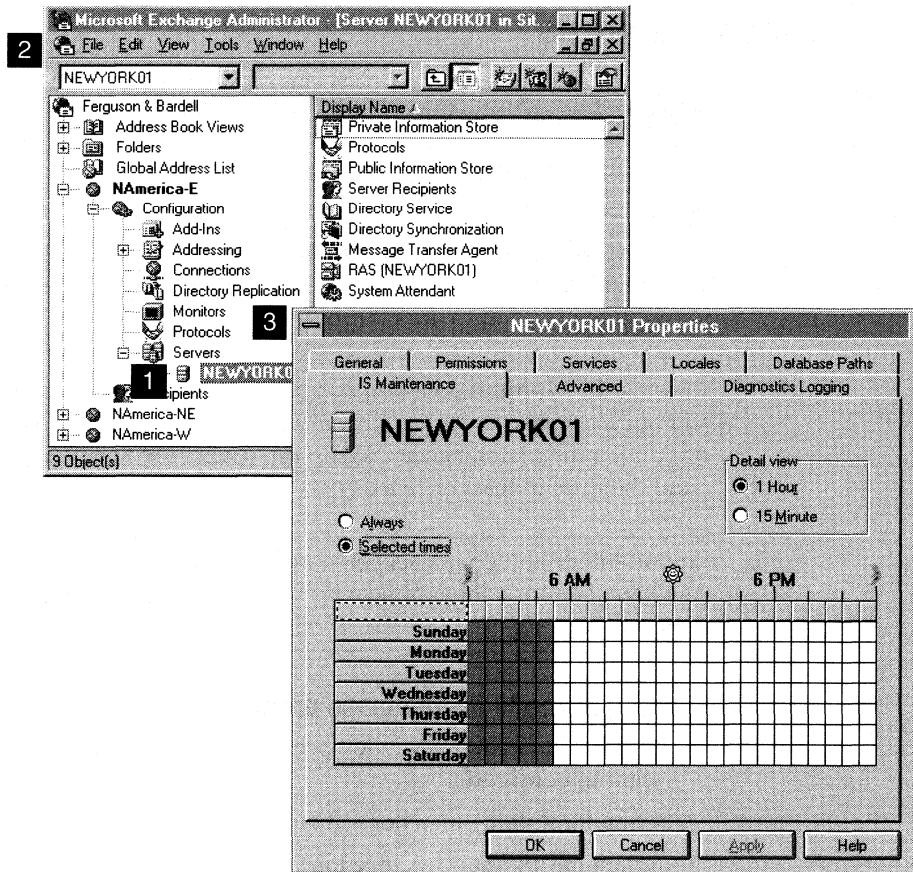
- Performing deleted item retention cleanup.
- Deleting expired folder indexes and expired items from public folders.
- Synchronizing the server's information store version with other servers in the organization.
- Removing expired public folder conflicts.

Use the **IS Maintenance** property page to schedule this maintenance for each server. Response times are slower while the server is performing maintenance tasks. Set the maintenance tasks to run during the least busy time of day, but make sure they run at least once a day.

Important If you do not schedule maintenance or schedule infrequent maintenance for a large or heavily used information store, performance can deteriorate.

Getting to the IS Maintenance property page

1. In the Administrator window, choose **Servers**, and then choose the server you want to configure.
2. From the **File** menu, choose **Properties**.
3. Select the **IS Maintenance** tab.



Setting the Maintenance Schedule

You create a maintenance schedule to prevent performance deterioration on the Microsoft Exchange Server computer. Knowing the server's least busy time helps you set time increments for scheduling maintenance.

1. Select the **IS Maintenance** tab.
2. Select **Never**, **Always**, or **Selected Times**.
3. Under **Detail View**, select a view for the schedule grid.

Option	Description
Always	Performs maintenance tasks every 15 minutes. This option is not recommended because it can affect server performance.
Selected times	Assigns specific maintenance times in the schedule grid. Select a time or block of time when maintenance should occur.
1 Hour	Displays the schedule grid in one-hour increments.
15 Minute	Displays the schedule grid in 15-minute increments.

Directory

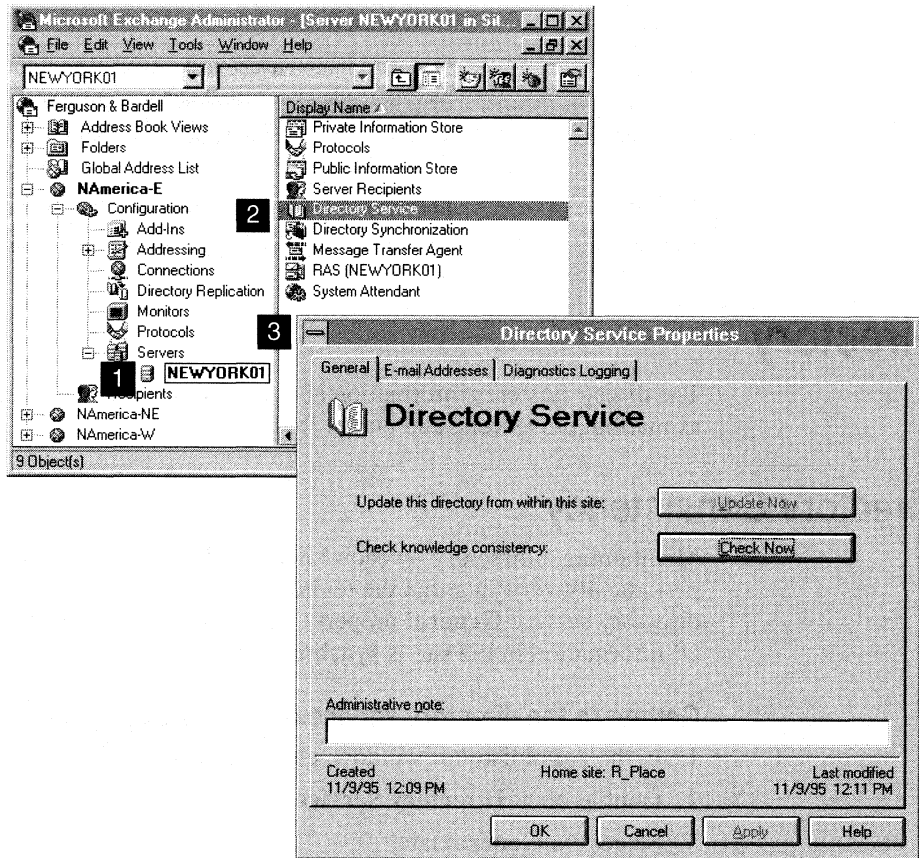
The directory stores information about an organization's resources and users, such as mailboxes, servers, and public folders.

Directory Consistency

Maintaining a directory on each Microsoft Exchange Server computer includes periodically verifying that the replicated directory information is correct. Use the directory service **General** property page to update the directory or to verify that all information in the site is synchronized.

Getting to the directory service General property page

1. In the Administrator window, choose **Servers**, and then choose a server.
2. Double-click **Directory Service**.
3. Select the **General** tab.



Verifying Directory Consistency

Replication of directory information between servers in the same site occurs automatically. Replication between sites is a scheduled process you set up using the directory replication connector. You can initiate a consistency check of all directories in your organization if servers or sites have been added while a server was not operating, or if you suspect an error has occurred during directory replication.

1. Select the **General** tab.
2. Choose **Check Now** to check the consistency of all directories in your organization.

Resynchronizing Replicated Directory Information

You can resynchronize the directory with other servers in the same site if a server has been added to your site or was temporarily offline, or you suspect an error has occurred. You can also initiate an immediate directory replication request to other sites in your organization if a site has recently been added, the connection between sites was temporarily offline, or you suspect a replication error has occurred.

Note Knowledge consistency is checked automatically once a day. If you manually check knowledge consistency and discover a new server or site, choose **Update Now** to update your local directory.

1. Select the **General** tab.
2. Choose **Update Now** to request updates from other servers within this site.

Directory Diagnostics Logging

Maintaining the directory on each Microsoft Exchange Server computer includes periodically viewing and clearing the event logs to verify that the directory, directory replication, and directory synchronization processes are working correctly.

You can control how logging information for the directory is written to the Windows NT Event Log. Using the **Diagnostics Logging** property page for the directory service and directory synchronization objects, you can specify the types of events logged and the level of logging information for each event. Viewing the event log for the directory can help you determine directory activity.

For more information, see Chapter 4, “Troubleshooting Tools and Resources.”

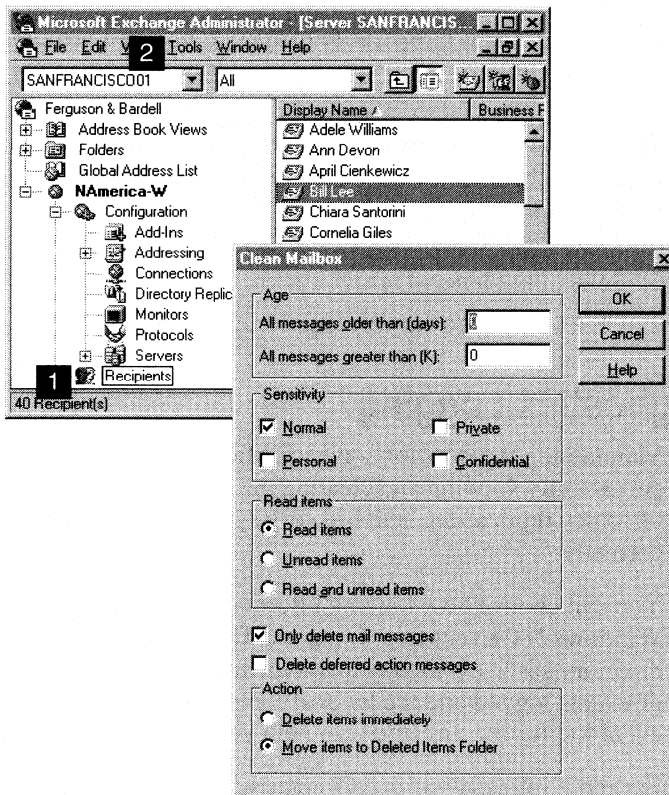
Mailbox Maintenance

You can clean a mailbox to delete messages from a user’s mailbox stored on a server. Cleaning the mailbox recovers space in the server’s private information store.

Note Cleaning a mailbox works only on single or multiple mailboxes but does not work for distribution lists, custom recipients, or public folders. Cleaning a user’s mailbox can be done while the mailbox is open.

Getting to the Clean Mailbox dialog box

1. In the Administrator window, choose **Recipients**, and then select a mailbox.
2. From the **Tools** menu, choose **Clean Mailbox**.



Setting Age Limits

You can specify which messages should be deleted from the mailbox.

1. From the **Tools** menu, choose **Clean Mailbox**.
2. In the **Age** box, select an option.

Option	Description
All messages older than (days)	Type a value representing days. All messages older than the specified number of days are deleted.
All messages greater than (K)	Type a value representing kilobytes. All messages larger than the specified number of kilobytes are deleted.

Setting the Sensitivity Level

Messages are marked with one of four sensitivity levels. All messages marked with the selected sensitivity levels will be deleted. Select the default sensitivity that you want to assign to all your outgoing mail.

1. From the **Tools** menu, choose **Clean Mailbox**.
2. In the **Sensitivity** box, select an option.

Option	Description
Normal	Leaves the item header blank and sends messages with no sensitivity.
Personal	Contains nonbusiness information.
Private	Prohibits any recipient from modifying your original message when it is replied to or forwarded.
Confidential	Handles the message according to your organization's policy on confidentiality.

Specifying Read Items

You can delete messages based on whether they have been read.

1. From the **Tools** menu, choose **Clean Mailbox**.
2. In the **Read Items** box, select an option.

Option	Description
Read items	Deletes all messages that have been read.
Unread items	Deletes all messages that have not been read.
Read and unread items	Deletes read and unread messages.

Deleting Other Information

When you clean a mailbox, you can delete all information associated with the selected folder or delete only mail messages.

1. From the **Tools** menu, choose **Clean Mailbox**.
2. Select **Only delete mail messages** and **Delete deferred action messages**.

Option	Description
Only delete mail messages	If cleared, mail messages and other messages containing information such as contact, calendaring, and tasks are deleted. If selected, only mail messages are deleted.
Delete deferred action messages	If selected, all messages in the deferred actions folder are deleted. Deferred action messages describe commands that are queued for the e-mail client to perform the next time it logs on to the server. These commands can include copying and moving messages to a personal folder or rules that delete messages from a personal folder. If cleared, deferred action messages are preserved.

Setting the Action Level

You can indicate what action should be taken on deleted messages.

1. From the **Tools** menu, choose **Clean Mailbox**.
2. In the **Action** box, select an option.

Option	Description
Delete items immediately	Immediately deletes all messages that meet the specified criteria.
Move items to Deleted Items Folder	Moves deleted messages into the selected user's Deleted Items folder. Messages in the Deleted Items folder can be retrieved, viewed, and moved to other folders.

Administrator Window Contents

You can save the contents of a window in the Administrator program to a comma-separated value (.csv) file. For example, if you want to print a list of all mailboxes in the Recipients container, you can save the contents of the Recipients container, open the file in a spreadsheet application such as Microsoft Excel, and print the list of recipients.

Saving the Window Contents

The following procedure describes how to save the contents of a window in the Administrator program.

1. Select the container with the items that you want to save, and then select an item in the container.
2. From the **File** menu, choose **Save Window Contents**.
3. Specify the name and location of the .csv file that will contain the window contents.

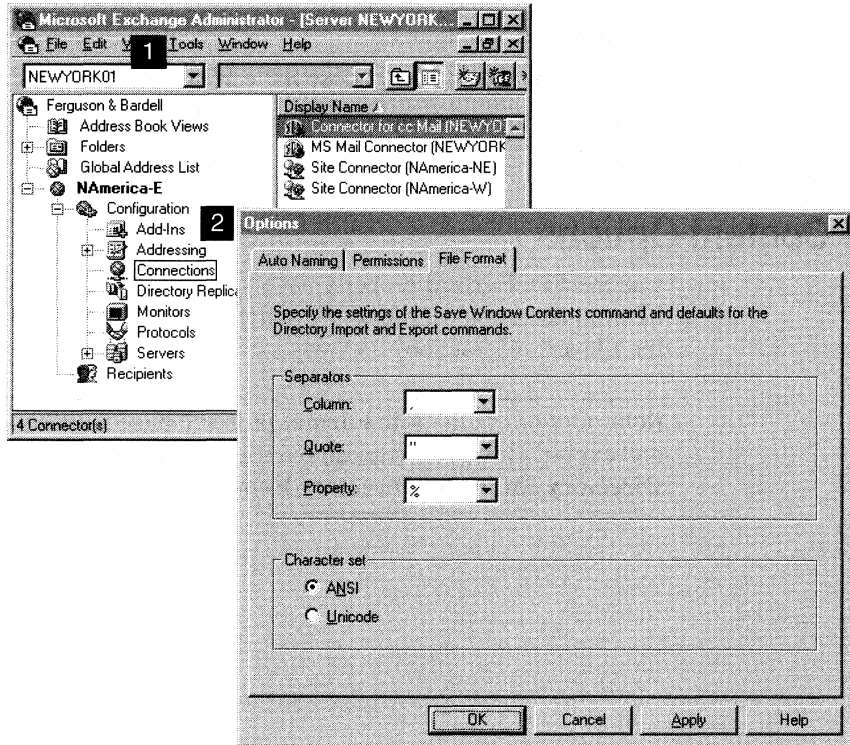
File Content Options

Use the **File Format** property page to specify the separators and character set to be used in the export file. For example, you can specify that column headings in the file are separated by commas.

Note Options in the **File Format** property page are also used for directory import and export. However, you can override the default values when using the **Directory Import** or **Directory Export** commands (**Tools** menu).

Getting to the File Format property page

1. From the **Tools** menu, choose **Options**.
2. Select the **File Format** tab.



Selecting Separators and Character Sets

Separators distinguish column, quote, and property types of information in the file.

Note The **Property** separator is not supported when saving the contents of the Administrator window.

1. Select the **File Format** tab.
2. Select the separators to be used to separate information in the export file and the character set.

Option	Description
Column	Separates columns of data. You can use a comma, tab, or space. By default, Microsoft Exchange Server uses a comma (,) to separate fields and columns.
Property	<p>Separates fields with multivalued properties. A multivalued property is a property that contains multiple values. For example, the Members field of a distribution list can contain the names of multiple recipients. In an import file, the Members field can appear as follows:</p> <p>adelew%alig%annd%aprilc%billl%chiaras.</p> <p>Any of the following characters for the property separator can be chosen: !, #, \$, %, &, *, @, ^, By default, Microsoft Exchange Server uses a percent sign (%) to separate fields within multivalued properties.</p>
Quote	Separates fields that contain the column separator character. For example, if a recipient's display name is Williams, Adele, the field must be enclosed in quotation marks to indicate that the comma is not intended to be treated as a column separator. For example, "Williams, Adele." You can use a single quotation mark (') or a double quotation mark ("). By default, Microsoft Exchange Server uses a double quotation mark (") to separate fields that contain the column separator character.
ANSI	Specifies the character set that is used when creating the .csv file. If this option is selected, the file uses the active American National Standards Institute (ANSI) code page.
Unicode	Specifies the character set that is used when creating the .csv file. If this option is selected, the file uses Unicode.

Directory Export and Import

You can use the **Directory Export** or **Directory Import** command on the **Tools** menu of the Administrator program to make global changes to directory objects, such as mailboxes, custom recipients, and distribution lists. For example, if you need to change the telephone prefix for all mailboxes, you can export the mailboxes from Microsoft Exchange Server to a comma-separated value (.csv) text file and edit the data in the file using a spreadsheet application. You can then import the data in the file to Microsoft Exchange Server.

Export and import files are in .csv format, which can be read by database programs such as Microsoft Access or spreadsheet programs such as Microsoft Excel. The first line of every import or export file contains a header followed by lines of data to be imported or exported. The header organizes the columns of information contained in the file when viewed in a spreadsheet application. By default, fields are separated by commas, and each line ends with a carriage return and line feed. There is no limit to the number of data lines in an import or export file.

For more information, see *Microsoft Exchange Server Migration* and the *Microsoft Exchange Server Programmer's Reference*.

Using Directory Export

You can export directory information for mailboxes, distribution lists, or custom recipients. By default, the **Directory Export** command creates an export file with the following header.

```
Obj-Class,First Name,Last name,Display Name,Alias Name,  
Directory Name,Primary Windows NT Account,Home-Server,  
E-mail address,E-mail Addresses,Members,Obj-Container,Hide from AB
```

If an existing export file is specified, the **Directory Export** command uses the header from the specified file when exporting recipients. To control which properties are exported, you should create a .csv file containing only the header information that you want to use, and then export recipients to that file.

Using the Directory Export Command

1. From the **Tools** menu in the Administrator window, choose **Directory Export**.
2. Select the appropriate options.
3. Choose **Export**.

Option	Description
Microsoft Exchange server	The server the information is read from.
Home server	The home server of the mailboxes to export.
Export File	The path and file name where you want to store the exported directory information.
Container	The container where the recipient objects will be exported.
Include subcontainers	Includes the recipient objects in the subcontainers of the specified recipient container.
Export objects	The recipient objects to be exported (mailbox, custom recipient, or distribution list).
Logging level	Specifies the event logging level when performing the export.
Separators	Specifies the separators used in the exported file. Separators distinguish column, quote, and property types of information in the file.
ANSI	Specifies the character set that is used when creating the export file. If this option is selected, the file uses the active ANSI code page.
Unicode	Specifies the character set that is used when creating the export file. If this option is selected, the export file uses Unicode.
Include hidden objects	Includes hidden recipient objects.

Using Command-line Directory Export Options

Directory exports can also be done from the command line. Use the following syntax in the Admin.exe program:

admin /e <export file> /d <directory server name> /n /o <options file>

The /e switch is required. All other switches are optional. For more information about command-line options, see Administrator program Help.

Option	Description
<export file>	The name of the file where the exported directory information is to be written.
<directory server name>	The name of the server from which the directory information will be exported.
/n	Specifies that the progress bar is not displayed during directory export.
/o	The name of an import options file.
<options file>	The name of a file containing options that control how directory information is exported.

The export options file is used to specify the same types of options as the Administrator program's **Directory Export** dialog box. The export options file is a text file and must be in the following format.

```
[Export]
DirectoryService=<DS server name>
;(default=NULL)
HomeServer=<server name>
;(default=NULL)
Basepoint=<DN of basepoint object>
;(default=NULL, which indicates the local site)
Container=<RDN of container object>
;(default=Recipients)
ExportObject=[Mailbox, Remote (custom recipients), DL, Recipients (all recipients), All (all object types)]
;(default=Mailbox)
InformationLevel=[None, Minimal, Full]
;(default=Minimal)
BasepointOnly=[Yes, No]
;(default=No)
RawMode=[Yes, No]
;(default=No)
Hidden=[Yes, No]
;(default=No)
Subcontainers=[Yes, No]
;(default=No)
CodePage=[-1,0,code-page-ID]
;(default = 0)
```

```
Column Separator=<ASCII value of column separator character>
;default=44(",")
MVSeparator=<ASCII value of multivalued separator character>
;default=37("%")
Quote Character=<ASCII value of quoted value delimiter>
;default=34("“”")
```

Using Directory Import

Import files are identical to export files except that import files contain a mode property that specifies an action to either update, create, modify, or delete the mailbox, distribution list, or custom recipient. If no mode is specified, the default mode is **update**, which creates the object if it does not exist or modifies the object if it does.

The following example shows how the mode property can be used in an import file.

```
Obj-Class,Mode,First Name,Last name,Display Name,Alias Name
mailbox,modify,Bill,Lee,Bill H. Lee,bill1
mailbox,create,Bill Lee,Bill S. Lee,bills1
mailbox,delete,Test,Testing,Test of Import File,test2i
```

Importing the example file would change the display name of Bill Lee’s mailbox to Bill H. Lee, create a mailbox for a new user named Bill S. Lee, and delete a test mailbox. You can create new import files using any text editor, word processor, or spreadsheet program that supports .csv files.

Using the Directory Import Command

1. From the **Tools** menu in the Administrator window, choose **Directory Import**.
2. Select the appropriate options.
3. Choose **Import** to start the import process.

Option	Description
Windows NT domain	The location where user accounts will be created.
Microsoft Exchange server	The server to which you want to import directory information.
Container	The container where recipient objects will be created or modified.
Recipient Template	A recipient object (mailbox, distribution list, custom recipient) to be used as a template object for all imported objects of the same type. It is chosen from the Address Book.
Import File	The path and file name of the file that contains the information you are importing.

(continued)

Option	Description
Create Windows NT account	Specifies whether Windows NT accounts should be created for imported recipients.
Generate random password	<p>If this option is not selected, new Windows NT accounts are created with a password based on the account name. If the account name has fewer than four characters, the password is padded with “x” characters to a length of four characters. Passwords generated from account names longer than 14 characters are truncated.</p> <p>If this option is selected, new Windows NT accounts are created with randomly generated passwords. The passwords are saved to the local disk in a .psw file in the same directory as the import file. If an NTFS partition is being used, the .psw file is accessible only to the user who is currently logged on.</p>
Delete Windows NT account	Specifies whether the Windows NT account associated with a recipient should be deleted when the recipient is deleted.
Logging level	Specifies the event logging level when performing the import.
Separators	Specifies the separators used in the imported file. Separators distinguish column, quote, and property types of information in the file.
Multivalued Properties	Select Append if imported data in a multivalued property should be added to existing data. Select Overwrite if imported data in a multivalued property should replace any existing data.

Using Command-line Directory Import Options

Directory imports can also be done from the command line. Use the following syntax in the Admin.exe program:

admin /i <import file> /d <directory server name> /n /o <options file>

The /i switch is required. All other switches are optional. For more information about command-line options, see Administrator program Help.

Option	Description
<import file>	The name of the file that contains directory information to be imported.
<directory server name>	The name of the server whose directory is to be updated.
/n	Specifies that the progress bar is not displayed during directory import.
/o	Specifies the name of an import options file.
<options file>	The name of a file containing options that control how directory information is imported.

The import options file is used to specify the same types of options as the Administrator program's **Directory Import** dialog box. The import options file is a text file and must be in the following format.

```
[Import]
DirectoryService=<DS server name>
;(default=NULL)
Basepoint=<DN of basepoint object>
;(default=NULL, which indicates the local site)
Container=<RDN of container object>
;(default=Recipients)
InformationLevel=[None, Minimal, Full]
;(default=Minimal)
RecipientTemplate=<DN of default recipient object>
;(default=none)
NTDomain=<NT domain where accounts will be created>
;(default=none)
OverwriteProperties=[Yes, No]
;(default=No)
CreateNTAccounts=[Yes, No]
;(default=No)
DeleteNTAccounts=[Yes, No]
;(default=No)
ApplyNTSecurity=[Yes, No]
;(default=Yes)
GeneratePassword=[Yes, No]
;(default=No)
RawMode=[Yes, No]
;(default=No)
CodePage=[-1,0,code-page-ID]
;(default=0)
```

Note The RawMode option is primarily intended for developers and should be enabled only by advanced users. Raw mode requires specific information about the directory schema. Files that can be imported normally are likely to fail in raw mode because they don't contain sufficient information. For more details about the directory schema, see the *Microsoft Exchange Server Software Developer's Kit*.

Selecting a Separator

There are three types of separators you can use with directory import and directory export: column, quote, and property. For descriptions, see “Selecting Separators and Character Sets” earlier in this chapter.

Quoting Behavior for Multivalued Properties

When you import or export multivalued properties, Microsoft Exchange Server quotes the entire multivalued property. Embedded, multivalued property separator characters are prefixed with a backslash (\) character. For example, a multivalued property with values "v,1", "v,2", and "v,3", is exported as:

```
"v,1\v,2\v,3"
```

A multivalued property with values "v%1", "v,2", and "v,3", is exported as:

```
"v\v%1\v,2\v,3"
```

For example, the multivalued property of an exported proxy address might look like the following. The CUSTOM: proxy address (Black, Maria at \\SANFRANCISCO01) has an embedded comma and embedded backslashes. The comma is the default multivalued attribute separator, and the backslash is the literal character introducer. Because of the presence of embedded commas, the entire multivalued proxy addresses property is quoted, and each of the two embedded backslashes is introduced by a backslash character.

```
"CCMAIL:Black, Maria at California%CUSTOM:Black, Maria at  
\\SANFRANCISCO01%MS:FERGUSONBA/NAMERICA-W/MARIAB%SMTP:MariaB@  
California.Ferguson&Bardell.com%X400:c=US;a= ;p=Ferguson ?  
Barde;o=California;s=Black;g=Maria;"
```

The following example shows the Members multivalued property of an exported distribution list, which shows the distinguished names of the members of the distribution list. Because there are no embedded special characters in the string (for example, commas and backslashes), the property is not quoted.

```
Recipients/cn=Letters/cn=marketing%Recipients/cn=Letters/cn=sales%  
Recipients/cn=Letters/cn=Support
```

Using .Csv Files Generated by Microsoft Exchange Server Version 4.0

In Microsoft Exchange Server version 4.0, if a multivalued property contained embedded separators (for example, commas and tabs), the property values making up the multivalued property were quoted individually. If Microsoft Excel was then used to edit the exported data file, the quotes embedded in the multivalued property value string were not recognized, and the property would be incorrectly split across several Microsoft Excel cells.

Import files generated for use with Microsoft Exchange Server version 4.0 are compatible with Microsoft Exchange Server version 5.5, with the following exceptions:

- If a quoted string is specified for a multivalued property, and the string contains one or more multivalued property separators, the string is split into multiple values unless the separator character is preceded by a backslash. Previous versions of Microsoft Exchange Server treated the string as a single value. Separator characters found in exported strings are preceded with the backslash, and are correctly handled on import. This behavior is unchanged from version 4.0, so data files exported with version 4.0 can be imported using version 5.5.
- To minimize the number of cases where this new handling of multivalued properties causes problems in user-edited files, multivalued property separator characters in single-valued properties are now ignored. In version 4.0, the value was split at the multivalued property separator, and only the first portion was used. In most cases, this would not generate a warning.

Monitoring Your Organization



Microsoft Exchange Server has several options for *monitoring* your organization. Monitoring involves checking for problems with services, servers, connections, and gateways, and then notifying the appropriate people to fix them.

Note You cannot use monitoring to check all Microsoft Exchange Server features. For example, directory and public folder replication events are logged, but alerts are not sent.

Monitoring tools include:

- Link monitor
- Server monitor
- Windows NT Performance Monitor

Link Monitor

You use link monitors to verify the efficient routing of test messages. These messages are called *ping messages*. At every polling interval, a ping message is sent to every server and system configured in the monitor.

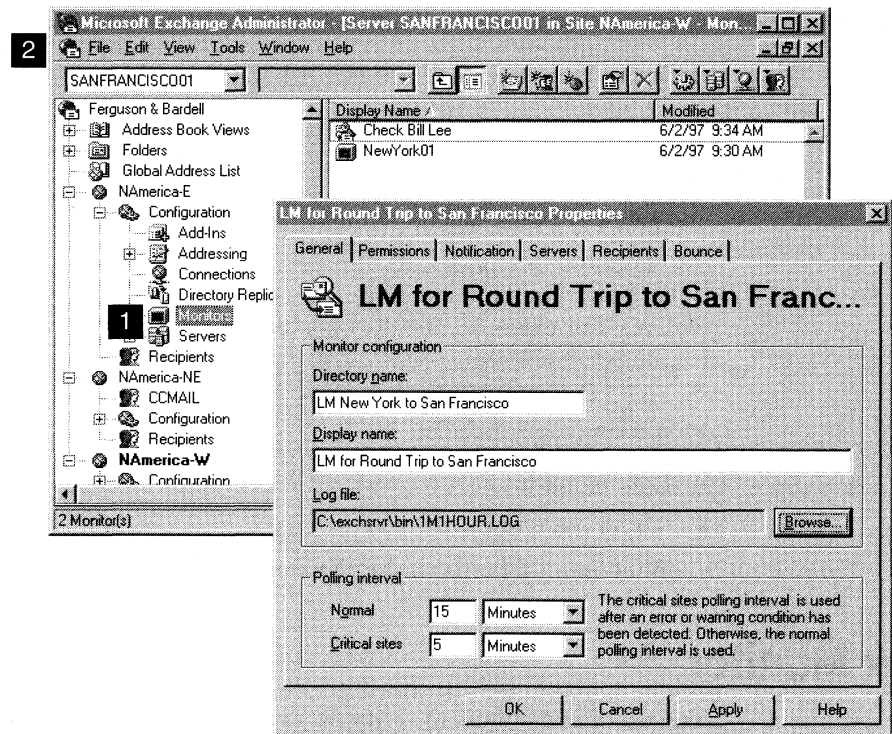
When you set up a link monitor, you can specify a nonexistent recipient on the target system. The link monitor determines if the link is active by sending a message to this recipient and waiting for a non-delivery report (NDR) from the server.

Note If a target custom recipient matches the link monitor's requested nonexistent custom recipient, the link monitor fails to receive an NDR and reports that the link is unavailable.

Link Monitor Configuration

When you set up a link monitor, you can configure it according to your needs. For example, you may want the link monitor to poll the link every six hours.

1. In the Administrator window, choose **Monitors**.
2. From the **File** menu, choose **New Other**, and then choose **Link Monitor**.



General Properties

Use the **General** property page to define a directory name and a display name, create log files, and set polling intervals.

Getting to the General property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the link monitor you want to view or update.
3. Select the **General** tab.

Defining the Directory Name and the Display Name

You provide a directory name used for identification by the system and a display name that appears in the Administrator window. The directory name is used for starting a link monitor automatically, though you can start it manually.

1. Select the **General** tab.
2. In the **Directory name** box, type a name.
3. In the **Display name** box, type a name.

Option	Description
Directory name	A maximum of 64 alphanumeric characters, which can include spaces and special characters. If no name is provided, the system prompts for a value. The name cannot be changed.
Display name	A maximum of 256 alphanumeric characters. The syntax of this field is Unicode, which understands all languages and their special characters. If no name is provided, the system prompts for a value. The name can be modified at any time.

Creating Log Files

The *log file* stores information about changes in connection and notification status. Creating log files is optional, but they are helpful for troubleshooting. If no directory and file name are specified, a log file is not created.

Tip The log file is easy to find on the network. Specify the path using the universal naming convention (UNC), such as: \\Servername\C\$\S1m1hour.log.

1. Select the **General** tab.
2. Choose **Browse**.
3. Type or select the directory and file name for the log file, and then choose **Save**.

Setting Polling Intervals

Use polling intervals to indicate how often the link monitor sends ping messages to check connections. Normal sites contain links that have ping messages returning within the specified bounce time. A critical link does not meet the criteria defined for a normal link. Because of this, the default polling interval for a normal site is longer than that for a critical site. Polling intervals for both normal and critical sites can be set to any duration.

1. Select the **General** tab.
2. In the **Normal** box, type a number, and then select either **Seconds**, **Minutes**, or **Hours**.
3. In the **Critical sites** box, type a number, and then select either **Seconds**, **Minutes**, or **Hours**.

Option	Description
Normal	Indicate how often to send a ping message. The default is 15 minutes.
Critical sites	Indicate how often to send a ping message to servers or systems that are in a warning or alert state. The default is 5 minutes.

Permissions

Use the **Permissions** property page to indicate which Windows NT accounts can modify the specified monitor. Permissions are necessary when a connection is being modified but are not necessary to start a link monitor.

Note By default, the **Permissions** property page is hidden. To view it, choose **Options** from the **Tools** menu.

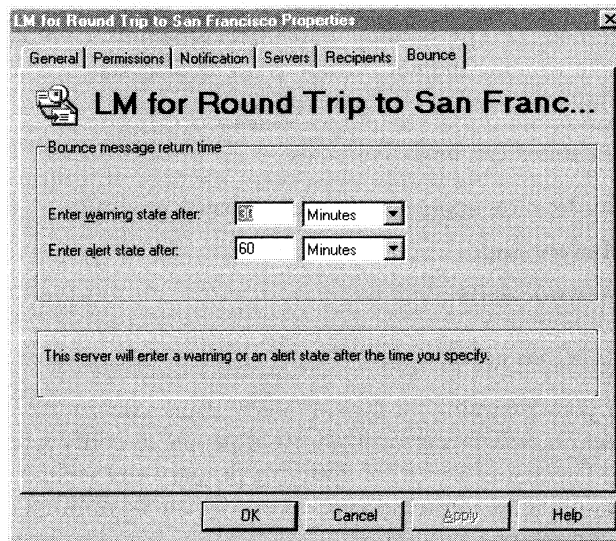
For more information on permissions, see *Microsoft Exchange Server Getting Started*.

Warning and Alert Durations

Use the **Bounce** property page to set the warning and alert durations for each link monitor. One set of durations is used for all recipients and servers. You can create multiple link monitors if the monitored servers and foreign systems have different *bounce durations*. A bounce duration is the longest acceptable round-trip time for a message to travel between the monitor's home server and another server or foreign system. You determine the value based on tests you have performed previously. An alert state indicates a more serious connection problem than a warning state.

Getting to the Bounce property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the link monitor you want to update.
3. Select the **Bounce** tab.



Specifying a Warning State Duration

A warning state occurs when the ping message returns late. An alert state occurs when the ping message is returned very late.

1. Select the **Bounce** tab.
2. In the **Enter warning state after** box, type a number, and then select **Seconds**, **Minutes**, or **Hours**. The default is 30 minutes.

Specifying an Alert State Duration

An alert state duration is the length of time after which the returned ping message should be considered very late.

1. Select the **Bounce** tab.
2. In the **Enter alert state after** box, type a number, and then select **Seconds**, **Minutes**, or **Hours**. The default is 60 minutes.

To start the link monitor, see “Starting Link and Server Monitors Automatically” later in this chapter.

Notification Process

Use the **Notification** property page to specify how to notify administrators when a connection is in a warning state or an alert state. A *warning state*, indicating a possible problem, occurs when a ping message fails to return within the bounce duration you set for warning status. An *alert state*, indicating a serious problem, occurs when a ping message fails to return within the bounce duration you set for an alert status. The symbols in the left column of the **Notification** property page indicate whether the notification is for an alert state (red down arrow) or a warning state (red exclamation point).

Notifications can be delivered as:

- Notification applications, such as pager programs
- Mail messages
- Network alerts

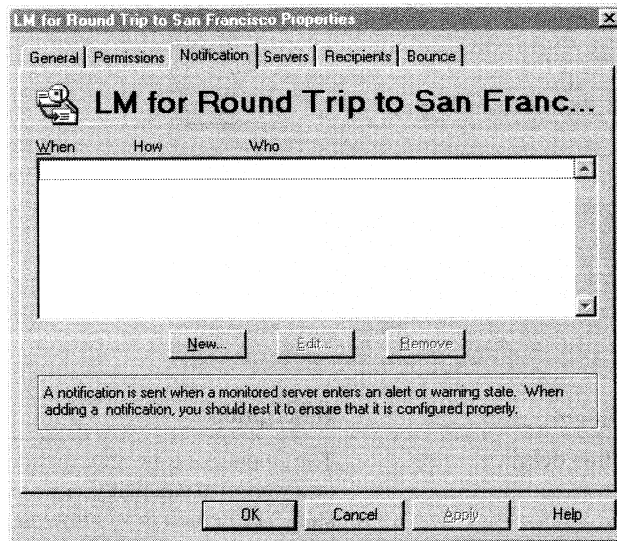
Notifications are also sent when connections are restored.

After you determine the type of notification, you set the escalation path. An *escalation path* is a prioritized list of people to notify when a monitor is in an alert state. This list is useful for notifying primary and secondary support personnel. For example, the primary support person can be notified immediately when the monitor enters a warning state, whereas the secondary personnel can have a longer time delay or not be notified until the monitor enters an alert state.

You might want to set a staggered time for three support people: a primary support person and two secondary support people. These three notifications could be staggered from immediate notification to one hour. You must complete the notification setup process three times, once for each person.

Getting to the Notification property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the link monitor you want to update.
3. Select the **Notification** tab.

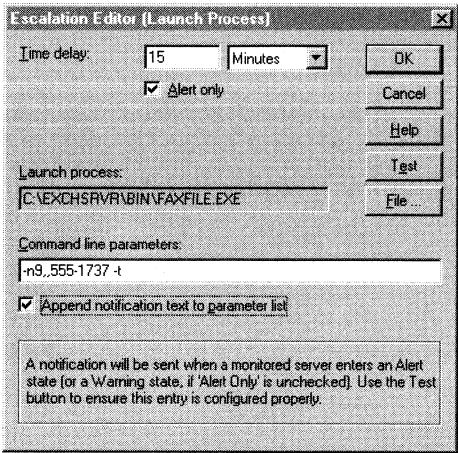


Using Notification Applications

You can use notification applications to alert users who are not logged on to the network. This is appropriate for an administrator who monitors the network remotely using a pager program.

1. Select the **Notification** tab.
2. Choose **New**.
3. Select **Launch a Process**, and then choose **OK**.
4. In the **Time delay** box, type the amount of time after entering an alert state that you want the notification process to begin. Select **Seconds**, **Minutes**, or **Hours**.

5. Choose **File** to browse for a process to launch.
6. In the **Command line parameters** box, type any command parameters.

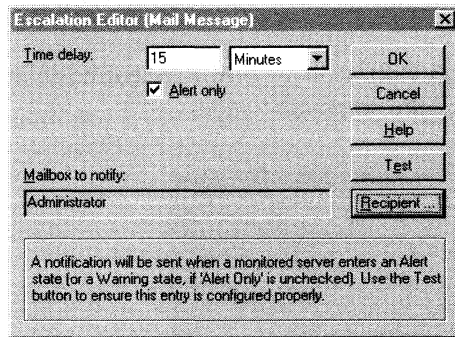


Option	Description
Time delay	The amount of time after the monitor enters an alert state or a warning state that you want the notification process to start. The default is 15 minutes.
Alert only	Select to send notification only if the monitor is in an alert state. Clear to send notification in both the warning and alert states.
File	Select a file name. This name appears in the Launch process box.
Command line parameters	Type special command-line parameters if appropriate.
Append notification text to parameter list	Select to attach the standard notification text to the parameters list specified in the Command line parameters box. Clear to avoid attaching any text to the parameter list.
Test	Verify that the process works as expected.

Using Mail Messages

You can use mail messages to alert a specified recipient when a problem occurs. This type of notification is useful for historical tracking and roving users.

1. Select the **Notification** tab.
2. Choose **New**.
3. Select **Mail Message**, and then choose **OK**.
4. Set the time delay when notification should occur, and the mailbox to notify.

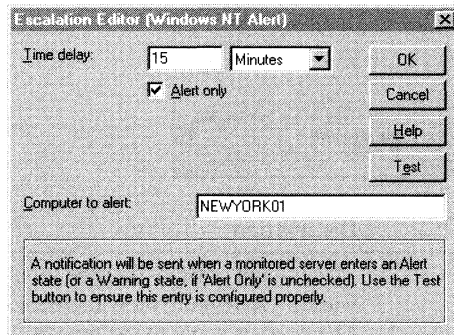


Option	Description
Time delay	The amount of time after the monitor enters an alert state or a warning state that you want the notification process to start. The delay is equal to the greater of the time delay or polling interval. The default is 15 minutes.
Alert only	Select to send notification only if the monitor is in an alert state. Clear to send notification in both the warning and alert states.
Recipient	Select a name from a list of recipients. This name appears in the Mailbox to notify box.
Test	Verify that the message is sent correctly.

Using Network Alerts

You can use network alerts to send an alert message to a computer. However, an alert message cannot be delivered if the computer is not turned on, no one is currently logged on to the computer, or the messaging service is not running. This type of notification is best for monitoring users on the same local area network (LAN) as the monitor.

1. Select the **Notification** tab.
2. Choose **New**.
3. In the **New Notification** dialog box, select **Windows NT Alert**, and then choose **OK**.
4. In the **Escalation Editor** dialog box, set the time delay when notification should occur and the computer to notify.



Option	Description
Time delay	The amount of time after the monitor enters an alert state or a warning state that you want the notification process to start. The default is 15 minutes.
Alert only	Select to send notification only if the monitor is in an alert state. Clear to send notification in both the warning and alert states.
Computer to alert	Type the name of the computer to receive the alert message.
Test	Verify that the message is sent correctly.

Modifying a Notification

You can change existing notifications. For example, you can change the time delay or the recipient of a mail message alert.

1. Select the **Notification** tab.
2. Select a notification, and then choose **Edit**.
3. In the **Escalation Editor** dialog box, make the changes, and then choose **OK**.

Removing a Notification

When you no longer want to use a particular notification, you can remove it from the list.

1. Select the **Notification** tab.
2. Select the notification you want to remove, and then choose **Remove**.

Link Monitoring Within an Organization

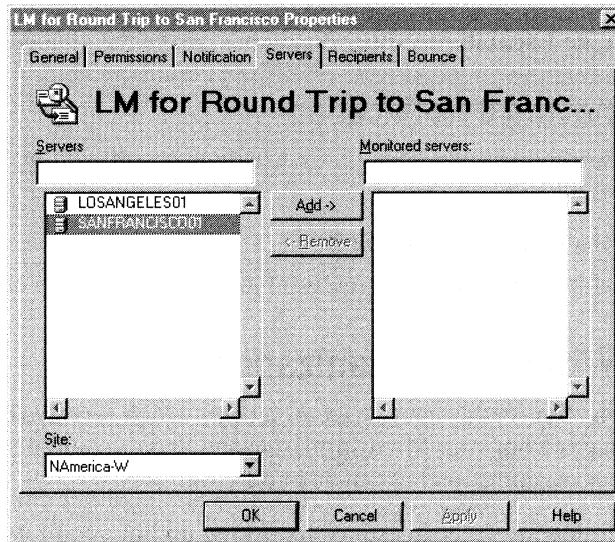
Use the **Servers** property page to specify which servers should receive ping messages from your Microsoft Exchange Server computer. The servers must be in your organization but can be in different sites.

The following are suggestions for setting up link monitors.

- When setting up link monitors, pay attention to routing costs and scheduling.
- When setting warning and alert durations, keep in mind the expected durations for each connection. This allows you to determine whether they are working as expected.

Getting to the Servers property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the link monitor you want to update.
3. Select the **Servers** tab.



Specifying Servers for Link Monitoring

Use the **Servers** property page to specify which servers in your organization should be monitored.

1. Select the **Servers** tab.
2. In the **Servers** box, select a server you want to monitor.
3. Choose **Add** to add the selected server to the list of monitored servers.

Removing Servers from Link Monitoring

If you no longer need to monitor a server, you can remove it from the list.

1. Select the **Servers** tab.
2. In the **Monitored servers** box, select a server, and then choose **Remove**.

Link Monitoring Outside an Organization

Use the **Recipients** property page to configure a link monitor that checks connections to other organizations or foreign systems. The link monitor checks for replies to ping messages sent to recipients. Based on whether or not a reply is returned, you can determine whether the link is working correctly.

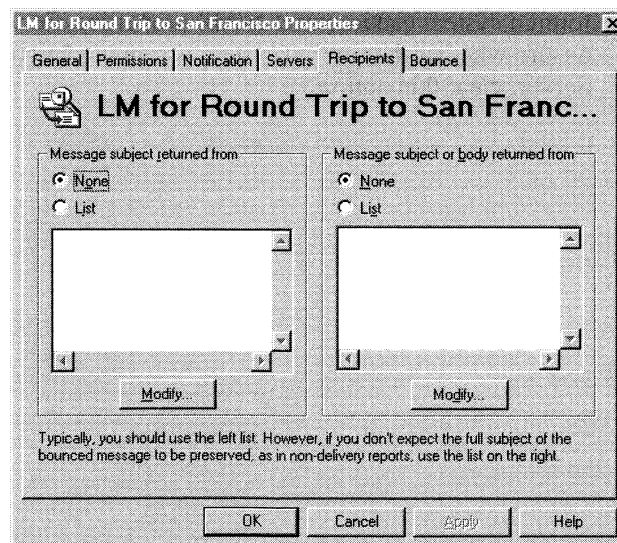
When you test a connection using a link monitor, specify a recipient that does not exist so you will be sent an NDR. If you specify an existing recipient, you will not receive a reply and will not know whether the ping message reached the recipient.

When the link monitor receives a reply, it does not read the contents of the message but instead looks for the subject of the original message. You must specify how you expect the subject of the original message to be returned. If you know that the recipient's system has an automatic reply program (and that the program puts the original subject text in the reply subject field), specify the **Message subject returned from** box. If you do not know how the recipient will return the subject, specify the **Message subject or body returned from** box.

Note The NDR does not contain the name of the recipient that sent it, so the NDR could have been sent from a system anywhere along the connection path.

Getting to the Recipients property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the link monitor you want to update.
3. Select the **Recipients** tab.



Tips for Monitoring Links to Foreign Systems

If you control or have access to the foreign system:

- Write a utility that recognizes Microsoft Exchange Server ping messages.
- If you can ensure that the subject of the original ping message will be included in the subject of the returned ping message, add the recipient to the **Message subject returned from** box.

If you do not control or have access to the foreign system:

- Try sending a ping message to a mailbox that doesn't exist. A message with an invalid address would make it across the gateway and into the system. However, it would be rejected as invalid by the foreign system and returned to Microsoft Exchange Server addressed to the sender. On return, examine the subject and body of the ping message to see if the subject or body is preserved. If the subject is preserved, add the recipient to the **Message subject returned from** box. If only the body is preserved, add the recipient to the **Message subject or body returned from** box.
- Create a custom recipients container for the invalid recipients used by this link monitor. It is recommended that after custom recipients have been set up, you use the custom recipients **Advanced** property page and select **Hide from Address Book**. This prevents anyone from accidentally sending messages to invalid addresses.
- Clear the **MAPI Recipients** option if you are not sure whether the foreign system can interpret MAPI properties. For example, if you are unsure whether the foreign system is running Microsoft Exchange Server, clear this option.

Specifying Recipients That Return Subjects

You can specify a recipient that responds with the original subject in the subject line. Using the **Message subject returned from** option saves time because the body of the message does not need to be opened.

1. Select the **Recipients** tab.
2. Under **Message subject returned from**, choose **Modify**.
3. Select the names of the recipients, and then choose **Add**.

Specifying Recipients That Return the Subject or Message Body

You can specify a recipient that responds with the original subject in either the subject line or the message body. Use the **Message subject or body returned from** option if you don't know whether the recipient returns the subject in the subject line or in the message body.

1. Select the **Recipients** tab.
2. Under **Message subject or body returned from**, choose **Modify**.
3. Select the names of the recipients, and then choose **Add**.

Link Status

Link status shows the last bounce message sent to each server and provides details about the time the message spent between key points in the path. You can use this information to determine why a message has exceeded its maximum acceptable threshold. Also, link properties show the status of notifications sent in response to alerts and whether notifications and repairs have been suspended.

Note The link monitor must have been active for at least the time period specified in the **Bounce** property page.

Getting to the General property page

1. In the Administrator window, choose **Monitors**, and then choose a link monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name or browse for the server you want to connect to, and then choose **OK**.
4. Double-click the appropriate link monitor, and then select the **General** tab.

NAmerica-E1NEWYORK01 Properties

General | Notification | Maintenance status

NAmerica-E1NEWYORK01

Last received bounce mail

Request sent:	Request time:	
6/4/97 3:03 PM	0:00:01	
Request received:	Turnaround time:	Total time:
6/4/97 3:03 PM	0:00:42	0:00:49
Reply sent:	Reply time:	
6/4/97 3:04 PM	0:00:06	
Reply received:		
6/4/97 3:04 PM		

Pending request:

OK Cancel Apply Help

Viewing the Last Received Bounce Mail Details

Use the **General** property page to view the results of the last successful bounce message. These values are informational and cannot be changed.

Option	Description
Request sent	The time the ping message was submitted by the system attendant on the sending server.
Request received	The time the ping message was received by the information store on the destination server.
Request time	The elapsed time between request sent and request received.
Reply sent	The time the system attendant on the destination server sent the ping message back.
Turnaround time	The elapsed time between request received and reply sent. This includes processing time of the system attendant on the destination server.

(continued)

Option	Description
Reply received	The time the link monitor received a reply to the ping message.
Reply time	The elapsed time between reply sent and reply received. This includes message transfer agent (MTA) transport time on both servers.
Total time	The elapsed time between request sent and reply received.
Pending request	The date and time of all ping messages sent but not yet returned.

Link Notification

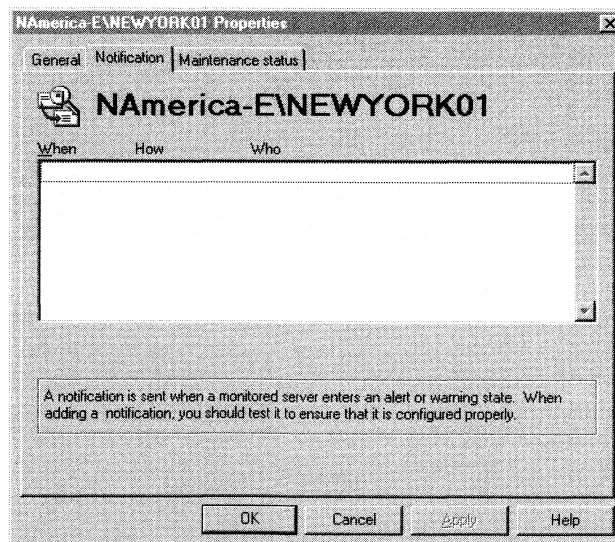
Use the **Notification** property page to view the current outstanding notification for a link. These values are informational and cannot be changed.

Getting to the link Notification property page

1. In the Administrator window, choose **Monitors**, and then choose a link monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name or browse for the server you want to connect to, and then choose **OK**.

Note The link monitor must have been active for at least the time period specified in the **Bounce** property page.

4. Double-click the connection that you want, and then select the **Notification** tab.



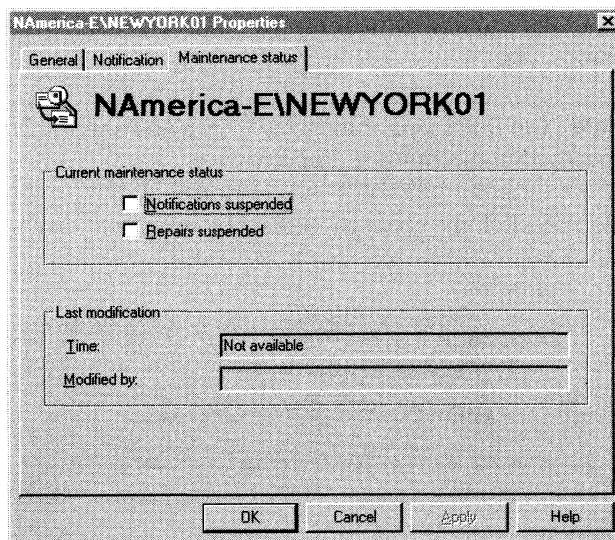
For more information on setting notifications, see “Notification Process” earlier in this chapter.

Link Maintenance Status

Maintenance status shows the current operating condition of maintenance notifications and repairs.

Getting to the Maintenance status property page

1. In the Administrator window, choose **Monitors**, and then choose a link monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name or browse for the server you want to connect to, and then choose **OK**.
4. Double-click the link that you want, and then select the **Maintenance status** tab.



Viewing the Maintenance Status Details

Use the **Maintenance status** property page to view the maintenance status and see who made the last modification and when. These values are informational and cannot be changed.

Note The maintenance status can be changed manually using options available with the **admin** command. For information, see “Manual Monitor Startup and Shutdown” later in this chapter.

Option	Description
Notifications suspended	Indicates whether notifications are stopped during maintenance.
Repairs suspended	Indicates whether repairs are stopped during maintenance.
Time	Shows the time of the last modification.
Modified by	Shows the name of the last person who made a modification.

Server Monitor

Server monitors check services running on servers in the site by using remote procedure calls (RPCs). They also check servers in other sites if the servers are connected with RPCs. No special permissions are required to check the state of services on servers in a remote site. However, without the correct permissions on those servers, it will not be possible for a monitor to synchronize the clocks or restart services.

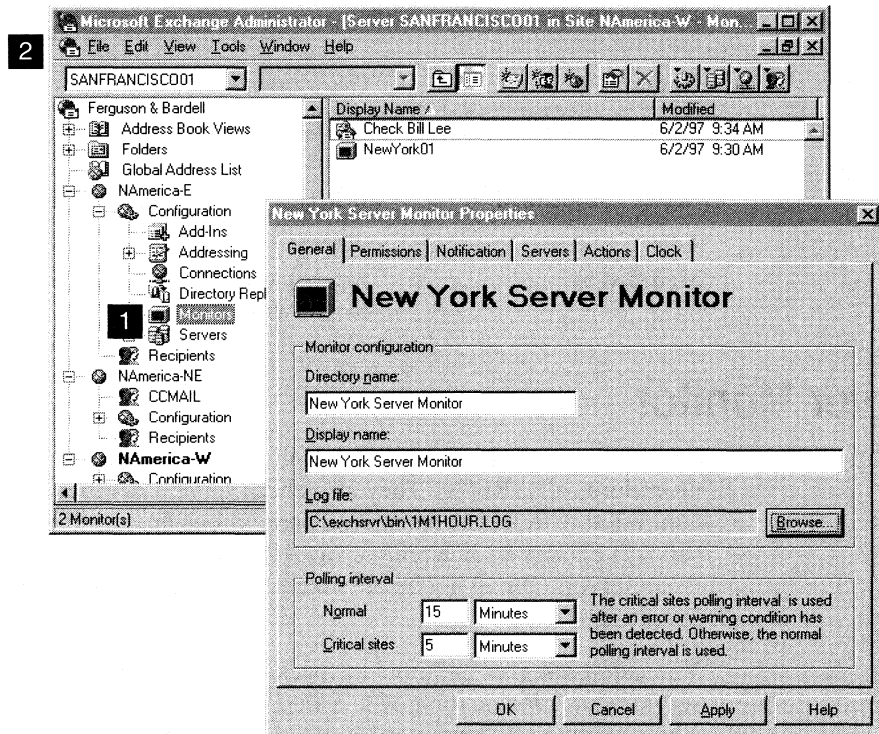
You can use server monitors to check the condition of all servers, including services and clocks, running at a site. You can also specify the notification actions when a service or computer has stopped, including restarting servers and services and resetting clocks.

One server monitor can monitor multiple servers, and each Administrator program can have multiple server monitors running. If you have different people to notify for different groups of servers, you can create multiple server monitors.

Server Monitor Configuration

Before you can use a server monitor, you must set up and configure it. For example, you may want the server monitor to synchronize the clock daily.

1. In the Administrator window, choose **Monitors**.
2. From the **File** menu, choose **New Other**, and then choose **Server Monitor**.



General Properties

Use the **General** property page to define a directory name and a display name, create a log file, and set polling intervals.

Getting to the General property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the server monitor you want to view or update.
3. Select the **General** tab.

Defining the Directory Name and the Display Name

Use the **General** property page to define a directory name and a display name for this server monitor. You provide a directory name used for identification by the system and a display name that appears in the Administrator window.

1. Select the **General** tab.
2. In the **Directory name** box, type a name.
3. In the **Display name** box, type a name.

Option	Description
Directory name	A maximum of 64 alphanumeric characters, which can include spaces and special characters. If no name is provided, the system prompts for a value.
Display name	A maximum of 256 alphanumeric characters. This is the name that is displayed in the Administrator window. The syntax of this field is Unicode, which understands all languages and their special characters. If no name is provided, the system prompts for a value.

Creating Log Files

The log file stores information about servers and systems configured for that server monitor. The log contains the results of RPC requests for information. Creating log files is optional. However, they are helpful for troubleshooting problems with services within your organization. If no path and file name are specified, a log file is not created.

Tip The log file is easy to find on the network if you specify the path using the UNC, such as \\Servername\C\$\S1m1hour.log.

1. Select the **General** tab.
2. Choose **Browse**.
3. Type or select the path and file name for the log file, and then choose **OK**.

Setting Polling Intervals

Use polling intervals to indicate how often the server monitor checks services. In a normal site, services are running, and the clock is not off by more than a specified interval. A critical site does not meet the criteria defined for a normal site. Because of this, the default polling interval for a normal site is longer than that of a critical site. Polling intervals for both normal and critical sites can be set to any duration.

1. Select the **General** tab.
2. In the **Normal** box, type a number, and then select either **Seconds**, **Minutes**, or **Hours**.
3. In the **Critical sites** box, type a number, and then select either **Seconds**, **Minutes**, or **Hours**.

Option	Description
Normal	Indicate how often the monitor is to check services. The default is 15 minutes.
Critical sites	Indicate how often the monitor is to check services on servers that are in a warning or alert state. The default is 5 minutes.

Permissions

Use the **Permissions** property page to identify which Windows NT accounts can modify the specified monitor. Permissions are necessary when a server monitor is being modified but are not necessary to start a server monitor.

Note By default, the **Permissions** property page is hidden. To view it, choose **Options** from the **Tools** menu.

For more information on permissions, see *Microsoft Exchange Server Getting Started*.

Notification Process

Use the **Notification** property page to specify how to notify administrators when a service is in a warning state or an alert state. A *warning state*, indicating a possible problem, occurs when the clock is off by a small amount. An *alert state*, indicating a serious problem, occurs when a service is not working, a server does not respond, or the clock is off by a large amount. The symbols in the left column of the **Notification** property page indicate whether the notification is for an alert state (red down arrow) or a warning state (red exclamation point).

Notifications can be delivered as:

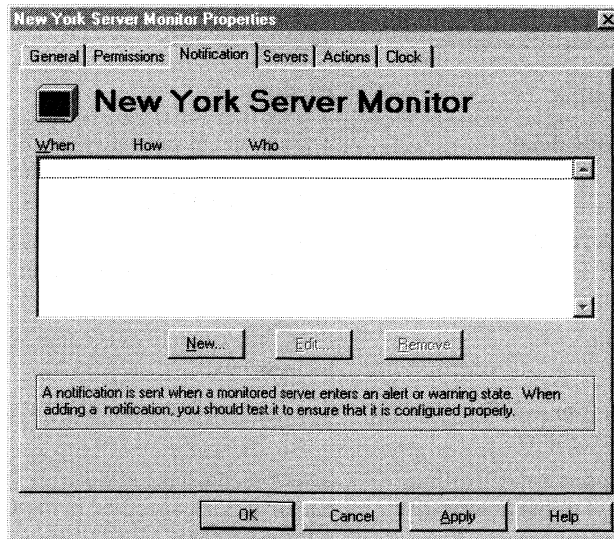
- Notification applications, such as pager programs
- Mail messages
- Network alerts

Once you determine the type of notification, you can specify how administrators should be notified by setting the escalation path. An *escalation path* is a prioritized list of people to notify when a monitor enters a warning or an alert state. This list is useful for notifying primary and secondary support personnel. For example, the primary support person can be notified immediately when the monitor enters a warning state. The secondary people that need to be notified can have a longer time delay or not be notified until the monitor enters an alert state.

For example, you could set a staggered time for three support people: a primary support person and two secondary support people. These three notifications could be staggered from immediate notification to one hour. You must complete the notification setup process three times, once for each person.

Getting to the Notification property page

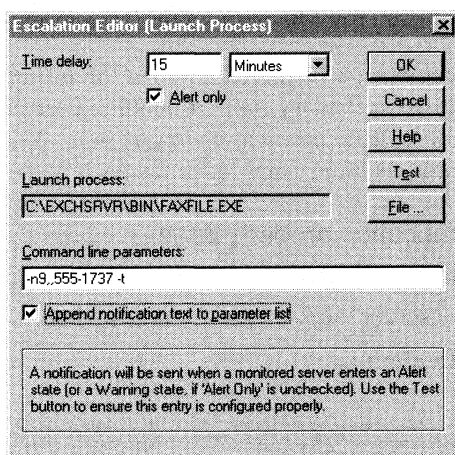
1. In the Administrator window, choose **Monitors**.
2. Double-click the server monitor you want to update.
3. Select the **Notification** tab.



Using Notification Applications

You can use notification applications to alert users who are not logged on to the network. This is appropriate for an administrator who monitors the network remotely using a pager program.

1. Select the **Notification** tab.
2. Choose **New**.
3. Select **Launch a Process**, and then choose **OK**.
4. Set the time delay when notification should occur and the appropriate notification parameters.

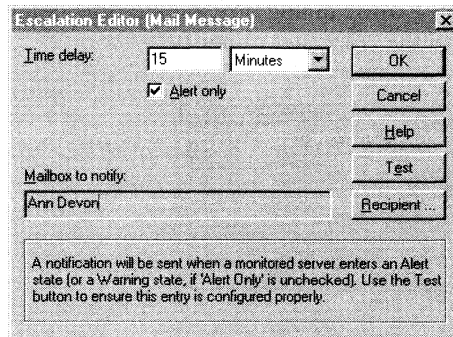


Option	Description
Time delay	The amount of time after the monitor enters an alert state or a warning state that you want the notification process to start. The default is 15 minutes.
Alert only	Select to send notification only if the monitor is in an alert state. Clear to send notification in both the warning state and the alert state.
File	Select a file name. This name appears in the Launch process box.
Command line parameters	Type special command-line parameters if appropriate.
Append notification text to parameter list	Select to attach the standard notification text to the parameters list specified in the Command line parameters box. Clear to avoid attaching any text to the parameter list.
Test	Verify that the process works as expected.

Using Mail Messages

You can use mail messages to alert a specified recipient when a problem occurs. This type of notification is useful for historical tracking.

1. Select the **Notification** tab.
2. Choose **New**.
3. Select **Mail Message**, and then choose **OK**.
4. Set the time delay when notification should occur and the mailbox to notify.

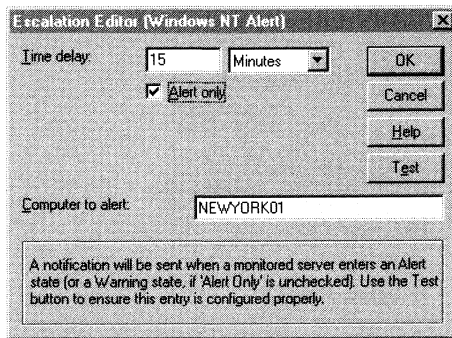


Option	Description
Time delay	The amount of time after the monitor enters an alert state or a warning state that you want the notification process to start. The delay is equal to the greater of the time delay or polling interval. The default is 15 minutes.
Alert only	Select to send notification only if the monitor is in an alert state. Clear to send notification in both the warning and alert states.
Recipient	Select a name from a list of recipients. This name appears in the Mailbox to notify box.
Test	Verify that the message is sent correctly.

Using Network Alerts

You can use network alerts to send an alert message to a computer. However, an alert message cannot be delivered if the computer is not turned on or no one is currently logged on to the computer.

1. Select the **Notification** tab.
2. Choose **New**.
3. In the **New Notification** dialog box, select **Windows NT Alert**, and then choose **OK**.
4. In the **Escalation Editor** dialog box, set the time delay, when notification should occur, and the computer to notify.



Option	Description
Time delay	The amount of time after the monitor enters an alert state or a warning state that you want the notification process to start. The default is 15 minutes.
Alert only	Select to send notification only if the monitor is in an alert state. Clear to send notification in both the warning and alert states.
Computer to alert	Type the name of the computer to receive the alert message.
Test	Verify that the message is sent correctly.

Modifying a Notification

You can change existing notifications. For example, you can change the time delay or the recipient of a mail message alert.

1. Select the **Notification** tab.
2. Select a notification, and then choose **Edit**.
3. In the **Escalation Editor** dialog box, make the appropriate changes, and then choose **OK**.

Removing a Notification

When you no longer want to use a particular notification, you can remove it from the list.

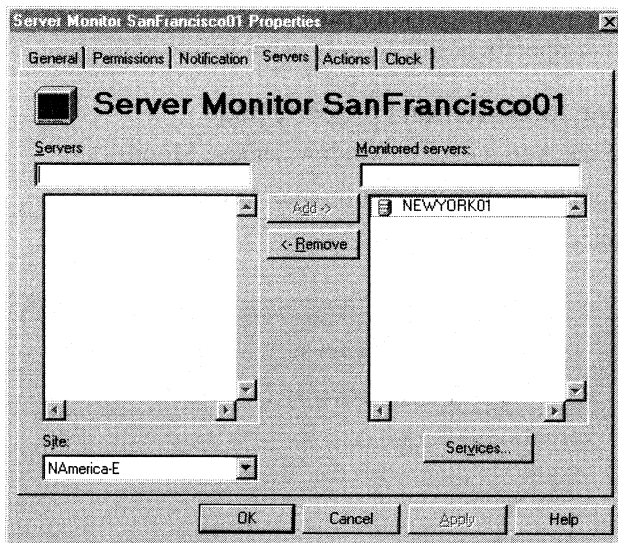
1. Select the **Notification** tab.
2. Select the notification you want to remove, and then choose **Remove**.

Server Monitoring Within an Organization

Use the **Servers** property page to specify which servers should be monitored. Servers to be monitored using a server monitor must have LAN connectivity.

Getting to the Servers property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the server monitor you want to update.
3. Select the **Servers** tab.



Specifying Servers for Monitoring

Use the **Servers** property page to specify which servers in your organization should be monitored.

1. Select the **Servers** tab.
2. In the **Servers** box, select a server you want to monitor.
3. Choose **Add** to add the selected server to the list of monitored servers.

Removing Servers from Monitoring

If you no longer need to monitor a specific server, you can remove it from the list.

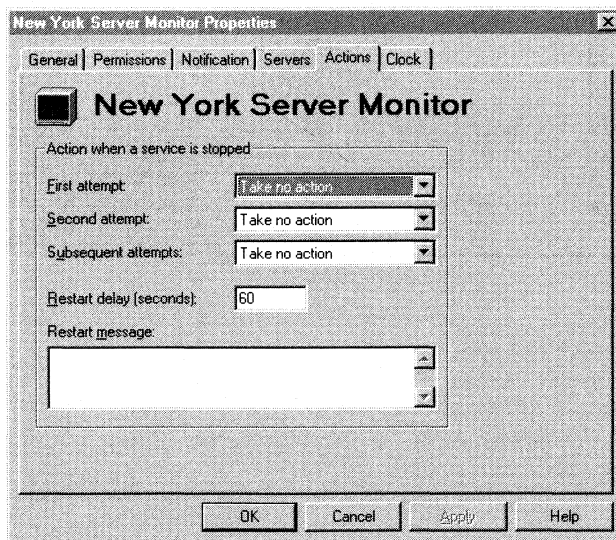
1. Select the **Servers** tab.
2. In the **Monitored servers** box, select a server, and then choose **Remove**.

Escalation Actions

Use the **Actions** property page to specify the escalation actions this server monitor takes when a service is not running. Actions and notification are independent. You can specify notification to occur before, during, or after actions.

Getting to the Actions property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the server monitor you want to update.
3. Select the **Actions** tab.



Specifying Escalation Actions

You can specify what action should be taken when a service is not running. One set of actions is used for all servers being monitored. You can create multiple server monitors if the monitored servers have different escalation actions.

Escalation occurs after an attempt to start the service has failed. Escalation attempts continue until the service successfully starts. When specifying options, be sure to consider how long it takes to restart your computer. For example, if the restart time is greater than the polling time and you choose to restart the computer, the action will fail repeatedly.

Caution Restarting the computer can interfere with other non-Microsoft Exchange Server services. If any of the monitored servers should not be restarted, do not select the **Restart the computer** option.

1. Select the **Actions** tab.
2. Under **Action when a service is stopped**, select an option in each attempt box.

Option	Description
Take no action	The server monitor should notify you only of a failed service.
Restart the service	The server monitor should attempt to restart the missing service.
Restart the computer	The server monitor should attempt to restart the computer with the missing service.

Specifying the Restart Delay

If you selected **Restart the computer** as one of the escalation actions, you can specify an interval before the computer is shut down. This delay gives those users using the server as a workstation time to save their work.

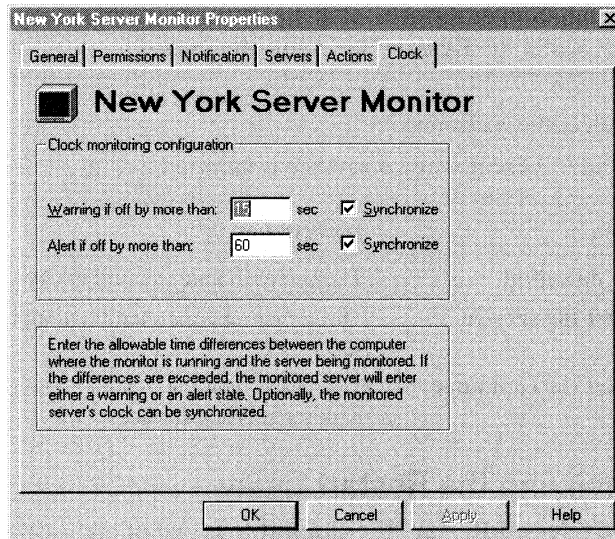
1. Select the **Actions** tab.
2. In any of the attempt boxes, select **Restart the computer**.
3. In the **Restart message** box, type a message that is to appear in the **Restart warning** box on the server to be restarted.

Clock Synchronization

Use the **Clock** property page to initiate an alert if a monitored server's internal clock is off by more than a specified number of seconds. You can also specify that the clocks of the monitored servers are synchronized with the monitoring computer's clock.

Getting to the Clock property page

1. In the Administrator window, choose **Monitors**.
2. Double-click the server monitor you want to update.
3. Select the **Clock** tab.



Setting Up Alerts

Use the **Clock** property page to specify the amount of time the clocks of the monitored servers and the server monitor can differ before notification occurs.

1. Select the **Clock** tab.
2. In the **Warning if off by more than** box, type the minimum number of seconds the two clocks can differ before a warning notification occurs.
3. In the **Alert if off by more than** box, type the minimum number of seconds the two clocks can differ before an alert notification occurs.

Setting Up Clock Synchronization

If you are monitoring services on servers in other time zones, you can specify that the clocks of the monitored servers are synchronized with the monitoring computer's clock. Synchronization uses the time zone information in Windows NT Server so monitors can function correctly with servers in other time zones. Clock synchronization ensures that time-based events such as message tracking and event logs are recorded accurately.

1. Select the **Clock** tab.
2. Select the **Synchronize** check boxes if you want the clocks of monitored servers to be synchronized with the server monitor's clock.

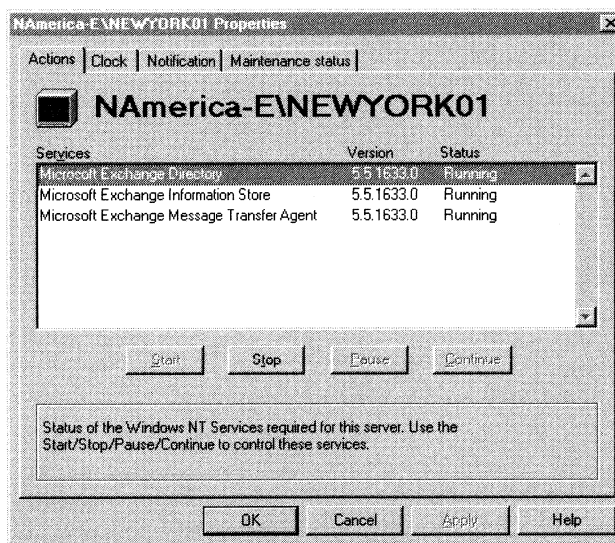
For more information on synchronization, see Chapter 4, "Troubleshooting Tools and Resources."

Server Status

Server status shows the last check performed on each server. The data shown provides details about the time of the last measurement performed and tracks the time of the last change. This information can be used to determine how a server is performing.

Getting to the Actions property page

1. In the Administrator window, choose **Monitors**, and then choose a server monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name or browse for the server you want to connect to, and then choose **OK**.
4. Double-click the server that you want, and then select the **Actions** tab.



Changing the Component Status

You can use the **Actions** property page to start, stop, pause, and continue service on any component or connector. The status is shown in real time, and the display is updated for each polling interval.

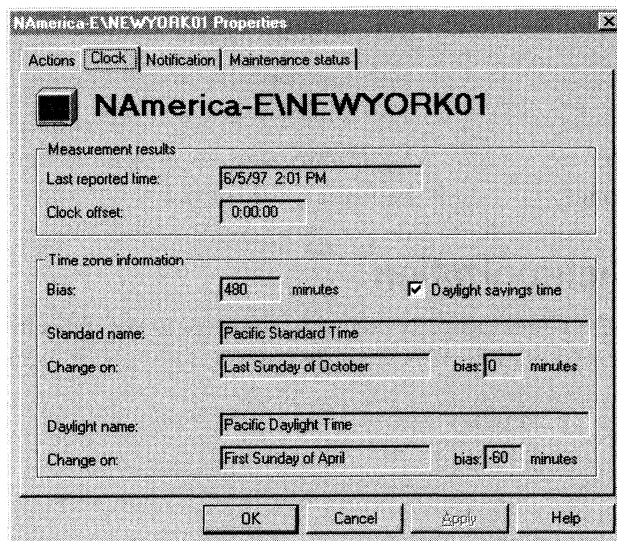
Option	Description
Services	Lists the components and connectors monitored.
Version	Lists the version of the service, if known.
Status	Lists the current status as determined by its response to the poll sent by the monitor.
Start	Starts a stopped service.
Stop	Stops a running service.
Pause	Temporarily stops a running service.
Continue	Restarts a paused service.

Server Clock Synchronization

Use the **Clock** property page for the server to see measurement results and time zone information. This property page is read-only; it cannot be edited.

Getting to the Clock property page

1. In the Administrator window, choose **Monitors**, and then choose a server monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name or browse for the server you want to connect to, and then choose **OK**.
4. Double-click the server that you want, and then select the **Clock** tab.



Option	Description
Last reported time	The time on the server's clock when the last monitored check occurred.
Clock offset	The difference between the clock on the server being monitored and the clock on the server running the server monitor.
Bias	The difference between the server clock time and Coordinated Universal Time (UTC).
Daylight savings time	The box selected when an adjustment is made for daylight saving time.
Standard name	The name of the standard local time for the server being monitored.
Change on	The day when standard local time changes to daylight saving time.
Daylight name	The name of the alternate local time for daylight saving.
Change on	The day when daylight saving time changes to standard local time.

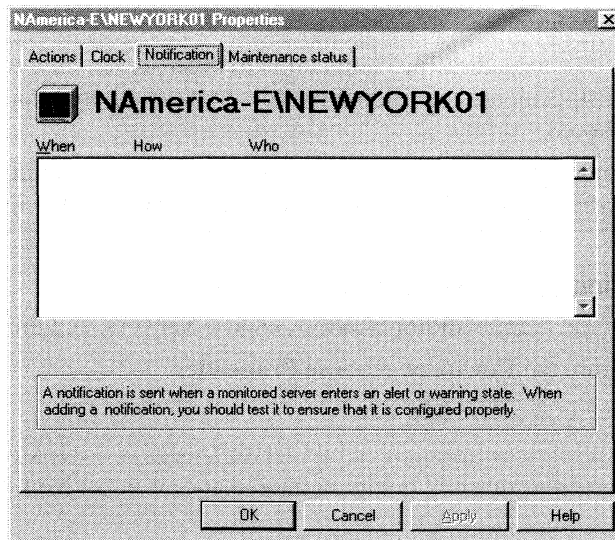
Server Notification

When a monitored server component does not respond, the server monitor starts processing the instructions for notifying people in the organization. These instructions are set in the **Notification** property page.

Use the monitored server's **Notification** property page to see who has been notified and how. Use the server monitor's **Notification** property page to determine if the instructions are being processed correctly and to anticipate notifications if the problem continues. This page is read-only; it cannot be edited.

Getting to the Notification property page

1. In the Administrator window, choose **Monitors**, and then choose a server monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name or browse for the server you want to connect to, and then choose **OK**.
4. Double-click the server that you want, and then select the **Notification** tab.



Option	Description
When	The time the notice was sent.
How	The method used for notification. The options are launch a process, send a message, or display a Windows NT alert.
Who	The person, mailbox, or computer notified.

Server Maintenance Status

Use the monitored server's **Maintenance status** property page to determine if the server is down for scheduled maintenance. The server monitor may have missed the server going into maintenance status. This happens when the server monitor does not poll the server while the server is still able to indicate that maintenance has been selected.

For more information about checking the maintenance status, see “Link Maintenance Status” earlier in this chapter.

Services to Monitor

By default, the only Microsoft Exchange Server services to be monitored are the directory, information store, and MTA. You can also monitor any Windows NT Server service running on a Microsoft Exchange Server computer.

Use the **Services** property page to specify which additional services you want to monitor. When services are configured to be monitored, that information is stored in the directory. This information is replicated to all servers in the organization where all monitors can find it.

Note Because directory replication to other servers in the same and other sites is not instantaneous, additional services to be monitored may not be immediately monitored.

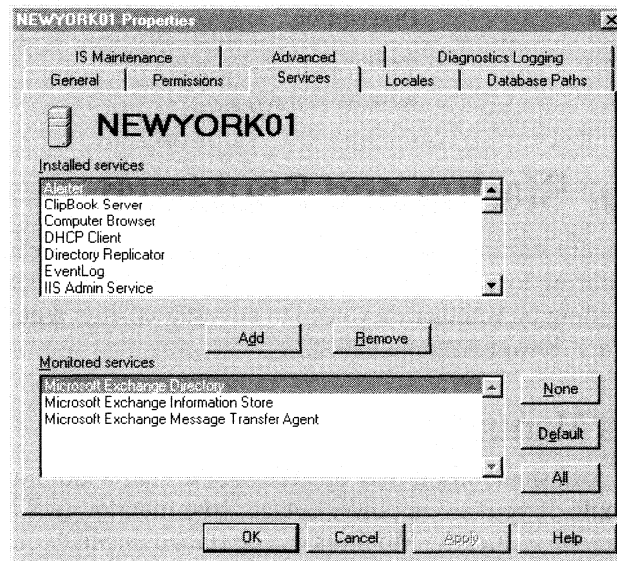
Monitors that are running do not pick up changes. You must restart the monitor after the data is replicated into the local directory of the monitoring server.

Getting to the Services property page

1. In the Administrator window, choose **Servers**, and then select a server.
2. From the **File** menu, choose **Properties**.
3. Select the **Services** tab.

All services installed on this server appear in the **Installed services** box. All services currently being monitored appear in the **Monitored services** box.

Note You can also choose **Services** in the **Servers** property page of a monitor to get to the **Services** property page.



Adding a Service

You can add selected services or all services to those being checked by this server monitor.

Note You must restart the monitor after services are added.

1. Select the **Services** tab.
2. Add the services you want to monitor.

Option	Description
Add	Adds the service selected in the Installed services box.
Default	Adds only installed Microsoft Exchange Server services.
All	Adds all services.

Removing a Service

If you no longer need to monitor some services, you can remove them from the list of monitored services.

Note You must restart the monitor after services are removed.

1. Select the **Services** tab.
2. Remove the services you no longer want to monitor.

Option	Description
Remove	Removes a selected service.
None	Removes all services.

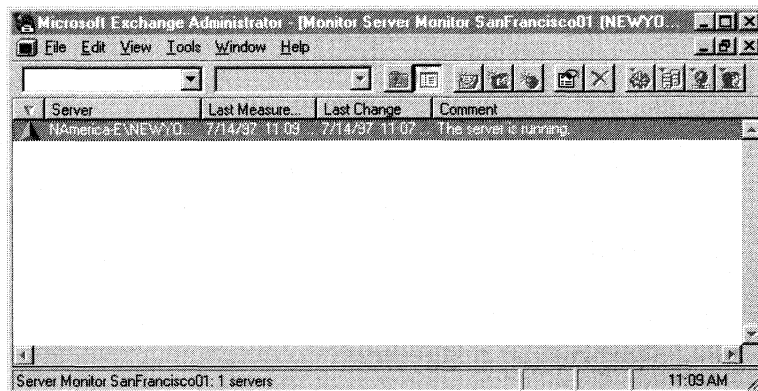
Manual Monitor Startup and Shutdown

Manually starting and stopping server and link monitors allows you to control monitoring for specific computers. You can selectively start and stop computers, depending on whether they need to be restarted after a power outage or whether they are down for maintenance.

Starting Monitors Manually

In certain situations, it may be necessary to start a monitor manually. For example, if you have a power outage, your monitor goes down and it is not set to restart automatically. Monitors can be started manually in the Administrator program or automatically from the command line. Monitors must be started before monitoring will function correctly.

1. In the Administrator window, choose **Monitors**, and then choose a monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name of the server you want to connect to, and then choose **OK**.



The symbols in the state column indicate the condition of the link as shown in the following table.

Symbol	Meaning
Question mark (?)	Unknown.
Green up arrow	Messages returning in normal time.
Red exclamation point	Link or server is in a warning state.
Red down arrow	Link or server is in an alert state.

For information on starting monitors automatically, see “Starting Link and Server Monitors Automatically” later in this chapter.

Pausing Monitors

When you take a computer down for maintenance or perform a backup, you can temporarily stop the monitoring actions that are scheduled for that computer or server. For example, any repairs or notifications initiated by a link or server monitor can be ignored while the computer is down for scheduled maintenance. This avoids unnecessary alerts, notifications, and system repairs from being sent.

You can use the **admin /t** command to temporarily suspend repairs and notifications initiated by link or server monitoring. You can use this command in an automated process for scheduled maintenance or you can use it from the command line.

Note When performing maintenance on a server, you must set the **admin /t** command to start before the server goes offline. Consider the polling intervals of the monitors and be sure that each monitor receives a notification reporting a change in maintenance status before the server goes down.

Option	Description
-t r	Suspends repairs during maintenance, but sends a notification if a problem is found.
-t n	Suspends notification during maintenance, but initiates any repairs specified by the monitor.
-t nr	Suspends both notification and repairs during maintenance.
-t	Resets the monitor to normal.

Note Either the dash (-) or slash (/) can be used in the command line option.

Windows NT Performance Monitor

Performance Monitor is a Windows NT tool that can be used with Microsoft Exchange Server. It provides a graphical user interface for measuring the performance of your computer and other computers on your network. Performance Monitor allows you to perform a variety of monitoring tasks, including:

- Monitoring hardware
- Comparing hardware before installation
- Monitoring workload queues
- Monitoring routing
- Detecting bottlenecks
- Tuning performance

Performance Monitor provides charting, alerting, and reporting capabilities that reflect current activity and ongoing logging. You can also open log files at a later time for browsing and charting as if they were reflecting current activity.

Monitoring involves looking at discrete components of a system. In Windows NT, an object represents an individual process, a section of shared memory, or a physical device. An object can have several counters associated with it. For example, the Memory object has many counters, including Available Bytes, Pages/Sec, and Page Faults/Sec. You can monitor any one of these memory counters.

Getting to the Windows NT Performance Monitor

1. From the **Start** menu, choose **Programs**.
2. Select **Administrative Tools**, and then select **Performance Monitor**.

For more information about Performance Monitor, see your Windows NT Server documentation.

Windows NT Performance Monitor Counters

You can monitor the values in Windows NT Performance Monitor counters to determine how Microsoft Exchange Server is performing or to track error conditions. The Performance Monitor counters used for showing system conditions are presented in two categories: general counters and Microsoft Exchange Server-specific counters. For a complete list of performance monitor counters, see the *Microsoft Exchange Server Resource Guide*.

Windows NT General Performance Monitor Counters

The complete list of Performance Monitor counters is extensive. The following table contains only those counters relevant to Microsoft Exchange Server.

Object	Counter	Uses
LogicalDisk	% Disk Time	Records the percentage of time a hard drive is either reading or writing. A sustained value above 90 percent indicates that the hard drive is a performance bottleneck. Use the diskperf command at the Windows NT command prompt to activate disk monitoring.
Memory	Pages/sec	Measures paging of memory from or to the virtual memory paging file. A high average value indicates the computer is short on memory. Sudden spikes in use should be ignored.
Processor	% Processor Time	Records the percentage of time the processor is running non-idle threads. If your server has multiple processors, you can watch each instance. Microsoft Exchange Server services can use multiple processors. An average value that is below 20 percent indicates the server is unused or services are down. An average value that is consistently above 90 percent indicates that the server is overburdened.
Process	Elapsed Time	Records the number of seconds a process has been running. It gives you a quick way to see whether a server or service has recently been restarted without looking through the event log.
Redirector	Bytes Total/sec	Measures the number of bytes per second sent and received by the network redirector. Compare the maximum throughput of your network card with the maximum value of this counter to see if network traffic is a bottleneck in your system.
Redirector	Network Errors/sec	Measures the number of unexpected errors the redirector receives. If you suspect network problems, check to see whether this counter is above zero. If it is above zero, check the system event log for details on the network error.

Microsoft Exchange Server Performance Monitor Counters

The following Windows NT Performance Monitor counters are designed specifically for Microsoft Exchange Server. This is a small sample of the most commonly used counters. You can convert any of these counters for use with Simple Network Management Protocol (SNMP) monitoring agents. For information about counters that you can use with SNMP, see “Chapter 4, “Troubleshooting Tools and Resources.”

Monitoring the Message Transfer Agent

Use these counters to monitor MTA activity.

Object	Counter	Description
MSExchangeMTA	Messages/Sec	A continuous average of the number of messages the MTA sends and receives each second. This is a good way to measure traffic sent to other servers.
MSExchangeMTA	Work Queue Length	A current count of messages in MTA queues awaiting delivery to other servers or processing by the MTA. Divide this value by Messages/Sec for a rough estimate of message delay in this queue before they are delivered or sent. A high number indicates a problem, either in performance or in transmitting to other servers.
MSExchangeMTA Connections	Queue Size	MTA Connections object counters display information for each connection established by the MTA. The Queue Size counter shows the number of objects in MTA queues to and from each connection.

Monitoring the Directory

Use these counters to monitor directory replication. When both counters reach zero, directory synchronization is complete.

Object	Counter	Description
MSExchangeDS	Pending Replication Synchronization	A current count of synchronization requests sent by this directory that are still unanswered. Check this counter after choosing Update Now in the directory General property page. This value should start high and decrease slowly as synchronization messages arrive.
MSExchangeDS	Remaining Replication Updates	A current count of synchronization updates waiting to be applied to the directory.

Monitoring the Information Store

Use these counters to monitor the activity of the information store. Each counter is available for both public and private information store objects.

Object	Counter	Description
MSExchangeISPriv MSExchangeISPub	Average Time for Delivery	The average length of time the last 10 messages waited in the information store queue to the MTA. Make note of this delay time when the load is low. A high value could indicate a performance problem with the MTA.
MSExchangeISPriv MSExchangeISPub	Average Time for Local Delivery	The average length of time the last 10 local delivery messages waited for transport to a mailbox in the same information store. Make note of this delay time when the load is low. A high value could indicate a performance problem with the private information store.
MSExchangeISPriv MSExchangeISPub	Logon Count	A current count of clients logged on to the information store.
MSExchangeISPriv MSExchangeISPub	Logon Active Count	A current count of clients logged on to the information store who have initiated some server activity within the last 10 minutes.
MSExchangeISPriv MSExchangeISPub	Messages Delivered/Min	A continuous average of the number of messages are delivered to the information store per minute. This includes messages submitted directly to the information store from clients on this server and messages delivered to the information store by the MTA.
MSExchangeISPriv MSExchangeISPub	Message Recipients Delivered/Min	A continuous average of the number of messages sent per minute divided by the number of recipients to which they were sent. This gives you a clearer picture of the actual number of deliveries.
MSExchangeISPriv MSExchangeISPub	Messages Sent/Min	A continuous average of the number of messages sent per minute from the information store to the MTA to be transported to other servers or gateways.

Monitoring the Microsoft Mail Connector

Use these counters to monitor Microsoft Mail Connector activity.

Object	Counter	Description
MSExchange MSMI	Messages Received	This counter measures how many messages have been received by Microsoft Exchange Server from the Microsoft Mail Connector. If this number is increasing, the connector is receiving mail. If this number is not changing, there could be either no mail to transfer or a problem.
MSExchange PCMTA	File contentions/ hour	The Microsoft Mail Connector (PC) MTA, any other Microsoft Mail (PC) MTA, and MS Mail clients try to read and write exclusively to key files in Microsoft Mail and Microsoft Mail Connector postoffices. It is normal for a few file contentions to occur. If too many occur, it could indicate a file is locked open or too much traffic is going through a particular postoffice.
MSExchange PCMTA	LAN/WAN Messages Moved/hour	Use to check Microsoft Mail Connector (PC) MTA performance. This counter should show similar numbers day to day for any given hour as long as there have been no configuration changes in it or other Microsoft Mail (PC) MTAs. Any strong deviance from the normal value should be investigated.

Monitoring the Internet Mail Service

Use these counters to monitor Internet Mail Service activity.

Object	Counter	Description
MSExchangeIMC	Queued MTS-IN	A current count of messages awaiting final delivery in Microsoft Exchange Server.
MSExchangeIMC	Bytes Queued MTS-IN	The size, in bytes, of messages that have been converted from Internet mail and are awaiting final delivery within Microsoft Exchange Server.
MSExchangeIMC	Messages Entering MTS-IN	A current count of messages entering the MTS-IN folder after conversion from Internet mail format.
MSExchangeIMC	Queued MTS-OUT	A current count of messages waiting to be converted to Internet mail format.
MSExchangeIMC	Bytes Queued MTS-OUT	The size, in bytes, of messages waiting to be converted to Internet mail format.
MSExchangeIMC	Messages Entering MTS-OUT	A current count of messages entering the MTS-OUT folder for conversion to Internet mail format.
MSExchangeIMC	Messages Leaving MTS-OUT	A current count of messages entering the outbound queue.
MSExchangeIMC	Connections Inbound	A current count of Simple Mail Transfer Protocol (SMTP) connections to the Internet Mail Service established by other SMTP hosts.

(continued)

Object	Counter	Description
MSExchangeIMC	Connections Outbound	A current count of SMTP connections the Internet Mail Service has established to other SMTP hosts.
MSExchangeIMC	Connections Total Outbound	A current count of successful SMTP connections that the Internet Mail Service has established since it was started.
MSExchangeIMC	Connections Total Inbound	The total number of SMTP connections the Internet Mail Service has accepted from other hosts since it was started.
MSExchangeIMC	Connections Total Rejected	The total number of SMTP connections that the Internet Mail Service has rejected from other hosts since it was started.
MSExchangeIMC	Connections Total Failed	The total number of SMTP connections the Internet Mail Service has attempted to other hosts that failed since it was started.
MSExchangeIMC	Queued Outbound	A current count of messages from Microsoft Exchange Server that are queued for delivery to the Internet.
MSExchangeIMC	Queued Inbound	A current count of messages received from the Internet destined for Microsoft Exchange Server.
MSExchangeIMC	NDRs Total Inbound	The total number of NDRs generated for inbound mail.
MSExchangeIMC	NDRs Total Outbound	The total number of NDRs generated for outbound mail.
MSExchangeIMC	Total Inbound Kilobytes	The total size, in kilobytes, transferred to Microsoft Exchange Server.
MSExchangeIMC	Total Outbound Kilobytes	The total size, in kilobytes, transferred from Microsoft Exchange Server.
MSExchangeIMC	Inbound Messages Total	The total number of Internet messages delivered to Microsoft Exchange Server.
MSExchangeIMC	Outbound Messages Total	The total number of outbound messages delivered to their destinations.

Monitoring the Microsoft Exchange Connector for Lotus cc:Mail

Use these counters to monitor the Microsoft Exchange Connector for Lotus cc:Mail activity.

Object	Counter	Description
MSExchange CCMC	NDRs to Microsoft Exchange	Number of NDRs submitted to Microsoft Exchange Server by the connector since the Microsoft Exchange Connector for Lotus cc:Mail service was started.
MSExchange CCMC	NDRs to Lotus cc:Mail	Number of NDRs submitted to Lotus cc:Mail by the connector since the Microsoft Exchange Connector for Lotus cc:Mail service was started.
MSExchange CCMC	Messages sent to Microsoft Exchange/hr	Average number of messages sent per hour from Lotus cc:Mail to Microsoft Exchange Server.
MSExchange CCMC	Messages sent to Lotus cc:Mail/hr	Average number of messages sent per hour from Microsoft Exchange Server to Lotus cc:Mail.
MSExchange CCMC	Microsoft Exchange MTS-IN	The number of messages in the MTS-IN queue awaiting delivery to Microsoft Exchange Server.
MSExchange CCMC	Microsoft Exchange MTS-OUT	The number of messages in the MTS-OUT queue awaiting delivery to the Microsoft Exchange Connector for Lotus cc:Mail information store.
MSExchange CCMC	Messages sent to Microsoft Exchange	The number of messages sent from Lotus cc:Mail to Microsoft Exchange Server since the Microsoft Exchange Connector for Lotus cc:Mail service was started.
MSExchange CCMC	Messages sent to Lotus cc:Mail	The number of messages sent from Microsoft Exchange Server to Lotus cc:Mail since the Microsoft Exchange Connector for Lotus cc:Mail service was started.
MSExchange CCMC	DirSync to Microsoft Exchange	The number of directory entries updated in the Microsoft Exchange Server global address list since the last directory synchronization cycle.
MSExchange CCMC	DirSync to Lotus cc:Mail	The number of directory entries updated in the Lotus cc:Mail address list since the last directory synchronization cycle.

Automatic Logon and Startup

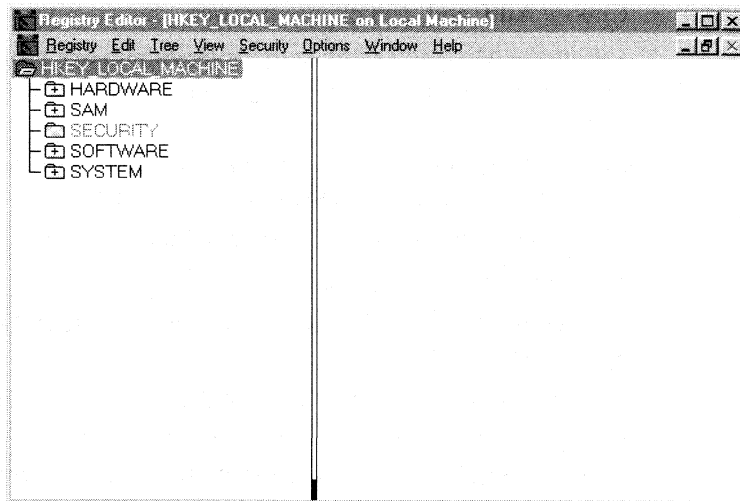
If you need your messaging system to run 24 hours a day, monitors should also run 24 hours a day. Power surges or outages can restart computers. When this happens, the computer must log on and start the monitor without assistance.

Logging On to Windows NT Server Automatically

If there is a power failure, no one may be available to log on to Windows NT Server when the power is restored. In this case, you can configure Windows NT to log on automatically at startup.

Important The Windows NT Server account configured to automatically log on at startup should be an account that has at least user-level permission on the monitors. It must also have sufficient permission for notification alerts and programs and for any escalation or clock synchronization actions to be taken.

1. From the **Start** menu, choose **Run**.
2. In the **Open** box, type **REGEDT32.EXE**, and then choose **OK** to start the Registry Editor.



3. From the **Window** menu, choose **HKEY_LOCAL_MACHINE**, and then open the following subkey:

SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

4. If the AutoAdminLogon entry appears in the subkey, double-click the entry and skip to step 7. If it does not appear, choose **Add Value** from the **Edit** menu.
5. In the Value Name box, type AutoAdminLogon.

6. In the **Data Type** box, select **REG_SZ**, and then choose **OK**.
7. In the **String** box, type **1**, and then choose **OK**.
8. From the Edit menu, choose **Add Value**.
9. In the **Value Name** box, type **DefaultPassword**.
10. In the **String** box, type the password for the default user, and then choose **OK**.
11. Check the string values of the entries LegalNoticeCaption and LegalNoticeText. If there is any text in either of these entries, you must remove it for automatic logon to occur.
12. From the **Registry** menu, choose **Exit** to save the changes and close the Registry Editor.

Starting Link and Server Monitors Automatically

Link and server monitors can be set to restart automatically when the Administrator program is started. This makes administration easier by not requiring you to manually start each monitor at startup.

1. From the **Start** menu, choose **Settings**.
2. Choose **Taskbar**, and then select the **Start Menu Items** tab.
3. Choose **Add**, and then choose **Browse**.
4. Locate the Microsoft Exchange Server Admin.exe program, and then double-click the program icon. This program is usually located in the \Exchsrvr\bin subdirectory.
5. In the **Command Line** box, add the **/m** option with the site name, monitor name, and server name in the following format:

path\admin.exe /m[site name]\monitor name\server name

For example, the complete command line could read:

c:\Exchsrvr\Bin\admin.exe /mNAmerica-W\Head Office Servers\Alpha103

Multiple monitors can be started on the same command line by adding additional *\monitor name\server name* entries in step 5, above. For example:

c:\Exchsrvr\Bin\admin.exe /mBerlin\server1 /mBerlinLink1\server1 /mParisLink2\server1 /mBerlinLink3\server1

6. Choose **Next**, and then double-click the StartUp folder.
7. Type the name that you want to see on the **StartUp** menu, and then choose **Finish**.
8. In the **Taskbar Properties** window, click **OK**.

Option	Description
Path	Full path to the Bin directory where the Administrator program is installed.
Site name	The name of the site where the monitor is defined, not where it runs. This parameter is optional.
Monitor name	The directory name of the monitor to be started.
Server name	The name of the server you want to read the monitor and perform all other operations requiring a home server, for example, sending mail.

Starting Performance Monitor Automatically

Performance Monitor can also be added to the StartUp folder, but the command-line argument is limited to one file. This is an alert file (.pma) that has been created, configured, and saved earlier.

1. From the **Start** menu, choose **Settings**.
2. Choose **Taskbar**, and then select the **Start Menu Items** tab.
3. Choose **Add**, and then choose **Browse**.
4. Locate the Windows NT Server Performance Monitor program (Perfmon.exe), and then double-click the program icon. This program is usually located in the Winnt\System32 subdirectory.
5. In the **Command Line** box, add the path and file name for the Performance Monitor alert file. Use the following format:

perfmon.exe *path\filename*

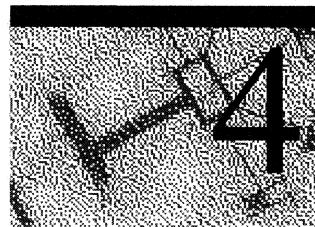
where *path\filename* is the path and file name of a Performance Monitor alert file.

6. Choose **Next**, and then double-click the StartUp folder.
7. Type the name that you want to see on the **StartUp** menu, and then click **Finish**.
8. In the **Taskbar Properties** window, choose **OK**.

For more information on creating and configuring alert files, see “Adding Selections to an Alert Log” earlier in this chapter.

CHAPTER 4

Troubleshooting Tools and Resources



Built-in tools and resources make troubleshooting Microsoft Exchange Server problems easier. Many of the tools can be used remotely to diagnose and fix problems throughout your organization.

This chapter describes the tools available for resolving problems. It includes Microsoft Exchange Server tools and Windows NT tools as well as those from other sources that are available to Microsoft Exchange Server. It is recommended that you read this chapter and familiarize yourself with the tools before a problem occurs.

Solving problems involves more than one source. Typically, you will consult:

- Link monitor display and log
- Server monitor display and log
- Message tracking log
- Diagnostic logs for connectors and services
- Your network topology or routing map
- Message queues
- Windows NT application event log

Link Monitor

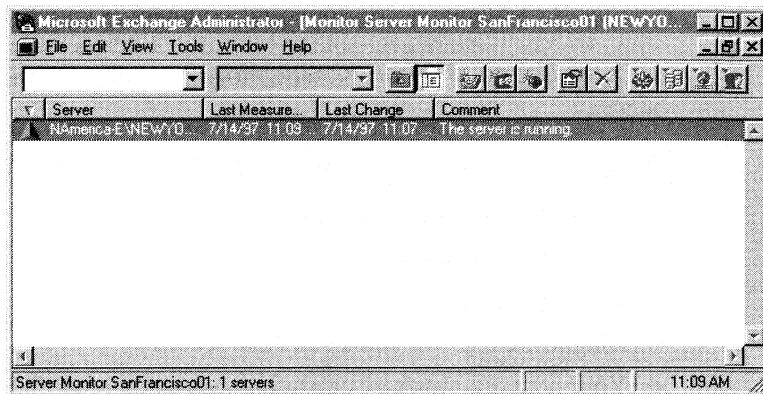
Link monitors are used to verify that test messages sent to other servers in the same or different site or to foreign systems are making the round-trip within a specified length of time. For more information on link monitors, see Chapter 3, “Monitoring Your Organization.”

Connection Status

When you are alerted to a connection problem, check the link monitor display to determine the scope of the problem and the components affected. To view the display for a link monitor, choose an existing configuration and start the monitor. Link monitor configurations are stored in the directory and are available to servers throughout the site.

Getting to the link monitor display

1. In the Administrator window, choose **Monitors**, and then choose a link monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name or browse to the server you want to connect to, and then choose **OK**.
4. Double-click the appropriate link.



Interpreting a Link Monitor Display

The link monitor displays the condition of monitored connections. Each line in the display represents one connection. You can sort the entries using the column heading buttons. You can also change the width of the columns to make the display easier to read.

Associate the condition of the connections to your network map. This can reveal the scope of the problem and point to the source. The comments and severity symbols depend on the thresholds set in the link monitor **Bounce** property page. If the alert tolerance is set too low, ping messages on fully operational connections will go into warning or alert states.

Option	Description
Symbol	The status of the connection. The status can be up, down, in a warning state, or not yet monitored.
Server	The server the ping message was sent to and the server it is expected to be returned from.
Last Measurement	The time the last ping message was sent from the sending server. It is displayed in local time.
Last Change	The time that the status of the connection changed. It is displayed in local time.
Last Time	The round-trip time of the last returned ping message on the connection.
Comment	The condition of the connection between the sending and destination server as measured by the round-trip time of a ping message sent between them.

Text in the **Comment** column describes the status of the connection based on the thresholds set in the **Bounce** property page. The following comments can appear in this column.

The link is operational.

The ping message was returned in less than or equal to the time specified in the bounce threshold.

Bounced mail took (*time*).

The last ping message was returned, but the bounce time exceeded the warning threshold in the link monitor **Bounce** property page. The value shows the actual elapsed time.

A message was due on (*time*).

The last ping message sent has not yet returned, and the elapsed time has already exceeded the warning threshold.

Not monitored yet.

No ping messages have been returned, and those that were sent are not yet late.

Link Monitor Logs

A link monitor log is a written record of recent connection problems. It includes all information that the link monitor displays such as time stamps, alerts, warnings, notifications, and dates and times when connections started, slowed, or stopped. The short history available in the log can be a useful addition to the data you are gathering about connection problems. You can view the information in the log file by using any text editor or word processing application.

There is one log for each link monitor, even if the link monitor sends ping messages to more than one server. It is available even if the link monitor is not operating.

You can set the log file name and path in the link monitor **General** property page when the link monitor is configured. The log file name can be read from any computer running the Administrator program that is logged on to a server in the site, even remotely.

The following is an example of a section from a link monitor log file.

```
9/15/97 6:47 PM SYDNEY Running The link is operational
9/15/97 6:57 PM MELBOURNE Warning A message was due on 9/15/97 6:56 PM.
9/15/97 6:57 PM Mail Message to /o=Ferguson/ou=Australia/cn=Recipients/cn=*AUOT01:
'MELBOURNE Warning since 9/15/97 6:57 PM A message was due on 9/15/97 6:56 PM.' -> Send
status: No error.
9/15/97 7:01 PM MELBOURNE Alert A message was due on 9/15/97 7:01 PM.
9/15/97 7:01 PM Launch a Process to C:\\PAGER.EXE SHORT.TXT:MELBOURNE Alert since 9/15/97
7:01 PM A message was due on 9/15/97 7:01 PM.' -> Send status: No error.
```

Connection Problems

When troubleshooting connection problems, it is important to determine the number of connections that are in error.

- If multiple connections are down, check your network topology map for common features of the problem connections, such as a certain server, router, bridge, gateway, or leased line.
- If just one connection is down, concentrate on why the ping message failed to complete the round-trip in time.

Examine the bounce detail of the ping message in the connection's **General** property page. A long delay between one hop and the next or a long delay at the last hop indicates a bottleneck or failing connection. Refer to your message routing map for components in the path that could be down.

Use other troubleshooting tools to supplement the data from the link monitor. This is essential until at least one ping message on a connection is returned.

- All ping messages should return eventually, unless they are deleted along the route. If a ping message does not return, check the queues in the message transfer agent (MTA) and information stores of the sending and receiving servers. If message tracking is enabled, the message tracking log also provides a trace of the ping message.

- Send a test message and search for it in the queues of servers and gateways along its route. Most problems that cause an alert in the link monitor also generate a large backlog of messages. This task can be made more difficult if there are multiple routes the message could follow. Use your message routing map to narrow the scope of your search.
- Check the queue size on servers in your site. Create a Windows NT Performance Monitor chart file that tracks the queue size on each server and look for one or more servers with large queues.
- Use Windows NT Event Viewer to search application event logs on the link monitor's home server and destination server. To make the search more efficient, filter the display to show only those events between the last successful message and the first link monitor warning. Look for warnings and alerts from the MTA, information store, and directory.
- Start or check a server monitor that is running to see if any servers in the route of the ping message are down, or use Windows NT Server Manager to see if the services are running.
- Use Performance Monitor to check connectors and gateways to see that they are processing mail. Check the messages/sec or messages/hour counters.

Troubleshooting Your Link Monitor

Your link monitor must be configured correctly to be a useful source of information about network connectivity.

- Configuring and starting a link monitor are separate processes. When you create a link monitor, you specify the characteristics and properties of the link monitor. The link monitor is not operational until it is started. Monitors can be started manually from the **Tools** menu in the Administrator window. Usually, they are started from the command line, from a batch file, or a program item in the Startup group on a dedicated server.
- Link monitors function only when they are started and open. If you close the link monitor window, you stop the monitor. It no longer sends or times ping messages or writes to the log.
- The configuration specifies the destination servers to which ping messages are sent; it does not specify which server is the source of the ping message. The source is determined by your entry in the **Connect to Server** box when you start the link monitor. The same link monitor configuration will be monitoring different connections if started with different source servers.
- Link monitors assign a status of warning and alerts based solely on the thresholds you establish on the link monitor's **Bounce** property page. If the threshold is not appropriate for every link monitored, the status is not accurate. If one of the routes requires a longer or shorter threshold, create a separate link monitor.

- Ping messages sent to servers in foreign systems should be received by an application that replies to it. If the ping message is sent to a nonexistent address, a non-delivery report (NDR) is interpreted as a sign that the link is operational. However, when NDRs are returned from foreign systems, it is not clear which host actually generated the NDR and which connection has been tested. Send a message along the route of the ping message and examine the NDR to determine the replying host.
- If the system clock is changed by more than a few minutes, restart the monitors. Otherwise, pending messages appear to be late, or connections appear to be down until the previous time is reached.

Server Monitor

Server monitors determine whether Microsoft Exchange Server components are running. They test all core and optional server components, including installed connectors. Once a server monitor alerts you to a problem, you can then use information from the monitor to research the cause and restart the service.

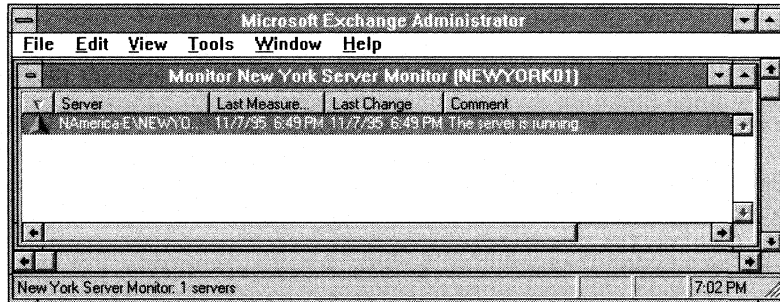
For more information about server monitors, see Chapter 3, “Monitoring Your Organization.”

Server Status

When you are alerted to a component failure, check the server monitor display to determine the scope of the problem and the components affected. Use the property pages for the server monitor to learn about its configuration before attempting to interpret the display. To view the display for a server monitor, choose an existing configuration and start the monitor. Remember that the server monitor’s configuration includes only the monitored servers. The originating server is the one you specify when you start the server monitor.

Getting to the server monitor display

1. In the Administrator window, choose **Monitors**, and then choose a server monitor.
2. From the **Tools** menu, choose **Start Monitor**.
3. Type the name or browse to the server you want to connect to, and then choose **OK**.
4. Double-click the appropriate server.



Interpreting a Server Monitor Display

The server monitor displays the status of monitored servers. Each line in the display represents one server. You can sort the entries using the column heading buttons. You can also change the width of the columns to make the display easier to read.

Option	Description
Symbol	The condition of all server components. If any component is down, the server is considered to be down.
Server	The server being monitored.
Last measure	The last time the server was polled. It is displayed in local time.
Last change	The time the condition of any component of the server changed. It is displayed in local time.
Comment	The condition of the server.

Server Monitor Logs

The server monitor log file is a record of recent server monitoring events. The short history available in the log can be a useful addition to the data you are gathering about server problems. You can view the information in the log file by using any text editor or word processing application.

You can set the log file name and path in the server monitor **General** property page when the server monitor is configured. The log file name can be read from any computer running the Administrator program that is logged on to a server in the site, even remotely.

The following is an example of a section of a server monitor log file.

```
9/15/97  5:49 PM SYDNEY Alert The service MExchangeMSMI is unavailable, its status is
Stopped.
9/15/97  5:49 PM Mail Message to /o=Ferguson/ou=Australia/cn=Recipients/cn=Alig: 'SYDNEY
Alert since 9/15/97  5:49 PM The service MExchangeMSMI is unavailable, it's status is
Stopped.' -> Send status: No error.
9/15/97  5:49 PM Launch a Process to c:\pager\page.exe server.txt: 'SYDNEY Alert since
9/15/97  5:49 PM The service MExchangeMSMI is unavailable, it's status is Stopped.' ->
Send status: No error.
9/15/97  5:49 PM MELBOURNE Repair Set the clock of the remote computer: No error.
9/15/97  5:49 PM MELBOURNE Alert Many services (2) are unavailable.
9/15/97  5:49 PM Mail Message to /o=Ferguson/ou=Australia/cn=Recipients/cn=Alig: 'MELBOURNE
Alert since 9/15/97  5:49 PM Many services (2) are unavailable.' -> Send status: No error.
9/15/97  5:54 PM SYDNEY Running The server is running.
9/15/97  6:00 PM MELBOURNE Running The server is running.
9/15/97  6:00 PM Mail Message to /o=Ferguson/ou=Australia/cn=Recipients/cn=Alig: 'MELBOURNE
Running since 9/15/97  6:00 PM The server is running.' -> Send status: No error.
```

Windows NT Performance Monitor

Performance Monitor is a Windows NT tool that can be used with Microsoft Exchange Server to measure server performance. For more information on Performance Monitor, see Chapter 3, “Monitoring Your Organization,” or your Windows NT Server documentation.

Windows NT Event Viewer

Windows NT logs events to application logging files that enable you to track significant events such as a server with a full disk or an interrupted power supply. You can use Windows NT Event Viewer to display, search, and maintain the application event logs for Microsoft Exchange Server computers and set alerts that notify you when there are problems. Because events differ considerably in their significance, you can set the level of detail of logged events by configuring the **Diagnostics Logging** property page on Microsoft Exchange Server components.

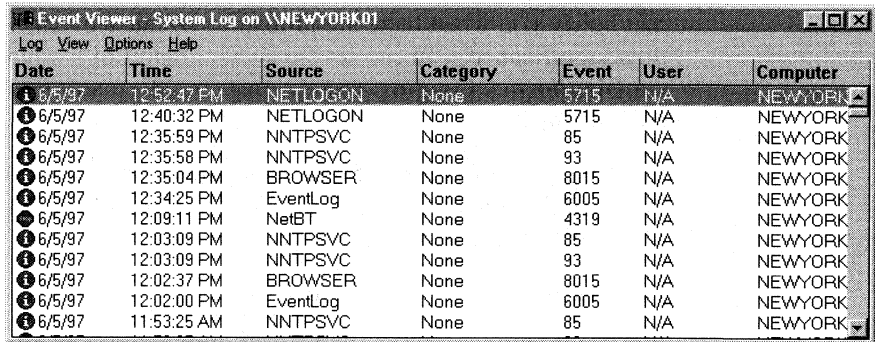
Each Microsoft Exchange Server component generates different kinds of events based on the functions it performs. The following table shows a few examples of Microsoft Exchange Server events.

Component	Events
All components	Start, failure to start, stop.
System attendant	Problems in routing table calculation, generating e-mail addresses, errors writing to the tracking log.
MTA	Opening and closing connections to other servers, transport problems, failed connections, and connection errors.
Directory	Replication request, success and failure messages, garbage collection, and changes in the security attributes.
Public information store	User logon and replication.
Private information store	User logon, sending, and receiving.
Administrator program	Replication configuration.
Directory import	Import start and finish, errors in importing, and warnings on possible problems.
Directory synchronization	Synchronization errors.
Security events	Logon, logoff, and privileged use.
Internet Mail Service	Mail connectivity, Internet services, and scheduled connection times.

For more information on Windows NT Event Viewer, see your Windows NT Server documentation.

Getting to Event Viewer

1. From the **Start** menu, choose **Administrative Tools**, and then select **Event Viewer**.
2. From the **Log** menu, choose **Application**.



Date	Time	Source	Category	Event	User	Computer
6/5/97	12:52:47 PM	NETLOGON	None	5715	N/A	NEWYORK
6/5/97	12:40:32 PM	NETLOGON	None	5715	N/A	NEWYORK
6/5/97	12:35:59 PM	NNTPSVC	None	85	N/A	NEWYORK
6/5/97	12:35:58 PM	NNTPSVC	None	93	N/A	NEWYORK
6/5/97	12:35:04 PM	BROWSER	None	8015	N/A	NEWYORK
6/5/97	12:34:25 PM	EventLog	None	6005	N/A	NEWYORK
6/5/97	12:09:11 PM	NetBT	None	4319	N/A	NEWYORK
6/5/97	12:03:09 PM	NNTPSVC	None	85	N/A	NEWYORK
6/5/97	12:03:09 PM	NNTPSVC	None	93	N/A	NEWYORK
6/5/97	12:02:37 PM	BROWSER	None	8015	N/A	NEWYORK
6/5/97	12:02:00 PM	EventLog	None	6005	N/A	NEWYORK
6/5/97	11:53:25 AM	NNTPSVC	None	85	N/A	NEWYORK

Searching Event Logs

Search the application event log to find specific events by event ID or those generated by a server component, service, or connector. You can also find events generated when a specific user was logged on or events generated by a certain computer.

Microsoft Exchange Server components are listed in Windows NT Event Viewer in the **Source** column by their application name. This name also appears in the **Service** box in the **Diagnostics Logging** property page for each component. For a complete list of the components and associated categories, see Appendix A, "Diagnostics Logging."

Diagnostics Logging

Diagnostics logging levels determine which Microsoft Exchange Server events are written to the Windows NT event log. An *event* is any significant occurrence in a system or application. You can configure diagnostic logging for Microsoft Exchange Server components to record only highly significant events, such as an application failure, or moderately important events, such as receipt of messages across a gateway, or events relevant only to debugging. Normally, you want to log only critical events.

Note Diagnostics logging affects events only. It does not affect error messages, error alerts, message tracking, or utility logs.

Diagnostics logging is available on the following Microsoft Exchange Server components:

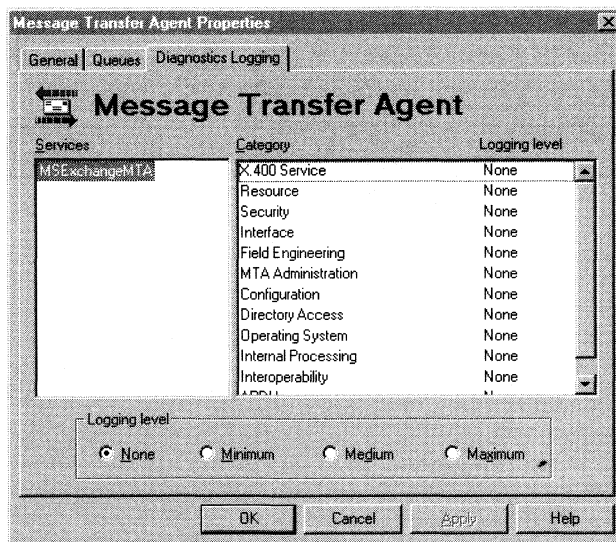
- MTA
- Directory
- Information store
- Internet Mail Service
- Microsoft Mail Connector
- Microsoft Schedule+ Free/Busy Connector
- Microsoft Exchange Connector for Lotus cc:Mail

Microsoft Exchange Server Components

The logging levels for Microsoft Exchange Server components are set in the **Diagnostics Logging** property page of each component. You can configure diagnostics logging for Microsoft Exchange Server components, such as the directory and MTA.

Getting to the components Diagnostics Logging property pages

1. In the Administrator window, select a server, and then select a component.
2. From the **File** menu, choose **Properties**.
3. Select the **Diagnostics Logging** tab.

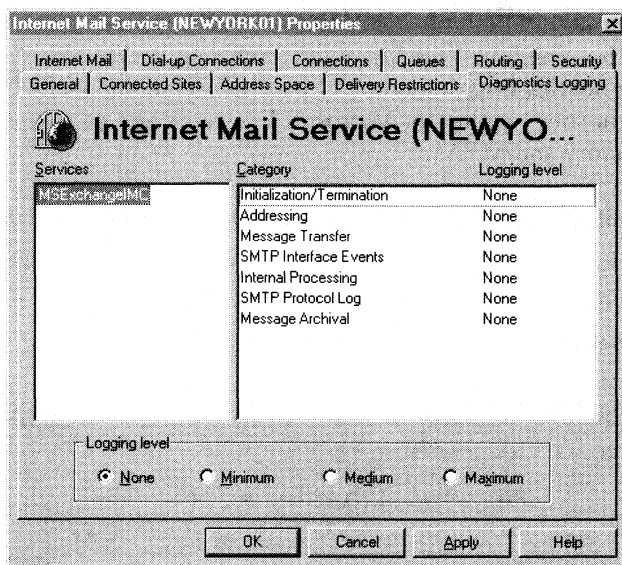


Microsoft Exchange Server Connectors

Each Microsoft Exchange Server connector is installed on a single server but can service a large site. A site with multiple servers can include more than one Internet Mail Service or Microsoft Mail Connector. Diagnostics logging is set independently on each connector. When tracking a connector problem in your site, you may need to increase the logging level on more than one connector.

Getting to the connectors Diagnostics Logging property pages

1. In the Administrator window, choose **Connections**.
2. Double-click a connector.
3. Select the **Diagnostics Logging** tab.



Diagnostics Logging Categories

Diagnostics logging levels are set by *category*. A category is a group of related functions. Each category of Microsoft Exchange Server service has a diagnostics logging level. When a service generates an event with a significance number less than or equal to the logging level, the event is recorded in the event log. If the significance number of the event is greater than the logging level, it is ignored.

Events can be logged from every category of every service on every server. However, during routine operation, to limit the amount of information that accumulates, you should set diagnostics logging to **None** for every category of every service on every server. At this level, only error events and critical error messages are written to the log. The logging level set for a component of a server applies only to that component. It does not affect levels set for other components of the same server or like components on other servers.

You can start diagnostics logging if you need to troubleshoot a problem. When you increase a logging level, be selective. Increase levels on only those aspects of the service that might be related to the problem. Setting a level too high can produce a log filled with events that are irrelevant to your investigation.

Understanding the Diagnostics Logging Property Page

The **Diagnostics Logging** property pages are similar for all components and connectors, except for the Microsoft Schedule+ Free/Busy Connector, which is described separately. This property page shows the application name of the service, a list of diagnostic categories, and the current logging level for each category.

The columns correspond roughly to the structure of Event Viewer. The application name in the **Service** column in the **Diagnostics Logging** property page appears in the **Source** box of the application event log. Also, the categories appear in the **Category** box of the application event log.

Option	Description
Services	The service name.
Category	A group of related application functions. Logging levels are set by category.
Logging level	The current logging level for the category.

Changing the Diagnostics Logging Level

The logging level determines which events are written to the Windows NT application event log. When Microsoft Exchange Server generates an event less than or equal to the logging level, the event is logged.

- 1. Select the **Diagnostics Logging** tab.
- 2. Select a category.
- 3. Choose a logging level.

Option	Description
None	Logs only critical events and error events. This is the default and should be changed only if a problem occurs.
Minimum	Logs high-level events in the event log. These might include one message for each major task performed by the service. Use this setting to begin an investigation when the location of the problem is unknown.
Medium	Messages are sent to the event log to record steps taken to run a task. This provides more information than the minimum level but not the detail of the maximum level. Use this when the problem has been narrowed to a service or group of categories.
Maximum	Provides a complete trail of the operation of the service; messages can be sent for each line of code in the service. Use this level when the problem has been traced to a particular category or a small set of categories. This level logs all events. This can log a large amount of information, which can affect server performance.

MTA

You can increase the level of detail of events written to the application event log by the MTA. In addition, Interoperability and Application Protocol Data Unit (APDU) text logs are triggered by the levels set with diagnostics logging. You can generate these text logs by increasing logging levels.

Use the MTA **Diagnostics Logging** property page to set or change logging levels and create Interoperability and APDU logs. The MTA on each server has its own **Diagnostics Logging** property page, so make sure you select the right one.

Getting to the MTA Diagnostics Logging property page

- 1. In the Administrator window, select a server.
- 2. Double-click **Message Transfer Agent**.
- 3. Select the **Diagnostics Logging** tab.

Changing MTA Diagnostics Logging Levels

Use the **Diagnostics Logging** property page to change the logging levels of MTA categories. The application name for the MTA, MExchangeMTA, is listed in the Services column. All events are logged under this name in the Windows NT application event log. The categories listed in the MTA **Diagnostics Logging** property page match the categories of events shown in the application event log.

For more information, see “Changing the Diagnostics Logging Level” earlier in this chapter.

Creating Interoperability Logs

Use the diagnostics logging levels in the Interface and Interoperability categories to create Interoperability logs. These text logs consist of the binary contents of X.400 protocol messages transported by the MTA.

Interoperability logs are text files stored in the Mtdatad directory. The current log is always named Ap0.log. Old logs are named Apx.log with the *x* increasing with the age of the log.

Interoperability logs are created when the logging levels in both the Interface and Interoperability categories are set to **Medium** or **Maximum**.

- The binary content of X.400 protocol messages passed between MTAs on different servers and between MTAs and client applications are written to the Interoperability log. This is also the result if one category is set to **Medium** and the other is set to **Maximum**.
- The binary content of X.400 protocol events between MTAs and gateways are logged in addition to the communication among MTAs and between MTAs and their clients.

Diagnostic logging levels for the Interface category also determine the detail of Interface events sent to the event log. Event logging is not affected by the logging level of the Interoperability category. It determines only whether Interoperability text logs are created.

Interoperability logs can be instrumental in tracking down configuration problems on MTAs. However, they are valuable only to those familiar with ASCII translations of X.400 protocol. These logs can grow large very quickly and affect server performance.

1. Select the **Diagnostics Logging** tab.
2. Select the **Interoperability** category.
3. Select **Medium** or **Maximum**.
4. Select the **Interface** category.
5. Select **Medium** or **Maximum**.

Creating APDU Logs

Use the diagnostics logging levels of the X.400 service and APDU categories to trigger the creation of APDU logs. APDU logs are binary representations of communication among MTAs in different sites and between MTA and client applications within a site. They include the fully encoded Asn.1 envelope.

These text logs are stored in the Mtaadmin\ directory. The current log is always named Bf0.log. Old logs are named Bfx.log with the *x* increasing with the age of the log.

APDU logs are enabled when the logging levels of the X.400 service and APDU categories are both set to **Medium** or **Maximum**. There is no difference between **Medium** and **Maximum** for the APDU category. However, in addition to its influence on APDU logs, the diagnostics logging level of the X.400 service category determines which X.400 events are written to the Windows NT application event log.

Once enabled, APDU logs are written when any of the following events occurs.

Event #	Description	Logging Level
200	Bad APDU transferred in from another MTA	Minimum
220	Bad APDU submitted to this MTA	Minimum
269	APDU delivery failed temporarily	Minimum
270	APDU delivery failed permanently	Minimum
271	APDU sent	Medium
271	APDU received	Medium

If the logging levels of both the X.400 service and APDU are set to **Minimum** or **Maximum**, the first four events will be written to the event log. If the logging levels of both categories are set to **Medium** or **Maximum**, all six events will be logged and the APDU text logs will be written.

APDU logs can be instrumental in diagnosing problems with the MTA. However, they are valuable only to those familiar with ASCII translations of X.400 protocol. These logs can grow large very quickly and affect server performance.

1. Select the **Diagnostics Logging** tab.
2. Select the **APDU** category.
3. Select **Medium** or **Maximum**.
4. Select the **X.400 Service** category.
5. Select **Medium** or **Maximum**.

Information Store Events

Events generated by the information store relate to the operation of the public and private information store databases and the system functions common to them. These events include establishing and maintaining connections, sending and receiving messages, applying rules set by users, and replicating public folders.

Information store events are categorized first by the subcomponent that generated the event. The subcomponents are divided into category groups. The category groups are then divided into categories of events. The application name of the subcomponent is listed as the source of the event in the application event log.

Subcomponent	Description	Category group	Application name
System	Functions common to both databases	General	MSExchangeIS
Public	Public information store	Replication Transport General	MSExchangeISPub
Private	Private information store	Transport General	MSExchangeISPriv

You can set diagnostics logging levels for any subcomponent of the information store in either the public information store or private information store

Diagnostics Logging property page. The logging level applies only to the information store on that server. Effective troubleshooting can involve increasing the logging level on more than one server and on the MTA of the servers.

Diagnostics logging levels for the information store are set by category, just like other services. However, the categories are used only to group events. They are not written to the event log. Instead, event log entries include the subcomponents and category groups.

Critical events generated by the information store are written to the event log regardless of the logging level set for any category. These events fall into categories that do not appear in the **Diagnostics Logging** property page. However, they do appear as categories in Event Viewer.

The critical event categories are:

- Performance
- Recovery
- DS/IS Consistency
- None

Getting to the information store Diagnostics Logging property page

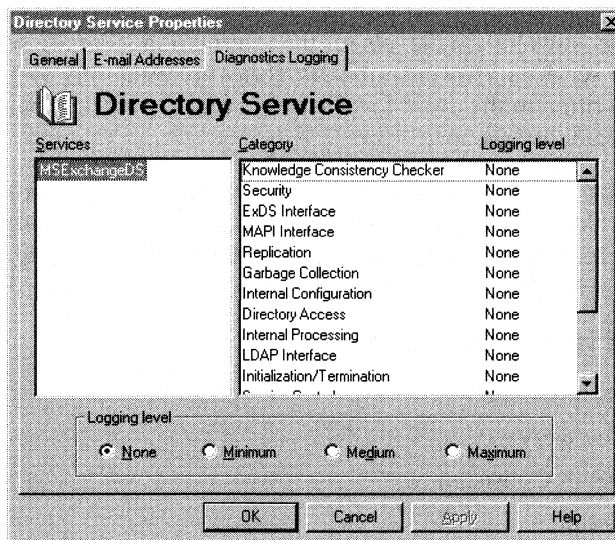
1. In the Administrator window, select a server, and then select **Private Information Store** or **Public Information Store**.
2. From the **File** menu, choose **Properties**.
3. Select the **Diagnostics Logging** tab.

Changing Information Store Logging Levels

The **Diagnostics Logging** property page for the public and private information store components are identical. They display the subcomponents of the information store as a hierarchy. The hierarchy expands to show the category groups for each subcomponent. When you select a category group, the categories for that group are displayed. Logging levels are set by category, but the category group, not the category, is logged with the event.

For more information on logging levels, see “Changing the Diagnostics Logging Level” earlier in this chapter.

1. Select the **Diagnostics Logging** tab.
2. Double-click a subcomponent.
3. Select a category group.
4. Select a category.
5. Select a logging level.



Using Diagnostics Logging of the Information Store

Diagnostics logging categories for the information store are very specific. It may be sufficient to increase the level on just one category to get the information you need. For example, if a problem occurs with public folder replication, use diagnostics logging to track it down. You can perform one or both of the following tasks.

- Increase the logging level of the Replication State Update category to **Minimum**. Events are logged when replication configurations are added or deleted.
- Increase the logging level of Incoming Messages and Outgoing Messages to **Maximum**. This logs all replication messages sent to or received by public folders.

Combine the information from the application event log with a search of the message tracking log and the logs from link monitors and the MTA. These tools help you narrow your search and diagnose information store problems.

Internet Mail Service

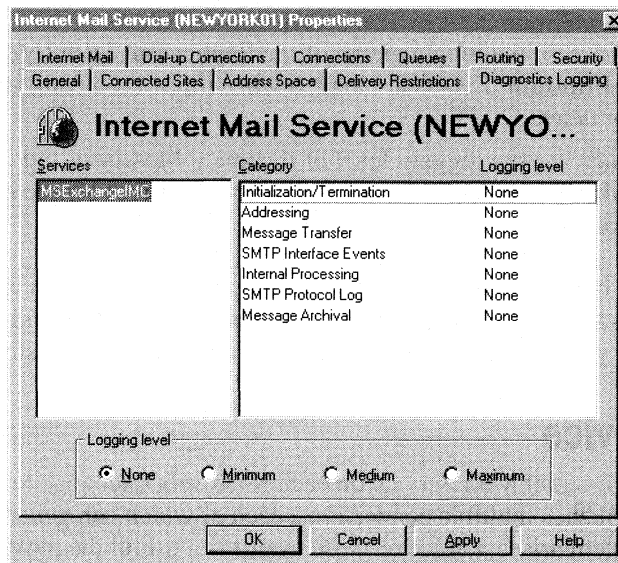
The Internet Mail Service on each Microsoft Exchange Server computer establishes multiple connections, each of which can generate events. When a problem arises, a trace of those events is a useful diagnostic tool. Use the **Diagnostics Logging** property page for the Internet Mail Service to set or change logging levels, log SMTP information, and create message archives.

SMTP protocol logs and message archives are triggered by the levels set in diagnostics logging. You generate these files by increasing the logging levels of the SMTP Protocol Log and Message Archival categories.

Important When you change a logging level, the **Logging Level** box displays the new level. However, events are logged at the previous level until the Internet Mail Service is restarted. Once you restart the Internet Mail Service, the change is effective immediately.

Getting to the Internet Mail Service Diagnostics Logging property page

1. In the Administrator window, choose **Connections**.
2. Double-click an Internet Mail Service.
3. Select the **Diagnostics Logging** tab.



Changing Internet Mail Service Logging Levels

The application name for the Internet Mail Service, MSExchangeIMC, is listed in the **Services** column. All events are logged under this name in the application event log. The categories listed in the Internet Mail Service **Diagnostics Logging** property page match the categories of events shown in the application event log.

Important You must restart the Internet Mail Service after changing logging levels. New logging levels do not take effect until the connector is restarted.

For more information, see “Changing the Diagnostics Logging Levels” earlier in this chapter.

1. Select the **Diagnostics Logging** tab.
2. Select one or more categories.
3. Select a logging level.
4. Restart the Internet Mail Service.

For more information, see “Changing the Diagnostics Logging Level” earlier in this chapter.

Logging SMTP Information

SMTP events are generated by Internet Mail Service connections. When you increase the diagnostics logging level for the SMTP Protocol Log category, Microsoft Exchange Server writes these events to text files. Each concurrent connection logs its events to a separate file. You can find these files in `Exchsrvr\Imcdata\Log`.

Tip A quick way to tell if SMTP logging is enabled is to check the application event log when the Internet Mail Service is started. If enabled, event 2004 is written to the event log. To locate this event in Event Viewer, search the application event log for the ID or the source, `MSExchangeIMC`, and the category, `SMTP Protocol Log`, of the event.

The headers and body of outgoing messages cannot be logged. However, the entire text of incoming messages is included.

1. Select the **Diagnostics Logging** tab.
2. Select **SMTP Protocol Log**.
3. Select a logging level.
4. Restart the Internet Mail Service.

Option	Description
None	No text logs are created. This is the default.
Minimum	Connection information is written to the SMTP log.
Medium	SMTP commands and headers are written to the SMTP log.
Maximum	Complete, unformatted protocol packets are written to the SMTP log. This can log a large amount of information, which can affect server performance.

Interpreting an SMTP Protocol Log

When the diagnostics logging level of the SMTP protocol log category is **Maximum**, the complete incoming message transfer is written to the log. This can include several input/output (I/O) lines per command, each representing one packet. Normal transmission messages are preceded by a 2xx or 3xx message code. Level 4xx codes are temporary problems that can be resolved by resending the message. Level 5xx codes are permanent negative responses requiring some repair before another attempt to send. Level 4xx and 5xx codes are accompanied by text describing the problem.

For more information, see Request for Comments (RFC) 821.

Creating a Message Archive

To solve some Internet mail problems, you may need to examine the entire text of an SMTP message. When you set the diagnostics logging level of the Message Archival category to **Medium** or **Maximum**, each message sent or received by the Internet Mail Service is moved to the Archive directory. Inbound messages are in `Imcdata\In\Archive`; outbound messages in `Imcdata\Out\Archive`.

Tip To quickly determine if message archiving is enabled, check the event log when the Internet Mail Service is started. If enabled, event 2005 is written to the event log. To locate this in Event Viewer, search for the event ID or the source, `MSExchangeIMC`, and the category, `Message Archival`, of the event.

1. Select the **Diagnostics Logging** tab.
2. Select the **Message Archival** category.
3. Select a logging level.
4. Restart the Internet Mail Service.

Option	Description
None	No messages are archived. This is the default.
Minimum	No messages are archived (same as None).
Medium	A copy of each message processed by the Internet Mail Service is written to a text file (same as Maximum).
Maximum	A copy of each message processed by the Internet Mail Service is written to a text file (same as Medium). This can log a large amount of information, which can affect server performance.

Microsoft Mail Connector

Events are generated by three subcomponents of each Microsoft Mail Connector. Use the **Diagnostics Logging** property page to set logging levels for all subcomponents of a Microsoft Mail Connector.

- Microsoft Mail interchange (MSMI).
- Microsoft Mail (PC) message transfer agent (PCMTA).
- Microsoft Mail (AppleTalk) message transfer agent (ATMTA).

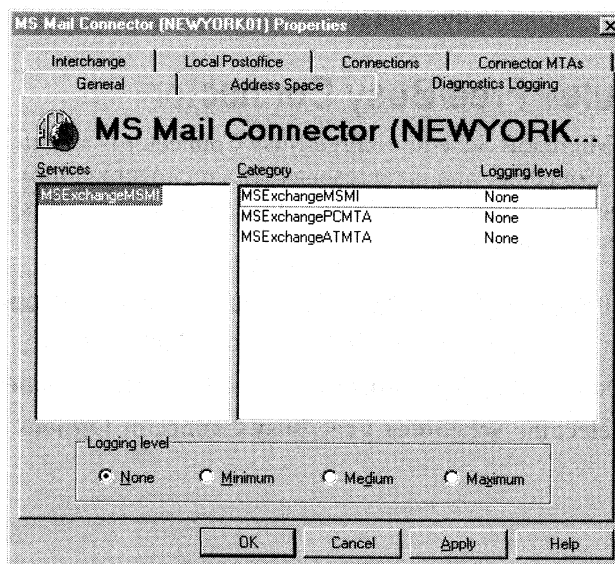
Diagnostics logging levels for the Microsoft Mail Connector are set by subcomponent, not by category. When events generated by a subcomponent are logged, the application name of the subcomponent appears as the source of the event. The event also includes the category of the subcomponent that generated the event, but these categories do not appear in the **Diagnostics Logging** property page for the Microsoft Mail Connector.

On some servers, multiple PCMTAs are created to improve performance. The logging level set for PCMTA applies to all PCMTAs on the server. When events are generated by one of the PCMTAs, the user-defined name of the PCMTA appears as the source of the event.

Diagnostics logging levels for each subcomponent are set independently. To completely investigate an MS Mail problem in Microsoft Exchange Server, increase the logging levels of more than one subcomponent and the Microsoft Exchange Server MTA.

Getting to the Microsoft Mail Connector Diagnostics Logging property page

1. In the Administrator window, select **Connections**.
2. Double-click a Microsoft Mail Connector.
3. Select the **Diagnostics Logging** tab.



Changing Microsoft Mail Connector Logging Levels

Increase the logging levels of Microsoft Mail categories to see more detailed events tracing mail through the gateway.

In the **Diagnostics Logging** property page for the Microsoft Mail Connector, the application name of the interchange, MExchangeMSMI, appears in the **Services** column. However, in the event log, the application name of the subcomponent appears in the **Source** column. The logging level set here for MExchangePCMTA applies to all PCMTAs on the server. MExchangeATMTA represents the MS Mail AppleTalk MTA.

1. Select the **Diagnostics Logging** tab.
2. Select one or more subcomponents.
3. Select a logging level.

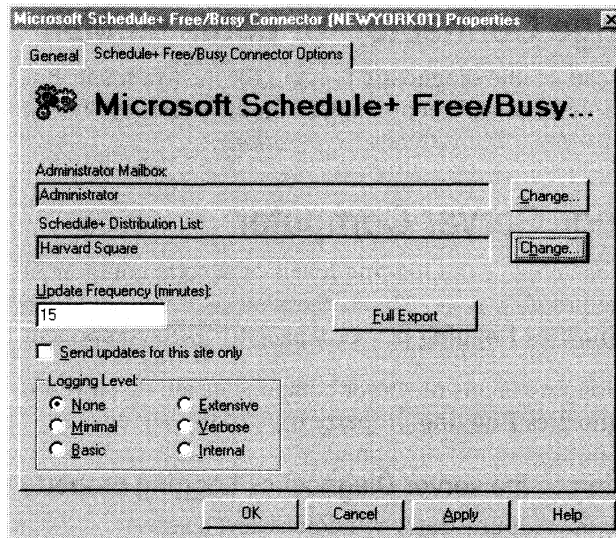
For a description of the logging levels, see “Changing the Diagnostics Logging Level” earlier in this chapter.

Microsoft Schedule+ Free/Busy Connector

The Microsoft Schedule+ Free/Busy Connector is an extension of the Microsoft Mail Connector and is represented as a recipient mailbox agent. Unlike other connectors, there is usually just one Schedule+ Free/Busy Connector per site, rather than one per server.

Getting to the Schedule+ Free/Busy Connector property page

1. In the Administrator window, choose **Recipients**.
2. Double-click **Microsoft Schedule+ Free/Busy Connector**.
3. Select the **Schedule+ Free/Busy Connector Options** tab.



Changing Schedule+ Free/Busy Connector Logging Levels

The Microsoft Schedule+ Free/Busy Connector has six logging levels. When you select a level, events at that level and all higher levels are written to the event log. There are no categories associated with this component.

The update frequency can be changed in the **Schedule+ Free/Busy Connector Options** property page.

1. Select the **Schedule+ Free/Busy Connector Options** tab.
2. In the **Logging Level** box, select a level.

Option	Description
None	Logs only critical events and error events, including initiations and terminations, NDRs, and shutdowns. This is the default.
Minimal	This level is the same as None .
Basic	Logs the number of messages received and number of information messages created.
Extensive	Logs the number of changes made and the names of users receiving messages from the Schedule+ Free/Busy Connector.
Verbose	This level is the same as Extensive .
Internal	Logs all events, including debug strings, configuration changes received, unknown address notifications, and validations of accounts.

Microsoft Exchange Connector for Lotus cc:Mail

You can enable diagnostic logging for the Microsoft Exchange Connector for Lotus cc:Mail and records events in the event log. For more information, see *Microsoft Exchange Server Operations*.

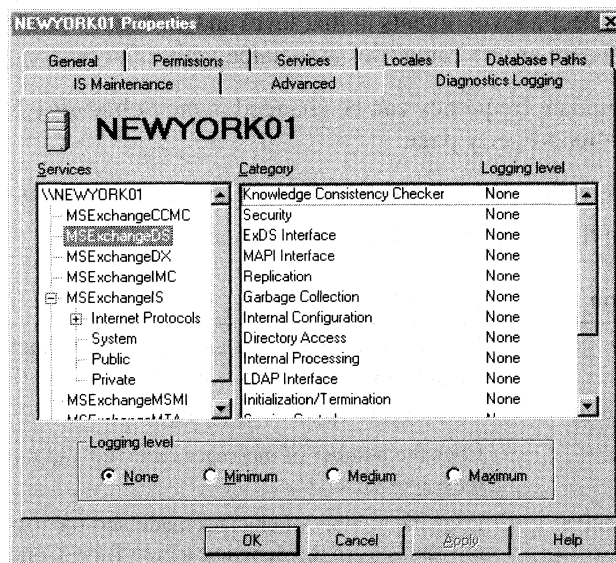
Microsoft Exchange Server Computer

You can change the logging levels of several components of a server from a single property page. This is the same as if you set levels by using the **Diagnostics Logging** property page for each component.

The logging levels of server components are displayed in a hierarchy in the **Diagnostics Logging** property page of the server

Getting to the server Diagnostics Logging property page

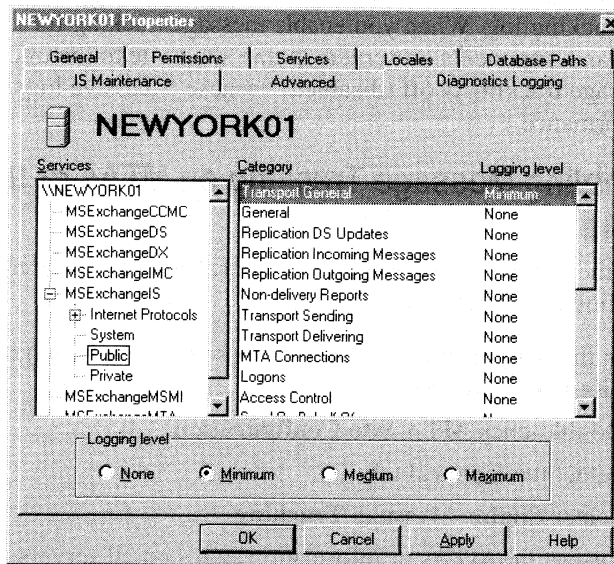
1. In the Administrator window, select a server.
2. From the **File** menu, choose **Properties**.
3. Select the **Diagnostics Logging** tab.



Changing Logging Levels

The information store is displayed as a hierarchy of its three subcomponents, just as it is in the public and private information store **Diagnostics Logging** property pages. To display the categories and logging levels, expand the hierarchy and select a category group.

1. Select the **Diagnostics Logging** tab.
2. Select a component.
3. Select a category.
4. Select a logging level.



Message Tracking

Messages sent to and from Microsoft Exchange Server can be tracked to determine the cause of mail-related problems. You can:

- Track messages to locate slow or stopped connections.
- Find lost mail.
- Determine the delay on each segment of a route for link monitoring and performance tuning.
- Track an unauthorized message and remove it from the system.

Message tracking can be enabled on the MTA, information store, and Microsoft Mail Connector. When message tracking is enabled, each component handling mail records its activities in a log maintained by the system attendant on each server. The log becomes a trace of the processing of each message as the component receives, processes, and delivers it to the next component.

After you enable message tracking, you must restart all components writing to the tracking log for message tracking to take effect. For example, if you enable message tracking on MTAs, you must restart all MTAs in the site.

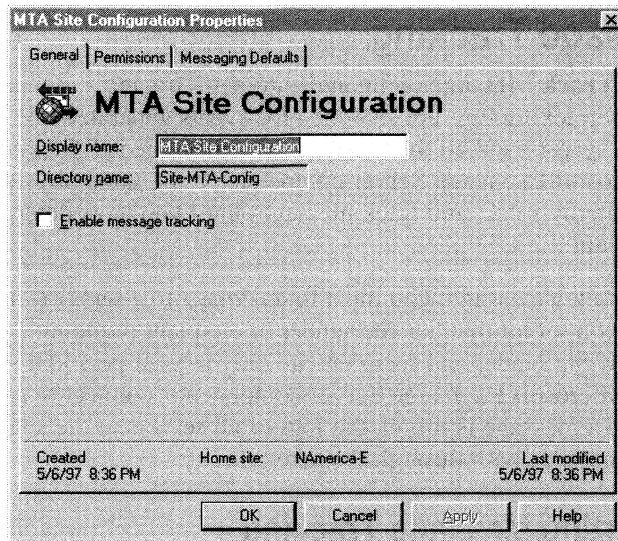
Enabling Message Tracking

Message tracking must be enabled for a component to begin recording activity in the tracking log. When you enable message tracking for any component, all similar components on servers in that site write to the tracking log. The default for message tracking is off (disabled) because excessive logging can affect server performance.

Enabling Message Tracking on MTAs or the Information Store

Use the MTA site configuration **General** property page to enable message tracking on all MTAs in the site.

1. In the Administrator window, choose **Configuration** or **Information Store Site Configuration**.
2. Double-click **MTA Site Configuration**.
3. Select the **General** tab.
4. Select **Enable Message Tracking**.
5. Restart the MTAs or information stores on all servers in the site.



Enabling Message Tracking on a Microsoft Mail Connector

Use the Microsoft Mail Connector **Interchange** property page to enable message tracking on the connector. You must enable message tracking separately on each Microsoft Mail Connector in the site.

1. In the Administrator window, choose **Connections**.
2. Double-click a Microsoft Mail Connector.
3. Select the **Interchange** tab.
4. Select **Enable Message Tracking**.
5. Restart the Microsoft Mail Connector.

Enabling Message Tracking on the Internet Mail Service

Use the Internet Mail Service **Internet Mail** property page to enable message tracking. Message tracking is enabled separately for each Internet Mail Service in a site. If your site has more than one Internet Mail Service, enable message tracking on each.

1. In the Administrator window, choose **Connections**.
2. Double-click an Internet Mail Service.
3. Select the **Internet Mail** tab.
4. Select **Enable Message Tracking**.
5. Restart the Internet Mail Service.

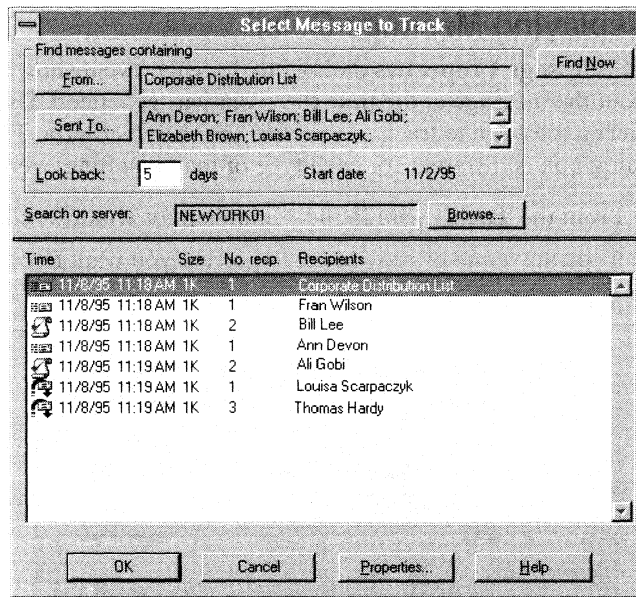
Performing Message Tracking

The **Track Message** command automates tracing a message through the network. Daily tracking logs are searched for events generated when the components of each server handled the message. The message is followed through the logs of all Microsoft Exchange Server computers on the same physical network. You can repeatedly select and track messages until you have determined the source of the problem.

To track a message, you must first connect to a server to locate the message. Select a server that has the sender or recipient of the message in its global address list. If the sender and recipient are only in your personal address book (PAB) or are Microsoft Exchange Server components, connect to any server in the site. Once a message is found, the logs of all servers in the site are searched to follow the message path through the network.

Starting Message Tracking

1. From the **Tools** menu in the Administrator window, choose **Track Message**.
2. Type the name or browse for the server you want to connect to.
3. Specify a message, and then choose **OK**.
4. Choose **From**, and then select the name of the sender.
5. Choose **Sent To** and select the name of a recipient in the global address list, and then choose **Add**. Repeat this for all recipients.
6. Specify the appropriate options.
7. Choose **Find Now**.

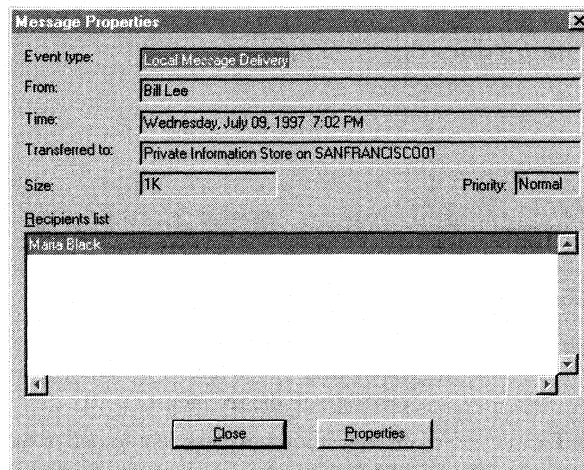


Option	Description
From	Searches for messages sent from this mailbox. Only one mailbox can appear in this box. If the box is blank, it searches for all messages to the recipients.
Sent To	Searches for messages sent to one or more mailboxes. More than one mailbox can be selected. Distribution lists can be recipients. If the box is blank, it searches for all messages from the sender.
Look back	Determines how many daily logs are searched. If 0, it searches the current day's log only. Daily logs begin and end at midnight Coordinated Universal Time (UTC), so you may have to look back one log to get today's log in local time.
Start date	The date of the first log to be searched. This is determined by the entry in the Look back box and cannot be edited.
Search on server	Searches the log of the server selected for the message to be tracked. The sender's home server is the default.
Time	The symbol represents the event type. Event types are described in "Tracking Log" later in this chapter. The time and date the message was sent as recorded by the information store on the sending server. It is displayed in local time.
Size	Message size in bytes.
No. recp.	The number of mailboxes to which the message was sent. A distribution list counts as one recipient.
Recipients	The first mailbox in the recipients list. An ellipsis follows the names in messages that have more than one recipient. Choose Properties to see the entire recipients list.

Displaying Message Detail

The **Message Properties** dialog box for each event shows detailed information about the message at the time the event was generated. Use this information to select a message to track or to refine the search criteria. The **Message Properties** dialog box is different for each type of mail handling event.

1. From the **Tools** menu in the Administrator window, choose **Track Message**.
2. Type the name or browse for the server you want to connect to.
3. Specify a message, and then choose **OK**.

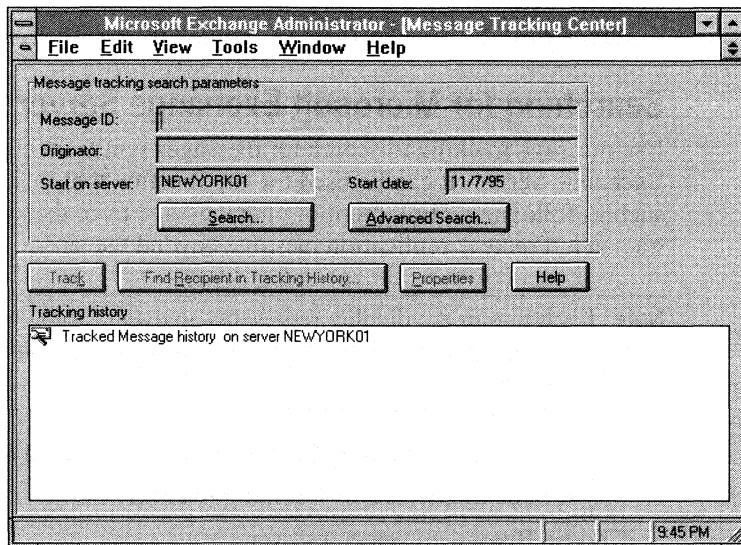


Option	Description
Event type	A description of the message tracking event.
From	The distinguished name of the originator.
Time	The time the mail message was sent or received is displayed in time local to the Administrator program.
Transferred to	The Microsoft Exchange Server component that generated this event.
Size	The message size, in bytes.
Priority	The importance level assigned to the message by the originator.
Recipients List	All addresses the message was sent to.

Using the Message Tracking Center

Once a message is found in a tracking log, its path through the network is traced through the logs of all servers that handled it. At each step, the process determines which service is expected to receive the message next and searches the logs on that server to find other events. The trace is complete when the message leaves the network or is delivered.

1. From the **Tools** menu in the Administrator window, choose **Track Message**.
2. Type the name or browse for the server you want to connect to, and then choose **OK**.
3. Specify a message, and then choose **OK**.



Option	Description
Message ID	The ID of the message selected for tracking. To change it, choose Advanced Search , which will track a different message.
Originator	The mailbox that sent the message. To search for messages from a different originator, choose Search .
Start on server	The message trace begins from the log of this server. An event was found in the server's tracking log indicating that the message was sent from or entered the network through this server.
Start date	The date the search begins. According to the tracking log, this is the date the selected message was sent or entered the network. Daily tracking logs begin and end at midnight UTC.

(continued)

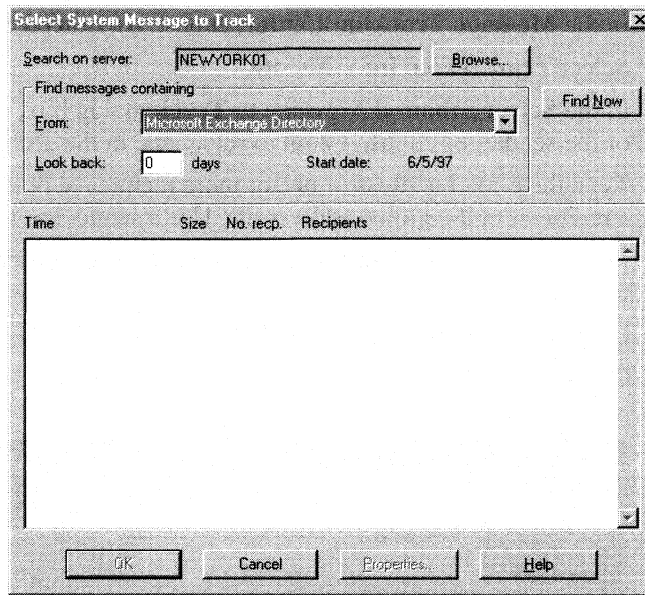
Option	Description
Search	Opens the Select Message to Track window so that you can search for a message.
Advanced Search	Opens the Advanced Search dialog box so you can search for a message by its ID, search for a message sent from outside the network, or search for a message from a Microsoft Exchange Server component.
Track	Activates message tracking for the selected message. When the search is complete, it displays the message tracking events found for the message in the Tracking History window.
Find Recipient in Tracking History	Finds events involving a recipient that you specify and displays them in bold.
Properties	Displays details of the event selected.

Searching for Microsoft Exchange Server Messages

Use message tracking to search for messages sent from components of Microsoft Exchange Server. It can be used for any function that involves sending messages, such as following a link monitor ping message from the system attendant or tracing a directory replication message beyond the site.

Note Each line in the display represents an event. Some messages appear in more than one event. It does not matter which you select because the message is tracked, not the event.

1. In the **Message Tracking Center**, choose **Advanced Search**.
2. Select **Sent by Microsoft Exchange Server**.
3. Choose **Browse** to select a server.
4. In the **From** box, select a Microsoft Exchange Server component.
5. Change the **Look back** date, if desired.
6. Choose **Find Now** to begin the search.



Option	Description
Search on server	Searches the log of the server selected for the message to be tracked. The server you are connected to is the default.
From	Searches for messages sent from this Microsoft Exchange Server core component. You must type a component name in this box.
Look back	Determines how many daily logs are searched. If 0, it searches the current day's log only. Daily logs begin and end at midnight UTC, so you may have to look back one log to get today's log in local time.
Start date	Displays the date of the first log to be searched. This is determined by the entry in the Look Back box and cannot be edited.

Searching Outside of an Organization

You can search for a message when either the sender or recipients are not in a global address list. You can type the names of recipients and search for messages originating at gateways.

Note Each line represents an entry event for a message. Some messages can appear in more than one event. It does not matter which you select because the message is tracked, not the event.

1. In the **Message Tracking Center**, choose **Advanced Search**.
2. Select **Transferred into this site**.
3. In the **Select Inbound Message to Track** dialog box, type the e-mail address of the sender, or choose **From** to select one in the global address list.
4. Type the e-mail address of one or more recipients, or choose **Sent To** to select a recipient in the global address list. Use a semicolon to separate addresses.
5. In the **Transferred from** box, select the connector used to transport the message.
6. Change the **Look back** date and server, if appropriate.
7. Choose **Find Now**.

Select Inbound Message to Track

Find messages containing

From...

Sent To...

Transferred from:

Look back: days Start date: 6/5/97

Search on server:

Time	Size	No. recp.	Recipients

Option	Description
From	<p>Searches for messages sent from this e-mail address. Only one address can appear in this box.</p> <p>Type the address in the appropriate format for the gateway, for example,</p> <p>SMTP:johnd@ferguson.com</p> <p>You can also select from the global address list if the sender is in it but the recipient is not.</p> <p>If the box is blank, it searches for all messages to the recipients.</p>
Sent To	<p>Searches for messages sent to one or more e-mail addresses, including distribution lists.</p> <p>Type the address in the appropriate format for the gateway. You can also select from the global address list if the recipient is in it but the sender is not.</p> <p>If the box is blank, it searches for all messages from the sender.</p>
Transferred from	<p>Lists all connectors in the site. Select from the list to search the log of the server where the connector is installed.</p>
Look back	<p>Determines how many daily logs are searched. If 0, it searches the current day's log only. Daily logs begin and end at midnight UTC, so you may have to look back one log to get today's log in local time.</p>
Start date	<p>Displays the date of the first log to be searched. This is determined by the entry in the Look back box and cannot be edited.</p>
Search on server	<p>Searches the log of the server selected for the message to be tracked. The home server of the connector is the default.</p>

Searching by Message ID

Use the **Advanced Search** button in the **Message Tracking Center** to find a message by its message ID.

Each message handled by Microsoft Exchange Server is assigned a message ID when it is created or enters the system from a gateway. Microsoft Exchange Server message IDs have a standard format, which includes the name of the originating server and the date and time the message was sent.

For example:

```
c=US;a=p=Ferguson;l=NEWYORK0196012020010800000CDE
```

1. In the **Message Tracking Center**, choose **Advanced Search**.
2. Select **By Message ID**.
3. Type the message ID.
4. Choose **Browse** to select a server whose tracking log will be searched.
5. Change the **Look back** information, if appropriate.

Option	Description
Message ID	Type the message ID.
Look back	Determines how many daily logs are searched. If 0, it searches the current day's log only. Daily logs begin and end at midnight UTC, so you may have to look back one log to get today's log in local time.
Start date	Displays the date of the first log to be searched. This is determined by the entry in the Look back box and cannot be edited.
Search on server	Searches the log of the server selected for the message to be tracked. The server you are connected to is the default.

Interpreting a Message Track

Message tracking results are displayed as a hierarchy of the mail handling events found in the tracking logs. Each line represents one event. Each level in the hierarchy represents a branch in the path of a message, some of which are concurrent.

To get more information, you can:

- Double-click a plus (+) or minus (-) button to expand or collapse the hierarchy.
- Select an event and choose **Properties** to see event detail.
- In the Message Tracking Center, choose **Find Recipient in Tracking History** to search for recipients specified in the message search. Events involving those recipients appear in bold.
- In the Message Tracking Center, choose **Search** to return to the **Select Message to Track** dialog box, and then select another message to track.
- In the Message Tracking Center, choose **Advanced Search** to return to the **Advanced Search** dialog box.

To follow up on a problem message, you can consult the message queues of affected components, raise the diagnostics logging level of a component or service, consult the Windows NT application event log, or change the configuration of a component.

Tracking Log

The tracking log is stored in Exchsrvr\tracking.log. Each day, a new log is created that records one day's activities on the server. Each daily log is named by the date on which it was created, in *yyyymmdd.log* format. The file name date, like all time in the tracking log, is in UTC.

The log can be displayed in any text editor, imported into spreadsheets such as Microsoft Excel, or used as input data to custom applications.

Activities recorded in the tracking log often include a message ID, which is a unique message identifier. By searching the tracking log for the message ID, you can follow the message as it is handled and transported within the site.

The Microsoft Exchange Server Administrator program includes an automated message tracking process. The **Track Message** command traces messages through all existing logs in the network. You can use this process instead of attempting a manual search of the logs.

Interpreting Tracking Log Fields

The following table describes the tab-separated columns in the tracking logs.

Field #	Field Name	Description
1	Message ID or MTS-ID	<p>Message ID is a unique identifier assigned to the message by Microsoft Exchange Server. It stays with the message from its origination to delivery or transfer from the network.</p> <p>Messages from foreign systems include a message transfer system-ID (MTS-ID) that uniquely identifies the component that transported the message.</p>
2	Event #	Represents the event type. For event details, see “Interpreting Events” later in this chapter.
3	Date/Time	Date and time of the event UTC.
4	Gateway name	Name of the gateway or connector that generated the event. If no gateway was involved, the field is blank.
5	Partner name	Name of the messaging service associated with the event. In Microsoft Exchange Server, the partner is the MTA or the information store.
6	Remote ID	Message ID used by the gateway.
7	Originator	Distinguished name of the originating mailbox, if known.
8	Priority	<p>Priority set by the sender.</p> <p>0 = Normal</p> <p>1 = High</p> <p>-1 = Low</p>
9	Length	Message length in bytes.
10	Seconds	<p>Transport time in seconds.</p> <p>Not used by Microsoft Exchange Server. The value in this field is 0 or blank.</p>
11	Cost	<p>Cost per second for message transfer.</p> <p>Not used by Microsoft Exchange Server. The value in this field is always 1.</p>
12	Recipients	Number of recipients.

(continued)

Field #	Field Name	Description
13	Recipient name	Distinguished name of the recipient of the message or a proxy address. This field is separated from the previous field by a line feed. This field is repeated for each recipient.
14	Recipient report status	A number representing the result of an attempt to deliver a report to the recipient. Delivered = 0 Not delivered = 1 This is used only for reports. On other events, it is blank. This field is repeated for each recipient.

Interpreting Events

The following table defines event numbers that appear in tracking logs.

Event #	Event Type	Description
0	Message transfer in	The MTA completed transfer of responsibility for a message from a gateway, X.400 link, or MTA into the local MTA.
1	Probe transfer in	The MTA completed transfer of responsibility for a probe from a gateway, X.400 link, or MTA into the local MTA.
2	Report transfer in	The MTA completed transfer of responsibility for a report from a gateway, X.400 link, or MTA into the local MTA.
4	Message submission	A message was submitted by a local e-mail client (usually through the information store).
5	Probe submission	An X.400 probe was submitted by a local e-mail client (usually through the information store).
6	Probe transfer out	The MTA completed transfer of responsibility for a probe from the local MTA to a gateway, X.400 link, or another MTA.
7	Message transfer out	The MTA completed transfer of responsibility for a message from the local MTA to a gateway, X.400 link, or another MTA.
8	Report transfer out	The MTA completed transfer of responsibility for a report from the local MTA to a gateway, X.400 link, or another MTA.
9	Message delivered	The MTA completed delivery of a message to local recipients (usually through the information store).

(continued)

Event #	Event Type	Description
10	Report delivered	The MTA completed delivery of a receipt or NDR to local recipients (usually through the information store).
26	Distribution list expansion	The MTA has expanded a distribution list to produce a new message that has recipients who are distribution list members.
28	Message redirected	The MTA has redirected a message or probe to an alternate recipient because of incorrect configuration data for the original recipient, or failure to route the object or reassignment of data contained in the message.
29	Message rerouted	The MTA has rerouted a message, report, or probe because of problems with next route X.400 link or MTA.
31	Downgrading	The MTA has mapped a message, report, or probe into the 1984 X.400 protocol before transferring it to a remote 1984 MTA.
33	Report absorption	The MTA has scheduled a report for deletion because the user did not request it. In X.400 protocol, NDRs are always routed back to the sending MTA even if the user did not request a report.
34	Report generation	The MTA has created a delivery receipt or NDR.
43	Unroutable report discarded	The MTA has discarded a report because the report cannot be routed to its destination.
50	Gateway deleted message	The administrator deleted an X.400 message that was queued by the MTA for transfer to a gateway. No delivery report is generated.
51	Gateway deleted probe	The administrator deleted an X.400 probe that was queued by the MTA for transfer to a gateway. No delivery report is generated.
52	Gateway deleted report	The administrator deleted an X.400 report that was queued by the MTA for transfer to a gateway. No delivery report is generated.
1000	Local Delivery	The sender and recipient are on the same server.
1001	Backbone transfer in	Mail was received from another Messaging Application Programming Interface (MAPI) system across a connector or gateway.
1002	Backbone transfer out	Mail was sent to another MAPI system across a connector or gateway.

(continued)

Event #	Event Type	Description
1003	Gateway transfer out	The message was sent through a gateway.
1004	Gateway transfer in	The message was received from a gateway.
1005	Gateway report transfer in	A delivery receipt or NDR was received from a gateway.
1006	Gateway report transfer out	A delivery receipt or NDR was sent through a gateway.
1007	Gateway report generation	A gateway generated an NDR for a message.
1010	SMTP Queued Outbound	Outbound mail was queued for delivery by the Internet Mail Service.
1011	SMTP Transferred Outbound	Outbound mail was transferred to an Internet recipient.
1012	SMTP Received Inbound	Inbound mail was received from by the Internet Mail Service.
1013	SMTP Transferred Inbound	Mail received by the Internet Mail Service was transferred to the Information Store.
1014	SMTP Message Rerouted	An Internet message is being rerouted or forwarded to the proper location.
1015	SMTP Report Transferred In	A delivery receipt or NDR was received by the Internet Mail Service.
1016	SMTP Report Transferred Out	A delivery receipt or NDR was sent to the Internet Mail Service.
1017	SMTP Report Generated	A delivery receipt or NDR was created.
1018	SMTP Report Absorbed	The receipt or NDR could not be delivered.

Message Queues

MTA, Internet Mail Service, and Microsoft Mail Connector message queues can be viewed and modified. The queues are accessed in the **Queues** property page for each component. You can display the queues, delete messages and, in some MTA queues, change the order of the message in the queue.

When mail is not reaching its destination, it is important to examine the queues. A long queue can indicate a problem with the physical connection between servers, a server or MTA configuration error, or an improperly configured connector. Normally, mail should not be retained in the queues for long. Use the **Queues** property page to delete any corrupted messages that are blocking the queues.

MTA Queues

The MTA maintains queues for each message destination. This includes the MTAs of other servers in its site, the information store on its server, and any installed connectors, including RAS Connectors, Site Connectors, X.400 Connectors, Internet Mail Services, and Microsoft Mail Connectors. If the server is a replication bridgehead, the MTA will also have a queue to the directory on its server.

There are two types of queues. The type determines when you see the queue in the MTA **Queues** property page and whether you can change the order of messages in the queue.

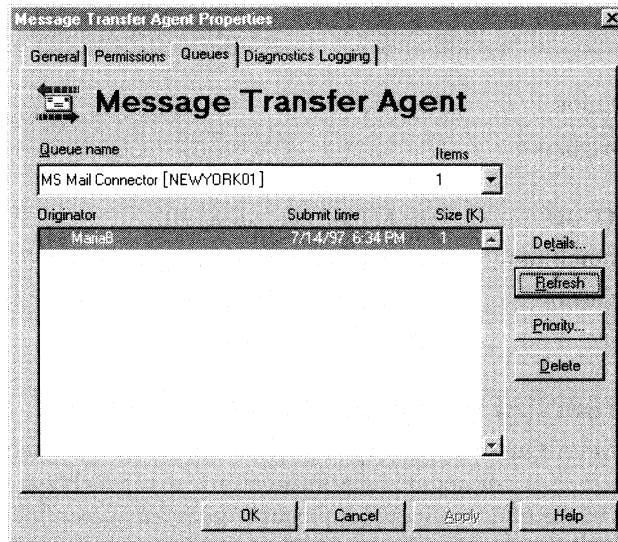
Secured queues Part of the application interface to the MTA. The MTA queues to the Internet Mail Service and Microsoft Mail Connector are secured. They do not appear in the queue list until the connector sends messages to or retrieves messages from the MTA. You cannot change the priority of messages in these queues.

Unsecured queues Part of the MTA and appear in the queue list whenever the receiving service is running. You can change the priority of messages in this queue. MTA queues to components on its server and to Site Connectors, RAS Connectors, X.400 Connectors, and the MTAs of other servers in its site are unsecured.

Use the MTA **Queues** property page to determine the number of messages in each queue, to view a message in the queue in detail, to delete a pending message, and, for unsecured queues, to change the order of messages in a queue.

Getting to the MTA Queues property page

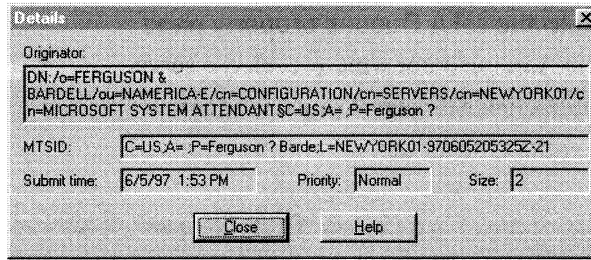
1. In the Administrator window, select a server.
2. Double-click **Message Transfer Agent**.
3. Select the **Queues** tab.



Viewing Message Detail

The message detail available in the queues can be useful for troubleshooting:

- The originator information, taken from the message heading, shows the sending or receiving server. If the same server is involved in several suspect messages, there may be a server configuration error.
 - Use the MTS-ID or message ID to trace the message through the tracking log, event log, or other queues.
1. Select the **Queues** tab.
 2. Under **Queue Name**, select a queue.
 3. Double-click a message.



Option	Description
Originator	The location of the sender, including the host address and sender name.
MTSID	The MTS-ID or message ID.
Submit time	The time the message was submitted in local time.
Priority	The importance assigned to the message by the sender.
Size	Size of the message in bytes.

Refreshing the Queue Property Page

The MTA **Queues** property page is a snapshot of the queues taken when you select it. It is not updated automatically. Use the **Refresh** button to update your view of the queues. Secured queues appear only when there is mail to be sent to or received from them. They can appear or disappear from the list when it is refreshed.

1. Select the **Queues** tab.
2. Choose **Refresh**.

Changing Message Order

You can change the order of pending messages in unsecured queues. Messages in MTA queues to components on its server and to site connectors, RAS Connectors, X.400 Connectors, and the MTAs of other servers in its site can be reordered. This is very useful if an urgent message needs to be delivered immediately, or you suspect that a message is defective.

Use the **Priority** button to increase the priority of urgent messages and lower the priority of messages that might block the queue. Priority is a sort parameter. Messages with the same priority appear in the queue in the order in which they were received.

Note You cannot change the priority of messages in MTA queues to the Microsoft Mail Connector or to the Internet Mail Service. These are secured queues. Also, you cannot change the priority of the first message in an MTA queue if it is already being transported.

1. Select the **Queues** tab.
2. Under **Queue Name**, select a queue.
3. Select a message in the queue.
4. Choose **Priority**, and then select a priority.

Option	Description
High	Highest priority level. If the priority of other messages in the queue is Normal or Low, setting the priority of a message to High moves it to the top of the queue.
Normal	Medium priority level. This is the default.
Low	Lowest priority level. If the priority of other messages in the queue is High or Normal, setting the priority of a message to Low moves it to the end of the queue.

Deleting Messages

Messages can be deleted from unsecured queues. Deleted messages are returned to the originator as non-deliverable. For example, you can delete a queued message if it is too large.

1. Select the **Queues** tab.
2. Under **Queue Name**, select a queue.
3. Select a message in the queue.
4. Choose **Delete**.

Using MTA Message Queues for Troubleshooting

You can use the information in MTA queues to resolve message delays and find missing messages.

Tip Use the MTA Connections **Queue Size** counter in Windows NT Performance Monitor to alert you when messages accumulate in MTA queues. For more information, see Chapter 3, “Monitoring Your Organization.”

- If a queue has more messages than expected, check the configuration of the destination server for the first messages in the queue, and search the application event log for problems with the connection.

- The **Submit Time** displayed in the **Queues** property page identifies when the MTA received the item. Compare this to the time the message was sent to determine where delays are occurring.
- If you suspect that a message will block the queue, delete the message, or, if the queue is unsecured, lower its priority to allow other messages to pass it.
- If the message being transported is blocking the queue, use your link and server monitors to make sure the receiving service is operating and that all connections are operating. Check the application event log for errors generated by the receiving service or the MTA. If you must delete the message, stop the receiving service. This releases the message so you can delete it.
- If messages are accumulating in the MTA queue to the Internet Mail Service, check the Internet Mail Service MTA Out queue to determine whether it is retrieving its messages from the queue. This is the destination for messages in the MTA queue to the Internet Mail Service.
- If an MTA queue to another service is blocked, most likely a message in the queue is corrupt, the receiving service is not retrieving its messages from the queue, or the MTA is not functioning correctly.

Internet Mail Service Queues

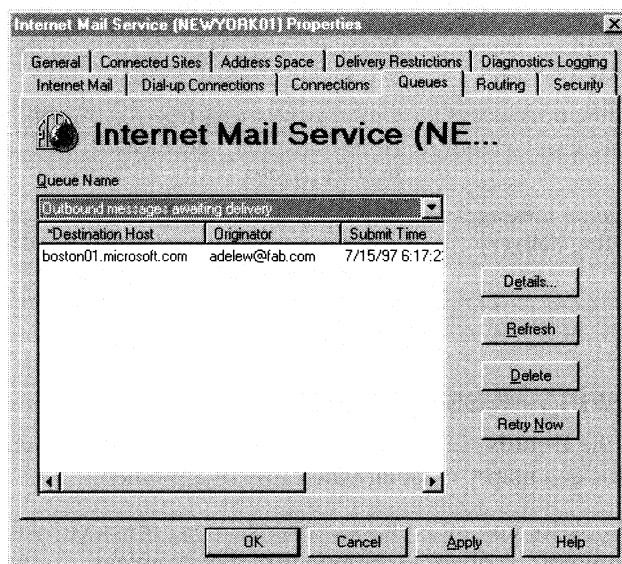
The Internet Mail Service queues on each server should be examined when you suspect problems with Internet mail. Using the Internet Mail Service **Queues** property page, you can view important information about messages in the queues and delete problem messages. However, you cannot reorder messages in the queue.

Use the Internet Mail Service **Queues** property page to determine the number of messages in each queue, to view message detail, and to delete messages.

For more information about configuring the Internet Mail Service, see *Microsoft Exchange Server Operations*.

Getting to the Internet Mail Service Queues property page

1. In the Administrator window, choose **Connections**.
2. Double-click an Internet Mail Service.
3. Select the **Queues** tab.



Selecting a Queue

There are four queues for the Internet Mail Service. Outbound messages travel from the MTA's Internet Mail Service queue (Exchsrvr\Imcddata\Out) to the Internet Mail Service's MTS-OUT queue in the information store. The Internet Mail Service converts the messages and places them in the Out queue until they are sent. The Internet Mail Service places messages received from the Internet in its In queue (Exchsrvr\Imcddata\In). The messages are then converted by the Internet Mail Service and moved to the MTS-IN queue in the information store.

1. Select the **Queues** tab.
2. Under **Queue Name**, select a queue.

Option	Description
Inbound messages awaiting conversion	Incoming messages waiting to be converted or rerouted by the Internet Mail Service and then delivered to the information store.
Inbound messages awaiting delivery	Messages in the MTS-IN folder in the information store. The next destination is the recipient.
Outbound messages awaiting conversion	Outgoing messages received from the MTA and waiting to be converted by the Internet Mail Service. The next destination is the Out queue.
Outgoing messages awaiting delivery	Messages queued for delivery in the Internet Mail Service scheduler, which roughly corresponds to the message files in the Imcdata\Out directory. Because some messages require delivery to multiple hosts, there may be more entries in the queue than there are files in the directory.

Viewing Message Detail

Use the **Details** dialog box to view additional information about a message. The details can help you isolate the cause of a problem.

- Look for common characteristics among messages with failed delivery attempts, such as a common server or recipient.
- Delivery status and information about failed attempts help to detect corrupt messages.
- Use the message transfer system ID (MTS-ID) and message ID to search for the message in the tracking log and application event log.

1. Select the **Queues** tab.
2. Under **Queue Name**, select a queue.
3. Double-click a message.

Option	Description
Originator	The address from which the message was sent.
MTS-ID	A unique identifier for the component that transported the message. It consists of the originating server, the date and time the message was sent, and a hexadecimal identifier. This is blank in messages in the In and Out queues.
Message ID	A unique identifier assigned to the message by Microsoft Exchange Server. It stays with the message from its origination to delivery or transfer from the network. This is blank in messages in the MTS Out queue.
Destination Host	The server computer to which the message is being delivered.
Submit Time	Time the message arrived in the queue UTC.
Size	Size of the message in bytes.
Next Retry Time	The time scheduled for resending the message if previous attempts were unsuccessful.
Retries	Number of times the connector attempted to deliver the message.
Expiration	The time when all retries will be exhausted.
Recipients	The addresses of intended recipients and the status of attempts to deliver the message to that address.

Refreshing the Queues Property Page

The Internet Mail Service **Queues** property page is a snapshot of the queues taken when you select it. It is not updated automatically. Use the **Refresh** button to update your view of the queues.

1. Select the **Queues** tab.
2. Choose **Refresh**.

Deleting Messages

You can delete messages that are interfering with queue processing. Deleted messages are permanently erased from the disk and a non-delivery report (NDR) is sent to the originator.

Note You cannot delete messages from the MTS-IN folder.

Undeliverable messages should be deleted so they don't block an Internet Mail Service queue. If a connector cannot transport a message, it continues processing other messages in the queue and attempts to send the undeliverable message later if it hasn't been deleted.

1. Select the **Queues** tab.
2. Under **Queue Name**, select a queue.
3. Select a message.
4. Choose **Delete**.

Forcing a Retry

Use the **Retry Now** button to force the Internet Mail Service to attempt to transport a message in the queue. For example, you can do this if you want to send a queued message immediately.

Note You can only force a retry for messages in the MTS-OUT folder.

1. Select the **Queues** tab.
2. Under **Queue Name**, select a queue.
3. Select a message.
4. Choose **Retry Now**.

Using Internet Mail Service Queues for Troubleshooting

Use the Internet Mail Service **Queues** property page to diagnose and resolve Internet mail problems.

- If messages are accumulating in the queue, check the configuration of the destination server for the first messages in the queue.
- Create an SMTP protocol log for the server. This log is created by increasing the diagnostics logging level for the SMTP Protocol Log category to Medium. For more information, see “Changing Internet Mail Service Logging Levels” earlier in this chapter.
- The **Submit Time** box displays the time the item arrived in the queue. Compare this time to the time the message was sent to determine at which point delays may be occurring.

- The **Delivery** column displays “pending” for messages it has not attempted to deliver. If a **Submit time** is displayed, at least one attempt to deliver the message has failed. The time shown is the scheduled time for the next attempt. Focus on messages that have failed at least one delivery and find common characteristics, such as a destination server.
- To view details on a specific message, select a recipient in the message list displayed in the **Outbound messages awaiting delivery** window.

Microsoft Mail Connector Queues

Each Microsoft Mail Connector maintains a queue of pending outbound messages from each of its connections. You can display the queue for each connection, return messages to the sender, and delete problem messages from the queue. Each message in a queue has an ID so you can follow the message in the tracking log and in the application event log.

Normally, messages appear in the queue for only a brief interval. Any lingering messages should be investigated.

Use the Microsoft Mail Connector **Connections** property page to examine the queue of outbound messages for each MS Mail connection. Each Microsoft Mail Connector in the site has its own queues, so make sure to select the correct one.

Getting to the Microsoft Mail Connector Connections property page

1. In the Administrator window, choose **Connections**.
2. Double-click a Microsoft Mail Connector.
3. Select the **Connections** tab.



Selecting a Queue

The **Connections** property page shows the hierarchy of connections for a Microsoft Mail Connector. You can select a connection and display its queue of outbound messages.

Each line under **Queued Messages** represents one outbound message pending delivery. The information comes from the message envelope. To sort queued messages, click the column heading buttons.

1. Select the **Connections** tab.
2. Select a connection.
3. Choose **Queue**.

Option	Description
From	The e-mail address of the sender.
Subject	Subject of the message as taken from the subject line.
Message ID	The unique identifier assigned to the message. This can be used to trace the message in the event log, tracking log, and MTA queues.
Date/Time	The date and time the message was submitted in local time.
Send Non-Delivery Reports when messages deleted	If selected, an NDR is sent to the originator when a message is deleted from the queue. Otherwise, there is no notification.

Refreshing the Queue

The information under **Queued Messages** is a snapshot of the queues taken when you open it. It is not updated automatically. Use the **Refresh** button to update your view of the queues.

1. In the **Connections** property page, choose **Queue**.
2. Choose **Refresh** to update your view of the queue.

Returning Messages

You can return messages from the outbound queue of any connector to its originator. In addition to responding to user requests, this is useful if a message appears to be blocking the queue. To test the path of a message, return the message, and follow it in the tracking log.

1. Select the **Connections** tab.
2. Select a connection.
3. Choose **Queue**.
4. Select a message.
5. Choose **Return**.

Deleting Messages

Messages that delay the processing of a queue can be deleted from the queue. Deleted messages are erased from the disk. If **Send Non-Delivery Reports when messages deleted** is selected, an NDR is sent to the originator.

1. Select the **Connections** tab.
2. Select a connection.
3. Choose **Queue**.
4. Select a message.
5. Choose **Delete**.

Using Microsoft Mail Queues for Troubleshooting

Use the information in the **Queues** property page to diagnose and resolve Microsoft Mail problems.

- The **Submit Time** box displays the time the item arrived in the queue. Compare this time to the time the message was sent to determine where delays are occurring.
- If sent messages are not appearing in this queue, check the MTA queue to the Microsoft Mail Connector to verify that messages are being submitted to the connector.
- Check the integrity of the connector postoffice.

Troubleshooting Utilities

Troubleshooting the components of Microsoft Exchange Server is made easier by using the MTACHECK and ISINTEG utilities.

MTACHECK

MTACHECK scans the internal database of the MTA looking for objects that are damaged and interfering with queue processing. It places defective objects from the queues in files for you to examine later. In addition, MTACHECK rebuilds the queues so the MTA can be restarted and resume to processing.

If your MTA stops and cannot be restarted, MTACHECK can get it running again. It can also be used for routine checks of the integrity of MTA database queues.

If MTACHECK removes objects from a database queue, you can recover them. MTACHECK places all objects it considers to be damaged in a Db*.dat file in Exchsrvr\Mtadata\Mtacheck.out. You can examine the objects and repair or delete them.

Running MTACHECK

Mtacheck.exe is in the Exchsrvr\Bin directory. It must be run from the command line of the server with the MTA problem. The MTA must be stopped, and the Mtacheck.out subdirectory, where MTACHECK places defective objects, must be empty or deleted. MTACHECK displays progress messages. Use the options to regulate the detail of the messages or to copy them to a log file.

1. Stop the MTA.
2. Empty Exchsrvr\Mtadata\Mtacheck.out*.*
3. At the command prompt, type **mtacheck**, followed by one or both of the options.

For example:

```
C:\EXCHSRVR\BIN> mtacheck /f mtacheck.log
```

runs MTACHECK with standard logging detail copied to Mtacheck.log.

Option	Description
<i>/v</i>	Increases the frequency and detail of progress messages.
<i>/f filename</i>	Displays progress messages and also sends them to the specified file.

Interpreting MTACHECK Output

MTACHECK examines each queue in the database. If it finds an error, it reports the name of the queue, the type of error, and the number of messages returned to the rebuilt queue.

For example:

```
Queue 'xxxxxxx' required reconstruction
- corrupted queue file
23 messages recovered to the queue
```

It then examines objects in the queues. If an object is in error, it removes it from the queue and places it in a file in Exchsrvr\Mtadata\Mtacheck.out. It reports the object ID, error type, queue name, and the MTS-ID of the corrupted message, if known.

An MTS-ID is assigned to each message by its transport service and remains with the message to its destination, although gateways can assign additional identifiers. It consists of the originating server, the date and time the message was sent, and a unique hexadecimal identifier.

A sample MTACHECK log can include:

```
Object 300596 invalid
- missing object file
Object removed from queue 'xxxxxxx'
MTS-ID: c=US;a=p=Ferguson;l=NEWYORK0196012020010800000CDE
```

When the MTA finishes processing, it displays one of following messages to describe the results:

```
Database clean, no errors detected
Database repaired, some data may have been lost
- (number) queues required repair out of x% detected
- (number) objects damaged out of y% detected
Database has serious errors and cannot be reconstructed
Some objects missing from the Boot Environment. Please reload the
files from the BOOTENV directory on the install CD.
```

The boot environment message indicates that report templates and other objects the MTA needs are missing, and the MTA cannot generate them. These objects are included in the files in the Bootenv directory. Once you have installed them, rerun MTACHECK. When the process is complete, restart the MTA.

Caution Copy only objects that are missing to the boot environment. If you replace existing objects, all messages in MTA queues will be deleted.

Searching Message Logs by Message ID

MTACHECK also reports the message ID of removed objects in its log if it can be determined. If message tracking is enabled, you can search the tracking log for the object by its message ID. Determining the path of the bad message can lead you to the cause of the problem. You may need to search the logs of more than one site to find the complete path of the message.

1. Copy the message ID from the MTACHECK log.
2. From the **Tools** menu in the Administrator window, choose **Track Message**.
3. In the **Connect to Server** dialog box, type the name of a server.
4. In the **Select Message to Track** dialog box, choose **Cancel**.
5. In the **Message Tracking Center**, choose **Advanced Search**.
6. Choose **By Message ID**.
7. Press CTRL+V to paste the MTS-ID into the **Message ID** box of the **Select Messages to Track** dialog box.
8. In the **Message Tracking Center**, choose **Track**.

For more information about message IDs and tracking messages, see “Message Tracking” earlier in this chapter.

ISINTEG

The Information Store Integrity Checker (ISINTEG) finds and eliminates common errors from the Microsoft Exchange Server public and private information store databases. These errors can prevent the information store from starting or prevent users from logging on and receiving, opening, or deleting mail.

ISINTEG has three modes that are run independently:

- Check mode
- Check and fix mode
- Patch mode

In Check mode, ISINTEG searches the information store databases for table errors, incorrect reference counts, and unreferenced objects. During this operation, ISINTEG displays the results and writes them to a log file.

Check and fix mode should be used only at the advice of Microsoft Technical Support. In check and fix mode, ISINTEG performs the tests in check mode and corrects the errors. It is recommended that you perform a backup before running this utility. Otherwise, it browses the database, displays the results, and writes them to a log file.

In patch mode, ISINTEG repairs information stores that will not start after being restored from an offline backup.

Checking the Tables

ISINTEG must be run separately on the public and private information store. It is run from the Windows NT Server command line. The information store must be stopped when you run the utility.

Normally, ISINTEG browses only the information store database tables for errors, displays the results, and reports them to a log file. The **-fix** option instructs it to repair the errors it finds. This option should be used only at the advice of Microsoft Technical Support. Details of all repairs are recorded in a log file. If a log file is not specified, the results are written to either `Isinteg.pri` or `Isinteg.pub`, depending on whether the private or public information store was chosen.

Complete the following procedure to run ISINTEG.

1. Stop the information store.
2. At the command prompt, type **isinteg** followed by one or more of the options. The options can be listed in any order. In the following example, ISINTEG checks the private information store database and writes the results to the specified log.

```
C:\EXCHSRVR\BIN> isinteg -pri -l c:\systest\private.log
```

In the following example, ISINTEG checks the public information store, fixes errors, and writes the results to a log file named Isinteg.pub.

```
C:\EXCHSRVR\BIN> isinteg -pub -fix
```

Option	Description
-?	Displays the option list. Does not run the utility.
-pri	Checks the private information store.
-pub	Checks the public information store.
-fix	Corrects table errors and inaccurate cross-reference counts, and deletes unreferenced names. This should be used only at the advice of Microsoft Technical Support.
-verbose	Verifies and reports all activity.
-l (filename)	Changes the name of the log file. The default is Isinteg.pri or Isinteg.pub.

Patching the Information Store

The Microsoft Exchange Server information store cannot start if the globally unique identifier (GUID) for the information store does not match the GUID stored in the Windows NT Registry and the directory. This can occur if the Microsoft Exchange Server has been restored from an offline backup.

In patch mode, ISINTEG replaces GUIDs, resetting the entries in the database, directory and registry. It also patches information used in replication to prevent incorrect backfilling. This completes the restore operation and allows the information store to start again.

ISINTEG patch mode runs on the entire information store. It cannot be run on just the public or private information store database.

Tip If the information store on your server won't start, search for Event ID 2084 in the Windows NT application event log:

The information store was restored from an offline backup. Run ISINTEG -patch before starting the information store.

This indicates that a restore patch is missing and that running the ISINTEG patch will fix the problem.

In patch mode, ISINTEG does not perform database integrity tests. Patch mode and check mode must be run separately. It is recommended that you run ISINTEG in check mode after running it in patch mode.

Complete the following procedure to run ISINTEG in patch mode.

1. Stop the information store.
2. At the command prompt, type **isinteg -patch** followed by one or more of the options described in the "Checking the Tables" section earlier in this chapter. In the following example, ISINTEG replaces GUIDs. The log uses the default file name.

```
C:\EXCHSRVR\BIN> isinteg -patch
```

SNMP Monitoring Agents

Microsoft Exchange Server complies with RFC 1566, which defines industry standards for the Management Information Base for Simple Network Management Protocol (SNMP) Mail and Directory Management (also known as MADMAN MIB). If your system supports SNMP, you can use SNMP to monitor and troubleshoot Microsoft Exchange Server.

Microsoft Exchange Server supports MADMAN MIB by making Windows NT Performance Monitor counters available as MIB objects. A subset of the MTA and Internet Mail Service Performance Monitor counters comprise the variables defined in RFC 1566. However, all counters for these components can be accessed through SNMP because Microsoft Exchange Server provides more comprehensive support than the RFC requires.

MIB Installation for Microsoft Exchange Server

Windows NT Server includes an SNMP agent that can respond to SNMP requests by accessing MIBs in the Mib.bin file. To enable Microsoft Exchange Server to support SNMP, you must install the MIB for the Microsoft Exchange Server computer (Exchange.mib) on your server in the Mib.bin file.

Microsoft Exchange Server provides a compiled version of Exchange.mib that you can install by running a batch file. If you've already configured extension MIBs on your server, you must use other tools included on the Microsoft Exchange Server compact disc to install Exchange.mib instead of the batch file.

Important Before you install SNMP support for Microsoft Exchange Server, the Windows NT SNMP service must already be installed. To install the Windows NT SNMP service, from Control Panel, choose **Network**. After you install the service, you must reinstall the Windows NT Service Pack 3.

Using the Batch File

If you have not installed any MIBs on your server other than those included with Windows NT, run the batch file included on the Microsoft Exchange Server compact disc.

- At the command prompt on the Microsoft Exchange Server computer you want to monitor, run Support\Snmp\platform\Install.bat.

Using Perf2mib.exe and Mibcc.exe

Microsoft Exchange Server includes tools that you can use to install SNMP support. You can use Perf2mib.exe to compile Performance Monitor counters into a new MIB for Microsoft Exchange Server. Mibcc.exe recompiles the Perfmib.mib file created by Perf2mib.exe and creates a new Mib.bin file.

You should use Perf2mib.exe and Mibcc.exe to add Exchange.mib to Mib.bin in the following cases.

- If you have previously added one or more MIBs to Mib.bin, then run Mibcc.exe to rebuild your current Mib.bin.
- If you have previously created a new Mib.bin using Perf2mib.exe, you must run Perf2mib.exe and Mibcc.exe again to create a new MIB.

These tools are available on the Microsoft Exchange Server compact disc in the Support\Snmp\platform directory and in the *Windows NT Resource Kit*. For more information about using these tools, see the *Windows NT Resource Kit*.

The following procedure describes how to use Perf2mib.exe and Mibcc.exe.

1. At the command prompt, run the **Perf2mib** command to create the Perf2mib.mib and Perf2mib.ini files, for example:

```
Perf2mib Perf2mib.mib Perf2mib.ini MExchangeMTA 1 MTA "MExchangeMTA
Connections" 2 "MTA Connections" MExchangeIMC 3 IMS <counter name>
<index> <description>
```

where *counter name*, *index*, and *description* are additional Performance Monitor counters you want to make available in the MIB.

2. Run the **Mibcc** command to create Mib.bin.

```
Mibcc -O mib.bin -n -t -w2 Smi.mib LMMIB2.MIB Mib_II.mib
Perf2mib.mib
```

3. Copy Perf2mib.dll, Perf2mib.ini, and Mib.bin to the System32 subdirectory.
4. Run the **regini** command to set up the registry with the values to support the performance MIB.

```
regini perf2mib.reg
```

5. Restart the SNMP service by choosing **Services** from the Control Panel.

MIB Viewing

You can use any SNMP version 1 compatible management console to view the Microsoft Exchange Server MIB. Your management console may need to load the MIB file for the object descriptions. This file is available on the Microsoft Exchange Server compact disc in Support\snmp\platform\exchange.mib.

Understanding Microsoft Exchange Server Object IDs

The following are Microsoft Exchange Server object IDs. The numerical representation of the object ID is shown following the ID.

MTA

MTA values are accessed using the following object ID.

```
.iso.org.dod.internet.private.enterprises.microsoft.software.systems.
os.winnt.performance.MExchangeMTA
.1.3.6.1.4.1.311.1.1.3.1.1.1
```

MTA Connections

The groups that the MTA services support the following object ID.

```
.iso.org.dod.internet.private.enterprises.microsoft.software.systems.  
os.winnt.performance.MSExchangeMTA  
.1.3.6.1.4.1.311.1.1.3.1.1.2.x
```

where *x* is the index of the group.

Internet Mail Service

Internet Mail Service values are accessed using the following object ID.

```
.iso.org.dod.internet.private.enterprises.microsoft.software.systems.  
os.winnt.performance.MSExchangeIMC  
.1.3.6.1.4.1.311.1.1.3.1.1.3
```

Using the Snmputil Utility

You can also use the **snmputil** utility available with the *Windows NT Resource Kit* to view a MIB.

The following displays the current value for the `mtaInboundBytesTotal` object variable for the Microsoft Exchange Server MTA.

```
snmputil get <server name> public .iso.org.dod.internet.private.  
enterprises.microsoft.software.sysems.OS.WinNT.Performance.1.38.0
```

The following displays the current value for the `mtaOutboundBytesTotal` object variable for the Microsoft Exchange Server MTA connection to the private information store.

```
snmputil get <server name> public .iso.org.dod.internet.private.  
enterprises.microsoft.software.sysems.OS.WinNT.Performance.2.1.32.0
```

The following returns the current value for the `imsQueuedMTS-IN` object variable for the Microsoft Exchange Server Internet Mail Service.

```
snmputil get <server name> public .iso.org.dod.internet.private.  
enterprises.microsoft.software.sysems.OS.WinNT.Performance.3.1.0
```

Performance Monitor Counters

The following table lists the MIB objects defined in RFC 1566 and their corresponding Microsoft Exchange Server counters.

MIB object	MSExchangeIMC counter	MSExchangeMTA counter
MtaReceivedMessages	Inbound Messages Total	Inbound Messages Total
MtaStoredMessages	Total Messages Queued	Work Queue Length
MtaTransmittedMessages	Outbound Messages Total	Outbound Messages Total
MtaReceivedVolume	Inbound Bytes Total	Inbound Bytes Total
MtaStoredVolume	Total Bytes Queued	Work Queue Bytes
MtaTransmittedVolume	Outbound Bytes Total	Outbound Bytes Total
MtaReceivedRecipients	Total Recipients Inbound	Total Recipients Inbound
mtaStoredRecipients	Total Recipients Queued	Total Recipients Queued
mtaTransmittedRecipients	Total Recipients Outbound	Total Recipients Outbound
mtaSuccessfulConvertedMessages	Total Successful Conversions	Total Successful Conversions
mtaFailedConvertedMessages	Total Failed Conversions	Total Failed Conversions
mtaLoopsDetected	Total Loops Detected	Total Loops Detected

Each MTA connection is categorized as a group. The performance monitor MSExchangeMTA Connections provides counters for each live MTA queue. The following table lists the MIB group objects and their related MTA Connections counters.

MIB object	MSExchangeMTA Connections counter
mtaGroupReceivedMessages	Inbound Message Total
mtaGroupRejectedMessages	Inbound Rejected Total
mtaGroupStoredMessages	Queue Length
mtaGroupTransmittedMessages	Outbound Messages Total
mtaGroupReceivedVolume	Inbound Bytes Total
mtaGroupStoredVolume	Queued Bytes
mtaGroupTransmittedVolume	Outbound Bytes Total
mtaGroupReceivedRecipients	Total Recipients Inbound
mtaGroupStoredRecipients	Total Recipients Queued
mtaGroupTransmittedRecipients	Total Recipients Outbound
mtaGroupOldestMessageStored	Oldest Message Queued (seconds)
mtaGroupInboundAssociations	Current Inbound Associations
mtaGroupOutboundAssociations	Current Outbound Associations
mtaGroupAccumulatedInbound Associations	Cumulative Inbound Associations
mtaGroupAccumulatedOutbound Associations	Cumulative Outbound Associations
mtaGroupLastInboundActivity	Last Inbound Association (seconds)
mtaGroupLastOutboundActivity	Last Outbound Association (seconds)
mtaGroupRejectedInbound Associations	Rejected Inbound Association
mtaGroupFailedOutbound Associations	Failed Outbound Associations
mtaGroupInboundRejectionReason	Inbound Rejection Reason
mtaGroupOutboundRejection Reason	Outbound Connect Failure Reason
mtaGroupScheduledRetry	Next Association Retry (seconds)

Other Tools and Resources

Additional tools and resources are available for troubleshooting Microsoft Exchange Server.

Other Tools

These tools are available to assist in troubleshooting Microsoft Exchange Server.

Windows NT Control Panel Controls the operation of Windows NT services and the Microsoft Exchange Server services built upon them.

Windows NT Server Manager Used to configure services and server shares remotely on Windows NT Server computers.

Windows NT Diagnostics Displays detailed system information on the local computer, including memory, drivers, services, network and environment configuration.

Dr. Watson A Windows NT utility that automatically creates reports on application errors. It appears only when an application error occurs.

PView Displays the memory and resources in use by each process on a Windows NT Server computer. This tool is part of the *Windows NT Resource Kit*.

RPC Ping Checks RPC connectivity between clients and servers.

Ping Tests the connectivity between SMTP servers by sending ping messages. If you add the command-line option **-l**, it displays the time it takes for a 1KB message to complete the route.

Ping-1 Measures the travel time of a ping message from one Internet Protocol (IP) address to another.

Netstat Shows protocol statistics and current TCP/IP network connections. Type **netstat** at the command prompt to determine how many connections are running on an Internet Mail Service.

Network Analyzer Watches network traffic on a local area network (LAN) or wide area network (WAN), including available bandwidth and collision errors. It is recommended that you have access to one of the many network analyzers available on the market.

Network Topology Maps and Message Routing Maps Topology and routing maps, usually prepared when planning your network, should include Microsoft Exchange Server computers, gateways to other systems, site boundaries, client installation points, computers running monitors, and user connections to the network. It should have keys describing bandwidth, supported protocols, file servers, routers, and bridges. The maps help you interpret the data you collect from link and server monitors to find patterns of outages.

Telnet to Port 25 Tests communication connections to SMTP networks. At the command line, type **telnet *hostname* 25**. When you are finished, type **quit**.

Documentation

The following additional documentation can help troubleshoot Microsoft Exchange Server:

- Windows NT Server documentation
- *Windows NT Resource Kit*
- *Microsoft Exchange Server Resource Guide* and *Microsoft Exchange Server Resource Guide, Supplement*
- Microsoft Systems Management Server documentation
- *Microsoft Mail for PC Networks Administrator Guide* (gateway, directory synchronization, modem script files)

Other Resources

You have other sources of troubleshooting help available to you. The following is a list of organizations and places to turn to for training, product updates and information, and professional help:

- Microsoft Technical Support
- Microsoft Exchange Server Web site at <http://www.microsoft.com/exchange>
- Microsoft Consulting Service (MCS)
- Microsoft Support Partners
- Microsoft Certified Professionals
- Microsoft's Internet File Transfer Protocol (FTP) site
- Microsoft Knowledge Base
- Microsoft TechNet subscription service

CHAPTER 5

Troubleshooting Your System



Troubleshooting Microsoft Exchange Server requires using the available tools and resources to narrow down a problem to a specific component, finding the cause, and then solving the problem.

This chapter covers some typical problems you can encounter while using Microsoft Exchange Server. It is organized alphabetically by problem type.

Note Advanced knowledge of Windows NT and your Microsoft Exchange Server network environment is recommended.

Addressing

Typical problems with addressing are caused by incorrect addresses or an inadequate address space. Address space problems occur if you remove routes before adding new ones. Recipient problems occur when recipients are removed from a site before the directories are replicated.

You can't find a recipient in the global address list.

Reasons	Actions
The recipient is in a different site in your organization or in a foreign system, and the directory has not been replicated.	Use the Administrator program to see the directory replication schedule. Replication messages can be traced in the message tracking log. Use the Windows NT application event log to determine if there are errors in directory replication.
The recipient has been removed from this site or another site in the network.	Use the Administrator program to confirm that the recipient was removed.
The recipient is hidden from the Address Book.	From the View menu in the Administrator window, choose Hidden Recipients . The recipient should appear. All public folders are hidden recipients.

You receive a non-delivery report (NDR) indicating an invalid address.

Reasons	Actions
The recipient's address is incorrect.	Confirm the recipient's address and update the user's personal address book (PAB) and the global address list.
The recipient was removed from another site or foreign system and the directory has not been replicated or synchronized.	Confirm that the recipient was removed. Verify that the update is included in the next directory replication.
There is a routing problem.	Trace the message in the message tracking log. Verify that the address space is configured correctly.

The PAB entry is invalid for a recipient in a different site.

Reasons	Actions
The address entry is incorrect.	Verify the recipient's address in the global address list. Copy the address from the global address list to the PAB. Use the Administrator program to check the address space.
The recipient has been removed.	Verify the entry in the global address list. If it is there, wait for the next directory replication and check again.
The address space for entries is not mapped to a gateway or connector.	Update the Address Space property page for the connector or gateway.

The PAB entry is invalid for a recipient in the same site.

Reasons	Actions
The recipient has been removed.	Verify the entry in the global address list.
The recipient was moved to a different recipient container.	Check the global address list to see if the recipient has been moved.

Administrator Program

Microsoft Exchange Server is designed to be easy for you to administer and to provide you with all the information you need. When an error occurs, there are many resources to fix the problem.

You can't connect to a server using the Administrator program.

Reasons	Actions
You do not have Administrator permissions for this site.	Have someone with the appropriate permissions use the Administrator program to grant you permissions for this site.
You do not have Administrator permissions for this site; the only person who does is unavailable.	Log on to Windows NT as the service account and start the Administrator program.

You can't open a server.

Reasons	Actions
There are no network connections to the server.	At the Windows NT command prompt, use the Net View \\servername command to check the network connections.
The server computer is not running.	At the Windows NT command prompt, use the Net View \\servername command to check the network connections.
The directory service is not running.	Establish a server monitor from another server in the site to determine the status of the directory.
You do not have Administrator permissions for this server or site.	Have someone with the appropriate permissions use the Administrator program to grant you permissions.

You can't modify an object.

Reasons	Actions
The object is in a different site in the same physical network.	Connect to a server in the site where the object is located, and modify it there.
You don't have permissions for the object.	Have someone with the appropriate permissions use the Administrator program to grant you permissions.
You need Add or Delete permission.	Use the Administrator program to modify the appropriate Permissions property page.

You can't view servers in another site.

Reason	Actions
If the servers have never been visible, either directory replication was not configured or it was unsuccessful.	<p>Use a link monitor to test connections. If they are operating, configure directory replication from the other site to this one.</p> <p>Trace the path of the replication message in the message tracking log.</p> <p>Increase the diagnostics logging level for the Directory Replication Events category, and then check the Windows NT application event log for directory replication errors.</p>

Another site isn't visible.

Reasons	Actions
Replication between sites has not been configured.	For information on connecting to other sites, see <i>Microsoft Exchange Server Operations</i> .
The directory is corrupted.	Restore the directory database from the tape backup.

You can't remove a recipient from a distribution list.

Reasons	Actions
The distribution list is in another site.	Connect to the server in the site where the distribution list is located, and modify it.
You do not have permissions to modify a distribution list.	Have someone with appropriate permissions make the changes or grant you permissions to modify it.

When you use the Browse button, you can't view a server.

Reasons	Actions
The server is not on this local area network (LAN) segment.	Type the name of the server in the Connect to Server box instead of using the Browse button.
The server is on this LAN segment, but it is not running.	Restart the server.
The server is on this LAN segment, but it is in a different site.	Browse from a server in the same site, or type the name of the server in the Connect to Server box instead of using the Browse button.

There are problems sending and receiving mail.

Reasons	Actions
The address is not correctly defined.	Modify the entries in the Address Space property page for the connector.
A message transfer agent (MTA) is down.	Use server monitors and message queues to locate the MTA.
The schedule is not set to transfer mail at this time.	Check the X.400 Connector or Dynamic RAS Connector Schedule property page.

Clients

E-mail client problems are usually related to the network, Windows NT permissions, or configuration problems.

Mail sent to a user never arrives.

Reasons	Actions
There is a problem on a foreign system.	Use the message tracking log to trace the path of the message to the gateway. Look for the message in the message queues of the connector. Check the Windows NT application event log for errors. If it is an Internet message, use diagnostics logging to create a Simple Mail Transfer Protocol (SMTP) log, and resend the message.
The message is still in the Outbox because the information store or MTA is not running.	Verify that the originator can send e-mail to other Microsoft Exchange Server mailboxes, or check the service with Performance Monitor or a server monitor.
The message stopped at an intermediate server or system.	Use message tracking to find the problem server. For more information, see Chapter 4, "Troubleshooting Tools and Resources."

A client can't connect to a server.

Reasons	Actions
The profile is not configured correctly.	Check the server and mailbox name configured for the e-mail client.
The server is unavailable.	<p>Use a link monitor or server monitor to check the service.</p> <p>Also, use the Net View \\servername command to determine if the server is running. If you are running a NetWare client, use the Ping command to test the connection.</p>
The server is using a different network protocol.	At the Windows NT command prompt, use the Rping command to determine remote procedure call (RPC) connectivity. If necessary, update the server or all affected clients with matching network protocols.
The common network protocol being used is not routed between LAN segments.	Move the client or server computers to the same LAN segment. Modify the router or bridge to route the network protocol. Update the client and server to use a commonly routed network protocol.
You do not have User permission for the mailbox.	Check the mailbox Permissions property page and modify it if necessary.
The Windows NT Server running Microsoft Exchange Server is not configured to support Novell NetWare clients.	Verify that the server is running the Gateway Services for NetWare and that the NWLink IPX/SPX transport is configured correctly using the Network icon in Control Panel.
Novell NetWare client and server computers have different frame type versions.	<p>On the client computer, the frame type is in the Link Driver section of the Net.cfg file. On the server, the frame type is in the configuration of the NWLink IPX/SPX compatible transport object in the Network icon of Control Panel.</p> <p>If the server computer supports more than one frame type, make sure that the internal network number is unique and Auto Frame type detection is not selected.</p>
There is no SAP agent computer accessible to both computers running the e-mail client and Microsoft Exchange Server.	<p>Verify that both the client and server computers can log on to a SAP agent computer. The SAP agent can run on a Microsoft Exchange Server computer or on a NetWare server.</p> <p>Verify that the client and server are on the same network segment and that the router between the segments is configured to transport SAP type 0x640 messages.</p>

Connections Between Microsoft Exchange Servers

Microsoft Exchange Server computers within a site communicate with each other automatically using RPCs and named pipes. Because there are many options for connecting servers, configuration and network problems can prevent communication.

The MTA queue is growing.

Reasons	Actions
There is not enough bandwidth to support the traffic.	Use a network analyzer to check network usage.
The destination MTA is down.	Use a server monitor and Performance Monitor to determine if the services are running and if mail is being processed.
The network is down between MTAs.	Use the Ping or Net Use command from one server to the other to determine if they can communicate with each other.

There are problems with mail between sites.

Reasons	Actions
The address space was defined incorrectly.	Use the Administrator program to change the address space for the connection.
One of the MTAs is down.	Use a server monitor or Performance Monitor to determine the status of the MTA. Message queues are helpful in determining the problem. A long queue can indicate a problem with the physical connection between servers, a server or MTA configuration error, or an incorrectly configured connector.
Mail is not scheduled to be transferred between sites at this time.	Check the Schedule property page for the connector.
Site-to-site communication is configured correctly, but the transport is not routed between sites on the wide area network (WAN).	Use network tools to test connectivity and the transport network protocol between bridgehead servers in the sites. Change the supported network protocol or reconfigure the network. An SMTP protocol log is available for Internet mail. For more information, see Chapter 4, "Troubleshooting Tools and Resources."
Mail is returned to sender because of size.	Check the NDR for details. If the recipient is a Microsoft Exchange Server mailbox, check the recipient's Inbox Assistant for advanced rules limiting the size of mail sent.
Message transfer was working, but it stopped after a change in network configuration.	Use network tools to test for network connectivity using the transport network protocol between the bridgehead servers in the sites. Change to a supported network protocol or reconfigure the network.

There are problems with mail delivery within a site.

Reasons	Actions
The MTA or information store is down.	Use a server monitor or Performance Monitor to determine if there is a problem. Check the Windows NT application event log on that server for the cause of the problem before trying to start the service.
A transport is not routed between servers on the LAN.	Install a network protocol that is routed within the LAN, change the network to route the common network protocol, or move all servers to the same LAN segment. The latter can reduce performance by increasing network traffic on that LAN segment.
The network is down between MTAs.	Start a link monitor to determine if the MTAs can communicate with each other on the network.

Directory

Changes to the directory are automatically replicated to all other servers in the site and can be replicated to all servers on the same physical network. This keeps directory information current. Directory problems are often related to servers that are not functioning correctly or to the network. Directory replication problems between sites are usually caused by connection or configuration errors.

Directory information isn't the same between servers in different sites.

Reasons	Actions
The directory has not yet been replicated.	Check the directory replication schedule. To initiate an update, use the Update Now button in the directory General property page. If the problem persists, increase diagnostics logging on the Replication Updates category of the directory, and then check the Windows NT application event log for errors.
Replication between sites has failed.	<p>Check the Windows NT application event log for replication failure messages. Check for directory consistency within the site.</p> <p>Use a server monitor and Performance Monitor to make sure servers in both sites are running normally. Track the replication messages between sites.</p>

Directory information isn't the same between servers within a site.

Reasons	Actions
Directory replication within a site has failed or is delayed.	Check the Windows NT application event log for replication failure messages. Use a server monitor and Performance Monitor to verify that servers in both sites are running normally.
The network is down between the servers.	Use the Ping or the Net Use command from one server to the other to see if they can communicate with each other on the network.

Directory Synchronization

Directory synchronization allows Microsoft Exchange Server to exchange directories with Microsoft Mail for PC and AppleTalk networks and other systems that support the Microsoft Mail directory synchronization protocol. The process relies on the Microsoft Mail Connector interchange, MS Mail (PC) MTA or MS Mail (AppleTalk) MTA, and the Microsoft Exchange Server MTA and directory, if used, to be functioning. Problems with directory synchronization can be in planning, messaging between the systems, or configuration problems in Microsoft Exchange Server, MS Mail (PC), or MS Mail (AppleTalk).

Duplicate display names appear for custom recipients and new Microsoft Exchange Server mailboxes.

Reasons	Actions
Migration of new accounts has created duplicate names. Both addresses are valid.	Either hide the Microsoft Exchange Server mailboxes from the Address Book or do not include Microsoft Mail addresses in directory synchronization.
Migration of new accounts has created duplicate names. Only Microsoft Exchange Server addresses are valid.	If migration is successful and all postoffice users were moved, remove the postoffice from directory synchronization.

You haven't received updates from MS Mail (PC).

Reasons	Actions
There is no message connectivity to the directory synchronization server.	Send a message to the directory synchronization postoffice from a Microsoft Exchange Server user, and reply when it is delivered. If delivery fails, treat this as a routing or connection problem.
Dispatch is not running on the postoffices.	Check the dispatch logs on the postoffices for reported successes and failures.
The configuration is incorrect.	Verify that the MS Mail (PC) directory synchronization server and requestor information is correct, including postoffice names, passwords, and types of addresses. Microsoft Exchange Server should show up as the Microsoft Mail Connector postoffice.

Updates for MS Mail (PC) are no longer being received.

Reasons	Actions
Mail is not getting through.	Check the queues on the connection and on the postoffices between the directory synchronization server and the requestors.
Dispatch is not running on the postoffices.	Look at the dispatch logs on the postoffices.
Configuration has been changed.	Check configuration with both Administrator programs for changes. Verify that network and postoffice names are accurate and that the requestor password is correct (if a password is being used). Verify that mail and replies to mail arrive as expected between Microsoft Exchange Server and the postoffice.

Updates for MS Mail (AppleTalk) are no longer being received.

Reasons	Actions
The directory exchange requestor does not run consistently.	Replace the MSMail GW file in the System Extension folder. If you are using Quarterdeck Mail 3.6 or later, contact Starnine for an updated file.
Mail is not being delivered.	Check the queues on both sides of the connection. Check the PCTOMAC and MACTOPC directories on the Microsoft Exchange Server. Verify that messages are queued and moved.
The directory synchronization custom recipient is not configured correctly.	The target recipient for Microsoft Exchange Server/Macintosh directory synchronization must be the network manager.
There is not enough memory on the directory exchange requestor.	Press COMMAND+I and increase the amount of available memory to the directory exchange requestor. Run the directory exchange requestor on another Macintosh® workstation.
The directory exchange requestor configuration is corrupted.	Delete the directory exchange requestor preferences file, and the log and input files. Restart the Macintosh and use the Chooser to establish the gateway with the Macintosh Mail server.

Internet Mail Service

The Internet Mail Service is fully integrated with Microsoft Exchange Server and Windows NT. You can troubleshoot problems with the tools used for other components. In addition, the Internet Mail Service can generate Simple Mail Transfer Protocol (SMTP) logs. For more information, see Chapter 4, “Troubleshooting Tools and Resources.”

If you are investigating an NDR, see “Non-Delivery Reports” later in this chapter.

If the problem is not solved by the actions suggested in this section, increase the diagnostics logging level to Maximum on all categories of the Internet Mail Service except Message Archival. Restart the Internet Mail Service, re-create the error, and then check the application event log and SMTP protocol logs.

The Internet Mail Service will not start.

Reasons	Actions
The Internet Mail Service was not configured.	Configure the Internet Mail Service. For more information, see <i>Microsoft Exchange Server Operations</i> .
Transmission Control Protocol/Internet Protocol (TCP/IP) is not installed.	Install TCP/IP from the Windows NT compact disc.
The delivery route of an e-mail domain cannot be resolved. At least one name in the E-Mail Domain box is incorrect.	Review the list in the E-Mail Domain box in the Internet Mail Service Connections property page. Correct misspelled domain names. If all domain names are correct, verify that they appear in the Domain Name System (DNS) or local Hosts file.
The domain name of the Internet Mail Service host is missing.	Add the host domain name to the DNS Configuration dialog box using the Network icon in Windows NT Control Panel.
A Messaging Application Programming Interface (MAPI) initialization error occurred.	Stop and restart all Microsoft Exchange Server services. Use the Services icon in Windows NT Control Panel. Select MSExchangeIMC and choose Startup . Verify that the entry in the Log on as box is the same as for other services. If the error is not resolved, remove and reinstall the Internet Mail Service.

No messages are being sent or received.

Reasons	Actions
An Internet Mail Service or the MTA on an Internet Mail Service's server is not running.	Use a server monitor or Performance Monitor to confirm that the services are operating. Restart if necessary.
The Internet Mail Service is configured for Flush Queue mode.	Change the Transfer Mode setting in the Internet Mail Service Connections property page.
The Internet Mail Service is not on the network.	Send a ping message to the Internet Mail Service host or perform a Telnet to port 25 to determine whether the connections are operational. If not, restore the network connection.
The Internet Mail Service is not started.	Start the Internet Mail Service from the command line or use the Services icon in Windows NT Control Panel.

You can't send outbound mail messages through the Internet Mail Service.

Reasons	Actions
The MTA is down.	Restart the MTA.
The address space is not configured.	Use the Internet Mail Service Address Space property page to complete the configuration of the Internet Mail Service.
The address space configuration is too limited.	Review the entry in the Internet Mail Service Address Space property page. Type an asterisk (*) in the Address column to have the MTA send all SMTP mail to the Internet Mail Service.
The MTA is returning the message.	Verify that the Internet Mail Service is configured to support the SMTP address space. In the Internet Mail Service Connections property page, choose E-Mail Domain . Type an asterisk (*) in the E-Mail Domain box so all SMTP traffic is routed through the Internet Mail Service.
The Internet Mail Service is configured for inbound traffic only.	Change the Transfer Mode setting in the Internet Mail Service Connections property page.
The address for the DNS server is incorrect.	Change the DNS server address using the Network icon in Windows NT Control Panel (DNS Configuration dialog box).
The domain address for Microsoft Exchange Server users is invalid.	Verify the SMTP site address in the Site Addressing property page.

You can't receive inbound mail messages through the Internet Mail Service.

Reasons	Actions
The recipient's address is incorrect.	In the E-mail Addresses property page for the recipient, verify the address.
The TCP/IP address on the Internet Mail Service does not match the values in the DNS, Hosts file, or Windows Internet Name Server (WINS) list.	<p>Verify that the Internet Protocol (IP) address and domain names match. If not, change either the DNS or the TCP/IP configuration.</p> <p>To check the IP address, use the Network icon in Windows NT Control Panel. Select TCP/IP Protocol in the Installed Network Software box, and choose Configure. Check the entry in the IP Address box.</p> <p>To check the domain name, use the Network icon in Windows NT Control Panel. Select TCP/IP Protocol in the Installed Network Software box, choose Configure, and then choose DNS. Check the entry in the Domain Name box.</p> <p>If using DNS, check for an mail exchanger (MX) record for the Microsoft Exchange Server site SMTP address.</p>
The transfer mode on the Internet Mail Service does not allow inbound connections.	Change the Transfer Mode in the Internet Mail Service Connections property page.
The Internet Mail Service is configured to reject connections from this host or all hosts.	Change the settings in the Accept or Reject by Host box of the Internet Mail Service Connections property page.
External SMTP hosts have an incorrect IP address for the Internet Mail Service server.	<p>Verify the address using the Network icon in Windows NT Control Panel TCP/IP Configuration dialog box.</p> <p>Verify the IP address published in DNS for the Internet Mail Service host.</p> <p>Verify that the domain is correct in the Site address property page in the Configurations container. The domain name can also be set by the Internet Wizard during Internet Mail Service installation.</p>
The domain is not set for inbound message transfer.	Use the Internet Mail Service Routing property page to add or change the domain for the inbound route.

You can't send mail to a user on the Internet.

Reasons	Actions
Mail does not arrive because either a server or the Internet Mail Service is down.	Use message tracking to locate the problem. For more information, see Chapter 4, "Troubleshooting Tools and Resources."
Mail is returned because the sender's address contains delivery restrictions that exclude the sender from using the Internet.	Change the delivery restrictions in the Internet Mail Service.
An address in the PAB is incorrect.	Use the client global address list to address mail.
Mail is returned as undeliverable.	Trace the message in the message tracking log. Verify that the address is correct.

Administrator program changes aren't taking effect.

Reason	Actions
All changes for the Internet Mail Service take effect only when the service is restarted.	Restart the Internet Mail Service. If the system is slow, the directory may not have updated the changes before the service was restarted. Wait a minute and restart it again.

Mail sent from Microsoft Exchange Server is received with garbled text or extra attachments.

Reason	Actions
The message was formatted with rich text and could not be resolved by the receiving system.	Remove the instruction to send the message in rich-text format. The rich-text format option can be changed in one of the following places: In the Internet Mail Service Internet Mail property page, choose Interoperability . Verify that Send Microsoft Exchange rich text formatting is not selected. In the custom recipient's Advanced property page, verify that Allow rich text in messages is not selected. In the sender's PAB, double-click the recipient's name, and then select the Address tab. Verify that Always send to this recipient in Microsoft Exchange rich-text format is not selected.

Microsoft Exchange Server Performance

Performance problems can occur if the server load is too heavy.

The hard disk is busy more than 90 percent of the time.

Reasons	Actions
There is not enough RAM; Windows NT is using virtual memory.	Use Performance Monitor to check pages/sec in the memory section. Increase RAM or decrease the load if necessary.
Public folders are busy.	Use Performance Monitor to determine the rate of open message and open folder operations. If necessary, move the public information store to another hard drive, increase the speed of the drive, or move key public folders to a server that is not being fully used.
Private folders are busy.	Check the rate of message submission and delivery. If necessary, move mailboxes to another hard drive, increase the speed of the drive, or move key users to other servers where recipients to whom they send or receive most of their mail reside.
The gateway or connector is constantly busy.	Use Performance Monitor to determine the rate of inbound and outbound messages and their size. If necessary, increase the speed of the hard drive, create a second gateway or connector on a second server to balance the load, or increase scheduled connection times to spread the load more evenly.

There is a slow response to client and Administrator program actions.

Reasons	Actions
There is not enough CPU power.	Use Performance Monitor to check CPU usage.
The network card is overloaded.	Use Performance Monitor to check the network interface for total bytes per second sent and received. Compare this with maximum tested throughput for the card.
The network is slow.	Use a network analyzer to check for network collisions and usage. Compare the current trace with the trace measured prior to installation of Microsoft Exchange Server.
The hard drive is too busy.	Add more hard drives to the RAID set, or add another drive and off-load some disk-intensive processes to it.
The Windows NT event log is large, adding time to every action that needs to be logged.	Set the event log to no larger than 5 megabytes (MB), and configure it to overwrite as needed.

Microsoft Exchange Server Setup

Setup copies files from the installation compact disc, configures services, creates registry entries, and starts the server's core services. Common problems are related to incorrectly preparing the server or service account before running Setup.

There is an error copying files.

Reasons	Actions
Other applications are using the files.	Close all other applications and run Setup again. If that fails, remove all programs from your Startup group, and restart the computer.
Windows NT Event Viewer displays the error "The system cannot find the file specified."	The ESE97 key in the registry was not created. Close all applications and run Setup again. If that fails, remove all programs from your Startup group, and then restart the computer.

You can't connect to an existing server in the site.

Reasons	Actions
The account running Setup does not have permissions for the other server.	Grant Administrator permissions for the other server to the person running Setup at the site and for configuration objects.
The two servers do not have RPC network connectivity.	Check for network problems. Install a common network protocol on both servers.

Services don't start after Setup is completed.

Reason	Action
There is not enough memory.	Use the System icon in Windows NT Control Panel to increase the virtual memory.

Microsoft Mail Connector

When a message is sent from an e-mail client, the route through which the message is transferred is selected by comparing the recipient address of the message with entries in the Microsoft Mail Connector **Address Space** property page.

Most problems in the Microsoft Mail Connector can be quickly traced using Windows NT Control Panel or the Microsoft Exchange Server Administrator program.

Mail isn't moving.

Reasons	Actions
The custom MS Mail (PC) message transfer agent (PCMTA) in the Services icon of Windows NT Control Panel has been started.	Disable PCMTA Performance Monitor in Windows NT Control Panel. Configure a named instance of the PCMTA in the Microsoft Mail Connector Connector MTAs property page and start it.
A custom PCMTA called PCMTA Performance Monitor is created at installation for performance monitoring. All functional PCMTAs are configured dynamically and assigned a user-defined name.	
The MTA instance service is not started.	Start the named instance of the MTA service in Windows NT Control Panel.
The MS Mail interchange service is not running.	Check the Windows NT event log for reported problems. Start the interchange service in Windows NT Control Panel.
There is no network access to postoffices.	Install the correct network protocol on the Microsoft Exchange Server, and check for connectivity.
You do not have permissions for the postoffice shares or volumes.	Have the administrator for those file servers grant Read, Write, and Delete permissions.
All licenses for the NetWare server are in use. No additional connections to the file server are permitted.	Try connecting to the file server with File Manager. If the server is overused, see your NetWare documentation for a solution.
The MS Mail (AppleTalk) message transfer agent (ATMTA) is spawning a 16-bit application. The NetWare redirector establishes unnecessary connections that use up NetWare postoffices.	Comment out the nw16 line in the Autoexec.nt file to disable the 16-bit NetWare redirector.
The connector mail database is corrupted.	Verify that all connector postoffice directories exist and their contents are intact.
The target postoffice mail database has become corrupted.	Verify that all target postoffice directories exist and their contents are intact. Check the Inqueue3.mbg mailbag. Make sure the file divides evenly by 116 (116 bytes per message header).
Messages are stalled in MS Mail queues.	Return or delete some of the oldest messages in the queue and test again. If you are unable to return or delete, the outbound mailbag may be failing.
An indirect routing connection is inoperative.	Verify that all routing is configured correctly. Check the integrity of the each inbound mailbag (Inqueue3.mbg). Verify the integrity of the mail database on each server along the route.

Some or all mail from MS Mail (PC) to Microsoft Exchange Server recipients is returned as non-deliverable.

Reasons	Actions
The address space is incorrect.	Check the addresses of the intended recipients against the address space for the connector.
The routing table was not rebuilt after the last changes.	In the MTA General property page, choose Recalculate Routing .

Mail arrives on MS Mail (PC) without OLE attachments.

Reason	Action
The interchange was not correctly configured.	Select the Maximize MS Mail (PC) Compatibility option in the MS Mail Connector Interchange property page.

Instances of the MS Mail (PC) MTA are trying to use the same modem.

Reasons	Actions
Both instances are using a modem script that specifies use of the same communications port.	Edit the modem script source file to change or remove the communications port setting. Recompile the source file into a new script file, and replace the old one with the new one.
Instances of the MS Mail (PC) MTA are configured to use the same communications port.	Combine instances or configure them to use different communications ports.

You can't install Macintosh Services for Windows NT.

Reason	Action
The hard drive where the connector postoffice is located is not formatted as a Windows NT file system (NTFS) volume.	Back up the drive; use the Windows NT Convert.exe program from the command prompt to update the drive format to NTFS.

You can't create an instance.

Reasons	Actions
An instance with the same name previously existed and was incorrectly removed.	If this occurs when you try to add the instance again, either use a different instance name or choose Apply three times and ignore the error messages.
You don't have permissions to create instances.	Check with the site administrator.

You are having trouble initializing a modem in the MS Mail (PC) MTA.

Reasons	Actions
There is a script problem.	For more information on script file modification and troubleshooting, see the <i>MS Mail for PC Networks Administrator's Guide</i> .
The modem cable doesn't support request to send (RTS) or clear to send (CTS) flow control.	Replace the modem cable with one that supports these pinouts.

Some files sent from the Macintosh don't arrive with an extension.

Reason	Action
The Mappings.txt file needs a new entry for this file type.	Use a Macintosh utility to find the file's creator and type. Edit the Mappings.txt file to map the creator and type to an extension.

Non-Delivery Reports

When Microsoft Exchange Server or a gateway is unable to deliver a mail message, it sends an NDR to the originator. The reason for the return is written below the recipients list in the report.

If the problem is not resolved, consult the Windows NT application event log, or create an SMTP log. For more information, see Chapter 4, "Troubleshooting Tools and Resources."

The recipient was not found.

Reasons	Actions
There is no such address in the network or in the domain of the gateway host.	Verify the address and the mapping of the address to a host.
The address was not unique.	Verify the address. Make sure that all addresses in your network are unique.
The address was a phrase in several addresses but not an entire address of any mailbox.	Have users press CTRL+K to verify the address before sending.

The host is unreachable.

Reasons	Actions
The receiving host is not operating.	Set up or consult a link monitor to verify that the receiving host is operational, and then retry.
There is no such host in the domain or the domain does not exist.	Check the IP address in the DNS table. Verify that all e-mail domain address names are spelled correctly in the DNS.

Arguments are missing.

Reason	Actions
The Internet Mail Service generated a protocol error.	<p>Check the Windows NT application event log for errors from MExchangeIMC.</p> <p>Create an SMTP log and look for the error. Error codes are explained in Requests for Comments (RFCs) 821, 822, and 1521. For more information, see Chapter 4, "Troubleshooting Tools and Resources."</p> <p>Track the message in the message tracking log.</p>

The time has expired.

Reason	Actions
The Internet Mail Service established a connection to an SMTP host, but the host did not respond to any communication. The time delay for retries exceeded the threshold set for the Internet Mail Service.	<p>Verify that the host is operational. If necessary, increase the message time-out threshold in the Internet Mail Service Connections property page.</p> <p>Run a Telnet to port 25. At the command prompt, type telnet hostname 25, and then type quit.</p>

Public Folders

Public folders are repositories of information that can be shared among users. These folders reside in the public information store on a Microsoft Exchange Server computer and can be replicated. When you make a change in a public folder, that change is copied to every replica of the folder that exists throughout the Microsoft Exchange Server organization.

Public folder problems are usually related to network connectivity, replication, or permissions.

You can't access a public folder.

Reasons	Actions
The server with the replica of the public folder is not running.	Determine the home server for the public folder, and verify that the server is running.
A replica of the public folder is on a server in a site that can't be reached by the client network protocol.	Determine what router, bridge, or gateway prevents the passage of the user's network protocol. Add the missing network protocol to the router, or add an acceptable network protocol to the user's computer.
A replica of the public folder is on a server in a site where affinities have not been established.	Use the information store site configuration Public Folder Affinity property page to establish affinities.
You do not have permissions to access the folder.	Use the e-mail client to grant permissions to access the public folder.
You lost the connection to the server.	Restart the client.

You can't view a public folder in the hierarchy.

Reasons	Actions
The public folder does not exist in your site or has not been replicated to your site.	Use the public information store Instances property page to add the public folder to the list to be replicated to this server.
No affinities were assigned to the public folder.	Use the information store site configuration Public Folder Affinity property page to establish affinities.
The public folder is replicated in the site, but directory replication has not occurred.	If the folder was just added to the site, check the public information store Replication Schedule property page for the next scheduled replication. If the folder is still not visible after replication, increase the diagnostics logging level of the Replication category group, and then check the Windows NT application event log for public folder replication errors.

You can't send mail to a public folder.

Reasons	Actions
The public folder is hidden from the Address Book.	Use the Administrator program to check the Hide From Address Book option in the public folder's Advanced property page.
The public folder does not have permission to create messages.	In the General property page of the public folder, choose Client Permissions , and then select Create Items .
Mail is returned because this user is excluded from sending to public folders.	Use the Administrator program to check the Reject Messages From option in the Delivery Restrictions property page.

Public folder replication isn't working.

Reasons	Actions
Mail between sites is not scheduled for this time.	Check the connection schedule. Send a test message to a mailbox or configure a link monitor.
Mail is not flowing between sites.	Treat this as a mail problem between sites. Check link monitors and queues. If necessary, track public folder replication messages.
Public folder replication is not scheduled for this time.	Check the public folder replication schedule.
The public information store or MTA on the source or destination server is not working.	Use a link monitor to check the MTA and the server; use Performance Monitor to check the public information store.

Internet News Service

The Internet News Service uses Network News Transfer Protocol (NNTP) to access Internet newsgroups. Microsoft Exchange Server replicates Internet newsgroups into public folders for viewing by e-mail clients. Most Internet newsgroup problems are related to insufficient disk space or Internet or network connectivity.

One or more Internet newsgroups are not replicated.

Reasons	Actions
The newsfeed host was not found.	Establish a connection to the newsfeed host. For more information, see <i>Microsoft Exchange Server Operations</i> . If Microsoft Exchange Server is already configured to receive a newsfeed from a specific host, use the Ping command to test the connection to that host.
Microsoft Exchange Server has insufficient disk space for storing Internet newsgroups.	Adjust the age limits and size warnings for Internet newsgroups in the Limits property page for the public information store. Set shorter age limits and smaller size warnings for folders that contain binary information, such as digitized images and sounds.

Sending Mail

Problems sending mail can usually be traced to a client, computer, server, or recipient. For example, if many users on different computers have the same problem, it is likely to be a server or recipient problem.

You can't connect to a server.

Reasons	Actions
The network connection to the server is down.	Use the Net View \\servername command from the command prompt, or use the RPC ping utility to test for network connectivity to the server. If the server is running and this test fails, there is a network problem.
You did not log on to a Windows NT security account that has Send Mail permission for this mailbox.	Use the Administrator program to determine which account has permissions for this mailbox. Log on again.
The profile is not configured correctly.	In Control Panel, use the Mail and Fax icon to check the profile's server name and mailbox name for the Microsoft Exchange Server information service.

You can't send to a recipient in a different site.

Reasons	Actions
The connection between sites is down.	Use link monitor logs to determine when the connection was last working. Use a server monitor to determine if all the services at both computers are working. Use the Administrator program or Performance Monitor to check the message queue lengths. For more information, see "Connections Between Microsoft Exchange Servers" earlier in this chapter.
The message tracking log on one of the servers has run out of disk space.	Use Performance Monitor to determine if the MTA is running. If not, check the available space on the disk where the tracking log is stored.
The private information store on one of the servers is not working.	Use Performance Monitor or a server monitor to determine if the service is running.
The recipient address is no longer valid because the recipient has moved to another recipient container or site.	Connect to a server in the other site and verify that the recipient still exists. Check for directory replication problems if this recipient modification is not a recent change.

You can't send to or receive from Internet Message Access Protocol, Version 4rev1 (IMAP4rev1) or Post Office Protocol (POP3) clients.

Reason	Actions
SMTP or the Internet Mail Service is not configured correctly.	<p>Verify the SMTP configuration.</p> <p>Verify that the Internet Mail Service is installed and running.</p> <p>Verify that rerouting is correctly configured to route mail outbound to the Internet or intranet.</p> <p>Check the IMAP4 or POP3 client installation to verify the correct values. For more information, see the documentation included with the IMAP4 or POP3 client software.</p>

You can't send to a user in the same site.

Reasons	Actions
The message tracking log on one of the servers has run out of disk space.	Check to see if the MTA is running on both servers. If not, check available disk space where the tracking log is stored.
The network connection between servers is down.	Use link monitor to determine when the connection was last working. Use a server monitor to determine if all the services at both computers are working. Use the Administrator program or Performance Monitor to check queue lengths.
The private information store, MTA, or directory on one of the servers is not working.	Use Performance Monitor or a server monitor to determine if the services are running.

You can't send to a user on the Internet.

Reasons	Actions
Mail does not arrive because either a server or the Internet Mail Service is down.	Use the Administrator program message tracking facility to locate the problem.
Mail is returned because the sender's address contains delivery restrictions that exclude the sender from using the Internet.	Change the delivery restrictions in the Internet Mail Service.

You can't send to a user on Microsoft Mail for AppleTalk Networks.

Reasons	Actions
The address space is defined incorrectly.	Follow the path (global routing report) and look for a circular route back to Microsoft Exchange Server.
The connector is down.	Use server monitor or Performance Monitor to determine the status. On an MS Mail (AppleTalk) system, use the Mail Network Administrator program to verify that all servers respond to a global response report, and check queues on all servers by using the Server Report command on the Global menu. Use the Windows NT Event Viewer to look for recent problems. Use message tracking to confirm that the message was delivered to the connector.

You can't send to a user on Microsoft Mail for PC Networks.

Reasons	Actions
The user has migrated to Microsoft Exchange Server, but the postoffice still exists.	Use the MS Mail (PC) Administrator program to see if the postoffice still exists.
Mail is returned as non-deliverable because of circular routing.	Use message tracking to follow the path of the message. Check the address space and routing definitions in each site and postoffice.
Mail is not moving in Microsoft Mail.	If link monitor sends to the destination postoffice, check the current status. Check queues in MS Mail (PC) and determine if the External program or the MS Mail (PC) MTA are running normally.
The Microsoft Mail Connector is not working.	Use server monitor or Performance Monitor to determine if the connector is running. Check the Windows NT application event log for errors. Use message tracking to trace the message to the connector.
The queue is too full.	Increase the blocking factor. Determine if the Mail directory is corrupted.

You can't send to a user on the same server.

Reasons	Actions
The message tracking log has run out of disk space.	Determine if the MTA is running. If not, check the available space on the disk where the tracking log is stored. The MTA is not needed for local delivery, but the message tracking log is.
The private information store or directory is not running.	Use server monitor or Performance Monitor to determine if the services are running.

Mail is late or is lost.

Reasons	Actions
The intermediate server or a component is down.	Track the message to its current location and troubleshoot from there. If the route taken seems unusual, there may be a problem along the route.
The connection between sites is too slow for traffic.	Use the Administrator program to check the queue size. Use Performance Monitor to compare that with the messages per second processed for that MTA.

X.400 Connections

Connecting to other X.400 systems must be done carefully. Configuration varies depending on which type of X.400 system you are connecting to and the method you use. Common problems are related to incorrect configuration.

An address is missing or incorrect.

Reasons	Actions
The address space is defined incorrectly.	Use the Administrator program to check address space definitions.
Custom recipients have incorrect e-mail names in Microsoft Exchange Server.	Create custom recipients with valid e-mail names or update the names of existing custom recipients.

Messages across an X.400 backbone lose rich text format.

Reason	Action
The Microsoft Exchange Server MTA is not configured to pass Transport-Neutral Encapsulation Format (TNEF) information.	Use the Administrator program to change the MTA configuration.

The Microsoft Exchange Server MTA can't connect to an X.400 MTA.

Reasons	Actions
You are using different network stacks.	Use a common stack.
The MTA name or password does not match the password used in the configuration.	Verify the MTA passwords and configuration. Passwords are usually case-sensitive.
The network connection is down.	Check the network connection. Find the network problem and fix it.

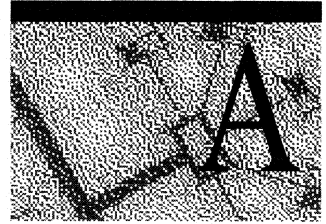
Unwanted binary attachments are being sent to an X.400 MTA.

Reason	Action
The Microsoft Exchange Server MTA is configured to pass TNEF information.	Disable TNEF in the X.400 Connector General property page.

Messaging fails when changing MTA conformance on X.400 Connectors.

Reason	Action
Messages are either returned as NDRs or are lost.	Verify that the MTA conformance option found in the X.400 Connector's Advanced property page matches what is used by the Microsoft Exchange Server or X.400 system at the other end of the connection. If a change is made, restart all the services on both servers. This will re-encode any messages in the queue waiting to be transmitted.

Diagnostics Logging



Diagnostics logging regulates the level of detail of events and information written to the Windows NT application event log by Microsoft Exchange Server services and components. Logging levels are set by category for each service and component.

Usually, the service name in the **Diagnostics Logging** property page corresponds to the source name in the event log as displayed by the Windows NT Event Viewer. Similarly, the categories in the **Diagnostics Logging** property page for each component match the categories of events as displayed in the Event Viewer.

As you adjust the logging levels for categories of a service, you can see the results in the application event log.

You can obtain diagnostics logging for the following services and components:

- Directory
- Directory synchronization
- Information store
- Internet Mail Service
- Key Management server (KM server)
- Message transfer agent (MTA)
- Microsoft Exchange Connector for Lotus cc:Mail
- Microsoft Mail Connector
- Microsoft Schedule+ Free/Busy Connector
- Internet Message Access Protocol, Version 4rev1 (IMAP4rev1)
- Network News Transfer Protocol (NNTP)
- Post Office Protocol version 3 (POP3)

Directory Service

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeDS	Knowledge Consistency Checker	Ensures that replication links between servers and sites are configured correctly.
MSExchangeDS	Security Events	Events related to Windows NT security, such as logon attempts and changing permissions on directory objects.
MSExchangeDS	EXDS Interface Events	Communication between the directory and the information store, MTA, and Administrator program.
MSExchangeDS	MAPI Interface Events	Communication between Messaging Application Programming Interface (MAPI) clients and the directory.
MSExchangeDS	Replication Events	Events related to replication of the directory to and from other Microsoft Exchange Server computers.
MSExchangeDS	Garbage Collection	Events generated when objects marked for deletion are deleted.
MSExchangeDS	Internal Configuration	Interpretation and display of the registry and configuration variables.
MSExchangeDS	Directory Access	Reads and writes directory objects from all sources.
MSExchangeDS	Internal Processing	Events related to the internal operation of directory application code. Error events in this category indicate bugs in the directory.
MSExchangeDS	LDAP Interface	Events related to clients accessing the directory using Lightweight Directory Access Protocol (LDAP). For example, Bind, Search, and Filter. It records what LDAP calls are made, whether calls succeed, and why a call failed.
MSExchangeDS	Initialization/Termination	Events related to starting and stopping the directory.
MSExchangeDS	Service Control	Processes Windows NT Control Panel services events, such as start service, stop service, and pause service.
MSExchangeDS	Name Resolution	Resolution of addresses and directory names.
MSExchangeDS	Backup	Events related to the backup and restoration of the directory database.
MSExchangeDS	Field Engineering	Internal debugging trace.
MSExchangeDS	Address Book Views	Events related to the Address Book views consistency checker, which ensures the validity of the entries in each Address Book view. It records information such as when the Address Book View containers were created and deleted.

Directory Synchronization

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeDX	MSExchangeDX	Events generated by directory synchronization with MS Mail.

Information Store

The diagnostics logging categories for the information store are organized into four groups: Internet Protocols, System, Public, and Private.

Diagnostics logging service	Diagnostics logging group	Diagnostics logging category	Description
MSExchangeIS	Internet Protocols/IMAP4rev1	Content Engine	Events related to converting messages from the database format of the information store to the formats required for IMAP4.
MSExchangeIS	Internet Protocols/IMAP4rev1	Connections	Events related to connecting and disconnecting e-mail clients.
MSExchangeIS	Internet Protocols/IMAP4rev1	Authentication	Events related to e-mail client logon and password authentication.
MSExchangeIS	Internet Protocols/IMAP4rev1	Client Actions	Events that log the IMAP4 commands issued by e-mail clients.
MSExchangeIS	Internet Protocols/IMAP4rev1	Configuration	Events related to configuration problems.
MSExchangeIS	Internet Protocols/NNTP	Content Engine	Events related to converting messages from the database format of the information store to the formats required for NNTP.
MSExchangeIS	Internet Protocols/NNTP	Internet News Service	Events related to retrieving and submitting articles to another NNTP server, usually an Internet service provider (ISP).
MSExchangeIS	Internet Protocols/NNTP	Connections	Events related to connecting and disconnecting NNTP clients.
MSExchangeIS	Internet Protocols/NNTP	Authentication	Events related to NNTP client logon and password authentication.
MSExchangeIS	Internet Protocols/NNTP	Client Actions	All actions of NNTP clients and NNTP inbound push newsfeeds.
MSExchangeIS	Internet Protocols/NNTP	Configuration	Events related to configuration problems.

(continued)

Diagnostics logging service	Diagnostics logging group	Diagnostics logging category	Description
MSExchangeIS	Internet Protocols/ NNTP	Replication	Events related to NNTP outbound push newsfeeds.
MSExchangeIS	Internet Protocols/ NNTP	NNTP Pull Newsfeed	Events related to NNTP inbound pull newsfeeds.
MSExchangeIS	Internet Protocols/ POP3	Content Engine	Events related to converting messages from the database format of the information store to the formats required for POP3.
MSExchangeIS	Internet Protocols/ POP3	Connections	Events related to connecting and disconnecting e-mail clients.
MSExchangeIS	Internet Protocols/ POP3	Authentication	Events related to e-mail client logon and password authentication.
MSExchangeIS	Internet Protocols/ POP3	Client Actions	Events that log the POP3 protocol commands issued by e-mail clients.
MSExchangeIS	Internet Protocols/ POP3	Configuration	Events related to configuration problems.
MSExchangeIS	System	Recovery	Events generated when the information store reads and verifies transaction log files when the information store is started.
MSExchangeIS	System	General	Miscellaneous system events.
MSExchangeIS	System	Connections	Attempts to establish connections, both successful and unsuccessful.
MSExchangeIS	System	Table Cache	Events related to the table cache.
MSExchangeIS	System	Content Engine	Events related to converting messages from the database format of the information store to the formats required for other services.
MSExchangeIS	System	Performance Monitor	Events related to Performance Monitor counters.
MSExchangeIS	System	Move Mailbox	Events related to moving mailboxes.
MSExchangeIS	System	Download	Events related to downloading mail or public folder contents to personal folder files.
MSExchangeIS	Public	Transport General	Miscellaneous events related to the transfer of messages to and from public folders.
MSExchangeIS	Public	General	Miscellaneous public information store events.

(continued)

Diagnostics logging service	Diagnostics logging group	Diagnostics logging category	Description
MSExchangeIS	Public	Replication DS Updates	Changes in replication configurations, including adding, deleting, and editing.
MSExchangeIS	Public	Replication Incoming Messages	Receipt of replication messages, including the numbers of updates.
MSExchangeIS	Public	Replication Outgoing Messages	Replication messages sent, including the number of updates.
MSExchangeIS	Public	Non-delivery Reports	Replication messages that could not be delivered.
MSExchangeIS	Public	Transport Sending	Sending messages according to public folder rules.
MSExchangeIS	Public	Transport Delivering	Delivery of messages to a public folder. The origin of the message can be a different information store.
MSExchangeIS	Public	Transfer Into Gateway	Receipt and delivery of mail to public folders from a gateway.
MSExchangeIS	Public	Transfer Out of Gateway	Sending mail from public folders to a gateway.
MSExchangeIS	Public	MTA Connections	Events related to establishing connections between the public information store and the MTA.
MSExchangeIS	Public	Logons	Successful and unsuccessful attempts to log on.
MSExchangeIS	Public	Access Control	Events related to assigning permissions.
MSExchangeIS	Public	Send On Behalf Of	Establishes rules directing public folders to send messages on behalf of a sender. These events can be used to trace security violations.
MSExchangeIS	Public	Send As	Establishes rules directing public folders to send messages with a different sender name. These events can be used to trace security violations.
MSExchangeIS	Public	Rule	Application of rules, including recognizing the situations where rules apply, applying them, and verifying the results.
MSExchangeIS	Public	Storage Limits	Reports when one or more public folders have exceeded their size limits. Storage limit events are reported during scheduled information store maintenance.

(continued)

Diagnostics logging service	Diagnostics logging group	Diagnostics logging category	Description
MSExchangeIS	Public	Replication Site Folders	Events related to the replication of site folders, including the offline Address Book and Microsoft Schedule+ free and busy times.
MSExchangeIS	Public	Replication Expiry	Events related to applying age limits.
MSExchangeIS	Public	Replication Conflicts	Events reported when two public folders attempt to update the same items simultaneously.
MSExchangeIS	Public	Replication Backfill	Events related to an information store requesting and receiving missed replication updates.
MSExchangeIS	Public	Background Cleanup	Events related to the background deletion of messages, folders, and attachments for public information stores.
MSExchangeIS	Public	Replication Errors	Unexpected replication errors.
MSExchangeIS	Public	IS/DS Synchronization	Events related to public information store and directory synchronization.
MSExchangeIS	Public	Views	Events related to caching public folder views.
MSExchangeIS	Public	Replication General	Miscellaneous events related to the replication of public folders.
MSExchangeIS	Public	Download	Events related to downloading public folder contents to personal folder files.
MSExchangeIS	Private	Transport General	Miscellaneous events related to the transfer of messages to and from private information stores.
MSExchangeIS	Private	General	Miscellaneous private information store events.
MSExchangeIS	Private	Transport Sending	Events related to sending messages.
MSExchangeIS	Private	Transport Delivering	Delivery of messages to a mailbox. The origin of the message can be a different information store.
MSExchangeIS	Private	Transfer Into Gateway	Receipt and delivery of mail to mailboxes from a gateway.
MSExchangeIS	Private	Transfer Out of Gateway	Sending mail from mailboxes to a gateway.
MSExchangeIS	Private	MTA Connections	Events related to establishing connections between the private information store and the MTA.

(continued)

Diagnostics logging service	Diagnostics logging group	Diagnostics logging category	Description
MSExchangeIS	Private	Logons	Successful and unsuccessful attempts to log on.
MSExchangeIS	Private	Access Control	Events related to applying permissions.
MSExchangeIS	Private	Send On Behalf Of	Events generated when users send messages on behalf of another user. These events can be used to trace security violations.
MSExchangeIS	Private	Send As	Events generated when users send messages with a different sender name. These events can be used to trace security violations.
MSExchangeIS	Private	Rule	Application of rules, including recognizing the situations where rules apply, applying them, and verifying the results.
MSExchangeIS	Private	Storage Limits	Reports when mailboxes have exceeded their size limits. Storage limit events are reported during scheduled information store maintenance.
MSExchangeIS	Private	Background Cleanup	Events related to the background deletion of messages, folders, and attachments for private information stores.
MSExchangeIS	Private	IS/DS Synchronization	Events related to the private information store and directory synchronization.
MSExchangeIS	Private	Views	Events related to caching mailbox folder views.
MSExchangeIS	Private	Download	Events related to downloading mail to personal folder files.

Critical Event Categories

Critical events generated by the information store are written to the Windows NT application event log regardless of the logging levels set for any category. These categories do not appear in the **Diagnostics Logging** property page, but they do appear in the event log.

Event Viewer source	Event Viewer category	Description
MSExchangeIS	None	Error events.
MSExchangeISPriv	DS/IS Consistency	Events generated when the DS/IS consistency adjustment utility runs on private information stores.
MSExchangeISPub	DS/IS Consistency	Events generated when the DS/IS consistency adjustment utility runs on public information stores.

Internet Mail Service

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeIMC	Initialization/ Termination	Events related to starting and stopping the Internet Mail Service.
MSExchangeIMC	Addressing	Address resolution, including directory searches and proxy generation.
MSExchangeIMC	Message Transfer	The movement of messages and message queue operation.
MSExchangeIMC	SMTP Interface Events	Interactions between Simple Mail Transfer Protocol (SMTP) hosts.
MSExchangeIMC	Internal Processing	Operation of the Internet Mail Service.
MSExchangeIMC	SMTP Protocol Log	Monitors SMTP connections. Setting the diagnostics logging level to Medium sends basic protocol information to text logs in ImcdData\Log. Setting it to Maximum sends entire unformatted packets to the same text logs.
MSExchangeIMC	Message Archival	Saves the text of messages. Setting the diagnostics logging level to Medium or Maximum writes each message to a file in ImcdData\In\Archive or ImcdData\Out\Archive.

KM Server

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeKM	None	Events generated by the KM server related to security, granting and revoking permissions, violations, and the internal operation of the KM server.

MTA

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeMTA	X.400 Service	X.400 protocol events, such as submission and delivery reports.
MSExchangeMTA	Resource	Events related to MTA resources.
MSExchangeMTA	Security	Events related to attempted security violations.
MSExchangeMTA	Interface	Communication among MTA components and between MTAs. Includes remote procedure call (RPC) use.
MSExchangeMTA	Field Engineering	Internal debugging trace.
MSExchangeMTA	MTA Administration	Administrator program access to MTA queues and routing information.
MSExchangeMTA	Configuration	Configuration of internal parameters and/or problems in one or more MTA configuration files.
MSExchangeMTA	Directory Access	Events related to the MTA's use of the directory.
MSExchangeMTA	Operating System	Events related to the MTA's use of Windows NT functions, such as thread creation and file operations.
MSExchangeMTA	Internal Processing	Events related to the internal operation of MTA application code. These events indicate serious problems in the MTA.
MSExchangeMTA	Interoperability	Tracks the binary content of protocol messages. Use this category and interface to log stack traces and X.400 application program interface (XAPI) traces to Mtadata\Ap*.log.
MSExchangeMTA	APDU (Application Protocol Data Unit)	Tracks complete P1 content (MTA send/receive) and fully encoded P1 APDU (communication between remote MTAs) to diagnose interoperability or conformance problems. Use this category and X.400 Service to log binary data to Mtadata\Bf*.log.

Microsoft Exchange Connector for Lotus cc:Mail

Diagnostics logging service	Diagnostics logging category	Description
MSEExchangeCCMC	General	Events, warnings, and errors related to general operating processes for the Microsoft Exchange Connector for Lotus cc:Mail.
MSEExchangeCCMC	Outbound	Events and errors related to messages sent outbound to Lotus cc:Mail.
MSEExchangeCCMC	Inbound	Events and errors related to messages sent inbound from Lotus cc:Mail.
MSEExchangeCCMC	NDR	Events and errors related to non-delivery reports (NDRs).
MSEExchangeCCMC	Dir Synch	Events related to directory synchronization.
MSEExchangeCCMC	MAPI	Warnings and errors related to MAPI communications with the information store.

Microsoft Mail Connector

The Microsoft Mail Connector uses the application name of the interchange, MExchangeMSMI, to represent the subcomponents of the service, including the interchange, the ATMTA, and all PCMTAs on a connector.

Diagnostics logging for the Microsoft Mail Connector is set by subcomponent, not by category. In the Event Viewer, the subcomponent name is the source of the service. Categories appear only in the Event Viewer.

Diagnostics logging service	Diagnostics logging category	Event Viewer source	Event Viewer category
MExchangeMSMI	MExchangeMSMI (Interchange)	MExchangeMSMI	Basic Session Debug Data Memory management Received NDR Routing Sent Session Data Session Error Session Warning
MExchangeMSMI	MExchangePCMTA	User name for PCMTA	Call in Call out Verbose Moved In Moved Out NDR Received Routing Sent Session Status
MExchangeMSMI	MExchangeATMTA	MExchangeATMTA	Debug NDR Message Received Message Sent Session Data Session Error Verbose Data

Microsoft Schedule+ Free/Busy Connector

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeFB	None	Events generated by the Microsoft Schedule+ Free/Busy Connector, including internal operations, messaging, and addressing.

IMAP4

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeIS	Content Engine	Events related to converting messages from the database format of the information store to the formats required for IMAP4.
MSExchangeIS	Connections	Events related to connecting and disconnecting e-mail clients.
MSExchangeIS	Authentication	Events related to e-mail client logon and password authentication.
MSExchangeIS	Client Actions	Events that log IMAP4 commands issued by e-mail clients.
MSExchangeIS	Configuration	Events related to configuration problems.

NNTP

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeIS	Content Engine	Events related to converting messages from the database format of the information store to the formats required for NNTP.
MSExchangeIS	Internet News Service	Events related to retrieving and submitting articles to another NNTP server, usually an ISP.
MSExchangeIS	Connections	Events related to connecting and disconnecting NNTP clients.
MSExchangeIS	Authentication	Events related to NNTP client logon and password authentication.
MSExchangeIS	Client Actions	All actions of NNTP clients and NNTP inbound push newfeeds.
MSExchangeIS	Configuration	Events related to configuration problems.
MSExchangeIS	Replication	Events related to NNTP outbound push newfeeds.
MSExchangeIS	NNTP Pull Newfeed	Events related to NNTP inbound pull newfeeds.

POP3

Diagnostics logging service	Diagnostics logging category	Description
MSExchangeIS	Content Engine	Events related to converting messages from the database format of the information store to the formats required for POP3.
MSExchangeIS	Connections	Events related to connecting and disconnecting e-mail clients.
MSExchangeIS	Authentication	Events related to e-mail client logon and password authentication.
MSExchangeIS	Client Actions	Events that log the POP3 protocol commands issued by clients.
MSExchangeIS	Configuration	Events related to configuration problems.

Index

\ (backslash) 47
 - (dash) 87
 / slash 87

A

Accessing public folders, problems 189
 Action levels 38
 Adding
 columns, information store status items 23
 services, monitoring 85
 Address Book
 addressing problems 169
 message tracking 128
 Address list, global, addressing problems 169
 Addresses
 incorrect 194
 missing 194
 spaces, problems 169, 184
 Addressing, troubleshooting 169
 Admin/t command 87
 Administrator program
 events 107
 troubleshooting 171, 179, 183
 Administrator window contents
 character sets 40
 options 39
 overview 38
 saving 39
 separators 40
 Administrators, training 6
 Advantages, backup routines 10
 Age limits, mailbox 36
 Alert
 durations, Link Monitor 52
 state
 Link Monitor 54
 Server Monitor 70
 Analysis, trend 3
 ANSI separator 40
 APDU logs, MTA 114
 Appletalk *See* Microsoft Mail (Appletalk)
 Archiving backups 12
 Arguments, missing 187
 Asn.1 envelope 114
 At.exe utility 14

ATMTA, diagnostics logging 120
 Attachments, problems 179, 184, 194
 Automatic
 rebuilding MTA routing table 21
 Windows NT Server logon 95
 Automating backup 14

B

Backslash (\) 47
 Backups
 archiving 12
 circular logging 9
 Copy option 12
 dedicated recovery systems 5
 devices 9
 differential 8, 10
 directory 8
 documenting 12
 full 9, 10
 incremental 8, 10
 information store 8
 overview 4, 7
 planning 8–12
 rotations 11
 routine 10
 servers
 automating 14
 command-line batch files 14
 offline, performing 14
 online, starting 13
 overview 12
 restoring servers 15–18
 starting services 19
 validating information store 15
 timely 11
 transaction log files 8
 validating 12
 verifying 12
 Batch files
 command-line, backup 14
 MIB installation 160
 Binary
 attachments, problems 194
 content, X.400 protocol messages 113

Body, message, returning 63
Boot environment 156
Bounce
 duration, defined 52
 messages, link status 63
Bridgehead servers, replication, MTA message queues 142
Browse button, problems 171
Busy hard disk 183

C

Cache, memory, write-ahead transaction log files 8
Catastrophe, restoring server after 18
Categories
 critical event, diagnostics logging 204
 defined 111
 information store events 115
cc:Mail, Microsoft Exchange Connector
 diagnostics logging 124, 206
 monitoring 94
Center, message tracking 131
Character sets, Administrator window contents 40
Chart file 101
Check mode 157
Checking tables 157
Circular logging 9
Cleaning mailboxes 35
Clients
 actions, slow response 183
 e-mail, troubleshooting 173, 184
 sending mail, problems 191
Clock
 synchronization
 server 81
 Server Monitor 78
 system 103
Columns
 information store status items 23
 separator 40, 47
 tracking log 138
Command-line
 batch files, backup 14
 options
 directory export 43
 directory import 45
 pausing monitors 87
Components
 diagnostics logging 108
 events 107
 information store events 115
 message tracking 126

Components (*continued*)
 Microsoft Exchange Server Computer, logging levels 125
 Microsoft Exchange Server, logging levels 109
 Microsoft Mail Connector, diagnostics logging 120
 Server Monitor, status 81
Confidential messages 37
Configuration
 backing up 12
 Link Monitor
 alert durations 52
 creating log files 51
 directory name 51
 display name 51
 foreign systems 62
 general properties 50–52
 link status 63
 mail messages 57
 maintenance status 66
 modifying notifications 59
 network alerts 58
 notification applications 55
 notification process 54–59
 outside organization 61
 outstanding notification 65
 overview 50
 permissions 52
 polling intervals 52
 removing notifications 59
 troubleshooting 103
 warning durations 52
 within organization 59
 preventing disasters 6
 Server Monitor
 clock synchronization 78
 component status 81
 creating log files 69
 directory name 69
 display name 69
 escalation actions 76
 general properties 69–70
 mail messages 73
 maintenance status 84
 modifying notifications 74
 network alerts 74
 notification 83
 notification applications 72
 notification process 70
 overview 68
 permissions 70
 polling intervals 70
 removing notifications 75

Configuration (*continued*)Server Monitor (*continued*)

- restart delay 77
- server clock synchronization 81
- server status 80, 105
- services, monitoring 84
- within organization 75

Connections

- information store events 115
- Link Monitor
 - logs 101
 - problems 101
 - status 100
- Microsoft Exchange Server, problems 175
- Microsoft Mail Connector, selecting queues 152
- servers, problems 171, 173, 184, 191
- X.400, troubleshooting 194

Connectors

- checking 101
- events 107
- Microsoft Exchange Connector for Lotus cc:Mail, diagnostics logging 124, 206
- Microsoft Exchange Server, logging levels 110
- Microsoft Mail Connector
 - diagnostics logging 120, 207
 - directory synchronization problems 177
 - enabling message tracking 127
 - monitoring 92
 - MTA message queues 142
 - overview 22
 - queues 151–154
 - troubleshooting 184
- Microsoft Schedule+ Free/Busy Connector, diagnostics logging 122, 206
- MTA routing table 20
- RAS, MTA message queues 142
- Site, MTA message queues 142
- X.400, MTA message queues 142

Consulting Service, Microsoft 166

Copy option, backups 12

Copying, files, errors 184

Correcting problems 3

Counters

- checking 101
- Microsoft Exchange Server Performance Monitor 89–94
- Windows NT Performance Monitor 88–94

Critical event categories, diagnostics logging 204

.csv files 38, 41, 47

Custom

- columns, information store status items 23
- recipients
 - mailbox cleaning 35
 - problems 177

D

Daily tracking logs 137

Dash (-) 87

Db*.dat file 154

Dedicated recovery systems 5

Delay, restart, Server Monitor 77

Deleted items

- restoring 18
- retention cleanup 31

Deleting

- expired items 31
- messages
 - action level 38
 - age limits 36
 - Internet Mail Service 149
 - Microsoft Mail Connector 154
 - MTA queues 145
 - other information 38
 - read levels 37

Designing

- preventing disasters 6
- system maintenance 1

Devices, backup 9, 12

Diagnosing problems 3

Diagnostics logging

- categories 111
- changing level 112
- critical event categories 204
- directory 35
- Directory Service 198
- directory synchronization 199
- IMAP4rev1 206
- information store 199
- information store events
 - changing level 116
 - overview 115
- Internet Mail Service
 - categories 204
 - changing level 118
 - overview 117
 - SMTP information 119

Diagnostics logging (*continued*)

- KM Server 205
- Microsoft Exchange Connector for Lotus cc:Mail 124, 206
- Microsoft Exchange Server
 - components 109
 - Computer 124
 - connectors 110
- Microsoft Mail Connector
 - categories 207
 - changing level 122
 - overview 120
- Microsoft Schedule+ Free/Busy Connector 122, 206
- MTA
 - APDU logs 114
 - categories 205
 - changing level 112, 113
 - interoperability logs 113
 - Windows NT Event Log 21
- multiple servers 110
- NNTP 197, 207
- overview 108, 197
- POP3 207
- property page 111

Differential backups 8, 10

Directory

- command-line options 45
- consistency 34
- diagnostics logging 35
- events 107
- export
 - command-line options 43
 - overview 41, 42
 - separators 47
- import
 - events 107
 - overview 41, 44
 - separators 47
- monitoring 90
- names
 - Link Monitor 51
 - Server Monitor 69
- offline backup, performing 14
- online backup, starting 13
- overview 33
- replication
 - problems 176
 - resynchronizing information 35
 - verifying consistency 34
- restoring from offline backup 18
- resynchronizing replicated information 35

Directory (*continued*)

- synchronization
 - diagnostics logging 199
 - events 107
 - Microsoft Mail, offline backup, performing 14
 - troubleshooting 177
- transaction log files 8
- troubleshooting 176
- Directory Service, diagnostics logging 198
- Disadvantages, backup routines 10
- Disaster recovery
 - dedicated recovery systems 5
 - design to prevent 6
 - overview 4
 - performing backups 4
 - planning 4
 - recovery toolkit 6
 - training administrators 6
- Display
 - Link Monitor 100
 - message tracking detail 130
 - names
 - Link Monitor 51
 - problems 177
 - Server Monitor 69
 - Server Monitor 105
 - tracking logs 137
- Distribution lists
 - mailbox cleaning 35
 - removing recipients 171
- Documentation
 - additional 165
 - Microsoft Exchange Server
 - conventions xiii
 - online xi
 - overview xi–xiii
- Documenting backups 12
- Dr. Watson 165
- Drive, tape, backing up to 12
- DS/IS consistency adjustment tool 18

E

- E-mail clients, problems 173, 184
- Enabling message tracking
 - information store 126
 - Internet Mail Service 127
 - Microsoft Mail Connector 127
 - MTAs 126
 - overview 126
- Envelope, Asn.1 114

Environment, boot 156
Erasing *See* Deleting
Escalation
 actions 76
 path 54, 71
Evaluating
 historical trends 3
 organizational needs 3
Event Log *See* Windows NT, Event Log
Event Viewer *See* Windows NT, Event Viewer
Events
 critical, diagnostics logging 204
 defined 108
 diagnostics logging categories 111
 information store
 changing logging level 116
 overview 115
 logs
 changing level 112
 searching 108
 troubleshooting 101
 message tracking 132
 numbers, tracking log 139
 tracking log 139
Exchange Server *See* Microsoft Exchange Server
Expired
 items, deleting 31
 time, NDRs 187
Export, directory
 command-line options 43
 overview 41, 42
 separators 47
Extensions, file, none 184
Extra attachments 179

F

Fault tolerance, write-ahead transaction log files 8
Fields, tracking log 138
Files
 .csv 38, 41, 47
 .pma 97
 Administrator window contents 39
 batch, MIB installation 160
 chart 101
 command-line batch, backup 14
 Db*.dat 154
 errors copying 184
 extensions, none 184
 headers 41

Files (*continued*)

 Link Monitor log 51, 101
 Mibcc.exe 160
 Perf2mib.exe 160
 Server Monitor log 69
 transaction log 8
Fix mode 157
Folders, public
 deleting expired indexes 31
 information store
 overview 22
 replication, viewing status 27
 viewing resources 28
 viewing server replication status 29
 mailbox cleaning 35
 replication, information store events 115
 restoring information store to different servers 17
 troubleshooting 189
 validating information store backups 15
Forcing retry, Internet Mail Service 150
Foreign systems
 Link Monitor 62
 ping messages 103
Formats, message ID 136
Free/Busy Connector *See* Microsoft Schedule+ Free/Busy
 Connector
FTP site 166
Full backups 9, 10

G

Gateways
 checking 101
 MTA routing table 20
 MTA, logs 113
General properties
 Link Monitor 50–52
 Server Monitor 69–70
Global address list, addressing problems 169
Globally unique identifier (GUID), information store 158
GUID, information store 158

H

Hard disk, busy 183
Headers, export and import files 41

Historical

tracking

Link Monitor 57

Server Monitor 73

trends, evaluating 3

Hosts, NDRs 187

I

ID

event 108

message

MTACHECK 156

tracking by 136

IMAP4rev1

diagnostics logging 206

problems 191

Implementation, backup plan 8–12

Import, directory

command-line options 45

events 107

overview 41, 44

separators 47

Incremental backups 8, 10

Indexes, folder, deleting expired 31

Information store

deleted items, restoring 18

diagnostics logging 199

different server, restoring to 17

enabling message tracking 126

events 107, 115, 116

ISINTEG

checking tables 157

overview 157

patching 158

maintenance schedule 31

monitoring 91

MTS-IN queue 147

MTS-OUT queue 147

offline backup, performing 14

offline backup, restoring from 18

online backup, starting 13

overview 22

same server, restoring to 16

status information

modifying columns 23

overview 22

viewing folder replication status 27

viewing logons 24

viewing mailbox resources 25

viewing public folder resources 28

viewing server replication status 29

Information store (*continued*)

transaction log files 8

validating backups 15

Information Store Integrity Checker *See* ISINTEG

Initializing modems, problems 184

Instances, problems 184

Interchange *See* Microsoft Mail Interchange

Interface logs, MTA 113

Internal clock 78

Internet File Transfer Protocol (FTP) Site 166

Internet Mail Service

diagnostics logging

categories 204

changing level 118

overview 117

SMTP information 119

enabling message tracking 127

events 107

monitoring 92

MTA message queues 142

object IDs 162

queues

deleting messages 149

forcing retry 150

overview 146

refreshing property page 149

selecting 147

viewing message detail 148

troubleshooting 179

Internet Message Access Protocol, Version 4rev1 *See*

IMAP4rev1

Internet News Service, troubleshooting 191

Internet protocols

See also specific protocols

diagnostics logging 199

Interoperability logs, MTA 113

Intervals, polling

Link Monitor 52

Server Monitor 70

Invalid addresses, addressing problems 169

IS Maintenance 31

ISINTEG

checking tables 157

overview 157

patching 18, 158

K

- Key Management Server *See* KM Server
- KM Server
 - diagnostics logging 205
 - offline backup, performing 14
- Knowledge Base, Microsoft 166

L

- LANs
 - Link Monitor 58
 - Server Monitor 75
- Late mail 191
- Link Monitor
 - configuration
 - alert durations 52
 - creating log files 51
 - directory name 51
 - display name 51
 - foreign systems 62
 - general properties 50–52
 - link status 63
 - mail messages 57
 - maintenance status 66
 - modifying notifications 59
 - network alerts 58
 - notification applications 55
 - notification process 54–59
 - outside organization 61
 - outstanding notification 65
 - overview 50
 - permissions 52
 - polling intervals 52
 - removing notifications 59
 - warning durations 52
 - within organization 59
 - connection problems 101
 - connection status 100
 - interpreting display 100
 - logs 101
 - overview 49, 99
 - ping messages
 - defined 49
 - display 100
 - nonreturning 101
 - notification process 54
 - outside organization 61
 - source 103
 - warning and alert durations 53
 - within organization 59
 - starting automatically 96
- Link Monitor (*continued*)
 - starting, manual 86
 - stopping, manual 86
 - troubleshooting 103
- Link status 63
- Lists, distribution
 - mailbox cleaning 35
 - removing recipients 171
- Log files
 - Link Monitor 51
 - Server Monitor 69
 - transaction 8
- Logging levels
 - categories 111
 - information store events
 - changing 116
 - overview 115
- Internet Mail Service 118
- Microsoft Exchange Server
 - components 109
 - Computer 125
 - connectors 110
- Microsoft Mail Connector 122
- Microsoft Schedule+ Free/Busy Connector 123
- MTA
 - APDU logs 114
 - changing 113
 - interoperability logs 113
 - Windows NT application event log 112
- Logging, circular 9
- Logging, diagnostics *See* Diagnostics logging
- LogicalDisk object 89
- Logons
 - information store 24
 - Windows NT Server, automatically 95
- Logs
 - Link Monitor 101
 - message
 - MTACHECK 156
 - tracking *See* Message tracking
 - MTA, interoperability 113
 - Server Monitor 106
 - tracking 137
- Lost mail 191
- Lotus cc:Mail, Microsoft Exchange Connector
 - diagnostics logging 124, 206
 - monitoring 94

M

Macintosh Services, problems 184

MADMAN MIB 159

Mail

See also Messages

between sites, problems 175

bounce, viewing details 64

Internet Mail Service

diagnostics logging 117–120, 204

enabling message tracking 127

events 107

monitoring 92

MTA message queues 142

object IDs 162

queues 146–150, 151–154

troubleshooting 179

late 191

Link Monitor 57

lost

See also Message tracking

troubleshooting 191

message queues 141

Microsoft Exchange Connector for Lotus cc:Mail,

monitoring 94

Microsoft Mail (Appletalk), directory synchronization

problems 177

Microsoft Mail (PC), directory synchronization

problems 177

Microsoft Mail Connector

diagnostics logging 207

enabling message tracking 127

monitoring 92

moving, problems 184

MTA message queues 142

receiving, problems 171, 179

sending, problems 171, 179, 189, 191

Server Monitor 73

user, problems 173

within site, problems 175

Mail Connector *See* Microsoft Mail Connector

Mailboxes

duplicate display names 177

information store

overview 22

viewing resources 25

maintenance

action level 38

age limits 36

deleting information 38

overview 35

read levels 37

sensitivity levels 37

restoring deleted items 18

Mailboxes (*continued*)

restoring information store to different servers 17

validating information store backups 15

Maintenance status

Link Monitor 66

Server Monitor 84

Maintenance, system

Administrator window contents

character sets 40

options 39

overview 38

saving 39

separators 40

backup

archiving 12

automating 14

circular logging 9

command-line batch files 14

Copy option 12

devices 9

documenting 12

offline, performing 14

online, starting 13

overview 7

planning 8–12

restoring servers 15–18

routine 10

servers 12–15

starting services 19

timely 11

transaction log files 8

validating 12

validating information store 15

verifying 12

concepts, overview 1

correcting problems 3

designing 1

diagnosing problems 3

directory

consistency 34

diagnostics logging 35

overview 33

resynchronizing replicated information 35

directory export

command-line options 43

overview 41, 42

separators 47

directory import

command-line options 45

overview 41, 44

separators 47

Maintenance, system *(continued)*

- disaster recovery
 - dedicated recovery systems 5
 - design to prevent 6
 - overview 4
 - performing backups 4
 - planning 4
 - recovery toolkit 6
 - training administrators 6

- evaluating organizational needs 3

information store

- maintenance schedule 31
- overview 22
- status information 22–29

mailboxes

- action level 38
- age limits 36
- deleting information 38
- overview 35
- read levels 37
- sensitivity levels 37

Microsoft Mail Connector 22**MTA**

- diagnostics logging 21
- messages 21
- overview 19
- queues 21
- routing table 20

overview 1, 7**performance, monitoring 2****performing, overview 2****planning 2****restore 7****trend analysis 3****Management Information Base** *See* MIB**Manual**

- rebuilding MTA routing table 20
- starting monitors 86

Maps

- message routing 165
- network, Link Monitor display 100
- topology, network 165

MCS 166**Media, backup 9, 12****Memory**

- cache, write-ahead transaction log files 8
- object 89

Message tracking**enabling**

- information store 126
- Internet Mail Service 127

Message tracking *(continued)***enabling** *(continued)*

- Microsoft Mail Connector 127

MTAs 126**overview 126****follow-up 137****overview 125****performing**

- displaying detail 130
- interpreting 137
- message ID 136
- message tracking center 131
- Microsoft Exchange Server messages 132
- outside organization 133
- overview 128
- starting 129

starting 129**tracking log**

- interpreting events 139
- interpreting fields 138
- overview 137

Messages

- action level 38
- body, returning 63
- deleting other information 38
- information store events 115
- logs, MTACHECK 156
- mail

Link Monitor 57**Server Monitor 73****mailbox age limits 36****Microsoft Mail Connector 22****MTA 21****ping****defined 49****Link Monitor display 100****nonreturning 101****notification process 54****outside organization 61****source 103****warning and alert durations 53****within organization 59****queues****Internet Mail Service 146–150****Microsoft Mail Connector 151–154****MTA 21, 142–145****overview 141****read levels 37****receiving, problems 179****routing maps 165****sending, problems 179**

Messages (*continued*)

- sensitivity levels 37
- SMTP archive 117, 120
- test 101
- tracking *See* Message tracking
- X.400
 - problems 194
 - protocol 113

MIB

- installation 160
- Internet Mail Service object ID 162
- MADMAN 159
- MTA Connections object ID 162
- MTA object ID 161
- snmputil utility 162
- viewing 161
- Windows NT Performance Monitor Counters 163

Mibcc.exe 160

Microsoft Certified Professionals 166

Microsoft Consulting Service (MCS) 166

Microsoft Exchange Connector for Lotus cc:Mail

- diagnostics logging 124, 206
- monitoring 94

Microsoft Exchange Server

- components, logging levels 109
- connection problems 175
- connectors, logging levels 110
- directory synchronization problems 177
- documentation
 - conventions xiii
 - online xi
 - overview xi–xiii
- message tracking 132
- MIB installation 160
- object IDs 161
- Performance Monitor counters 89–94
- performance, troubleshooting 183
- Setup, troubleshooting 184
- version 4.0 .csv files 47
- Web site 166

Microsoft Exchange Server Computer

- diagnostics logging 124

Microsoft Internet File Transfer Protocol (FTP) site 166

Microsoft Knowledge Base 166

Microsoft Mail (Appletalk)

- MTA, diagnostics logging 120
- problems 177, 191

Microsoft Mail (PC)

- directory synchronization problems 177
- MTA, diagnostics logging 120
- non-deliverable mail, problems 184
- problems 191

Microsoft Mail Connector

- diagnostics logging 120, 122, 207
- directory synchronization problems 177
- enabling message tracking 127
- monitoring 92
- MTA message queues 142
- overview 22
- queues
 - deleting messages 154
 - overview 151
 - refreshing queue 153
 - returning messages 153
 - selecting 152
- troubleshooting 184

Microsoft Mail Interchange, diagnostics logging 120

Microsoft Mail, directory synchronization, offline backup, performing 14

Microsoft Schedule+ Free/Busy Connector, diagnostics logging 122, 206

Microsoft Support Partners 166

Microsoft TechNet subscription service 166

Microsoft Technical Support 166

Modems, problems 184

Monitors

- defined 49
- directory 90
- information store 91
- Internet Mail Service 92
- Link Monitor *See* Link Monitor
- Microsoft Exchange Connector for Lotus cc:Mail 94
- Microsoft Mail Connector 92
- MTA 90
- Performance Monitor *See* Windows NT Performance Monitor
- performance, overview 2
- Server Monitor *See* Server Monitor
- SNMP monitoring agents
 - MIB installation 160
 - MIB viewing 161
 - overview 159
 - Windows NT Performance Monitor Counters 89
- startup, manual 86
- Windows NT Performance Monitor *See* Windows NT Performance Monitor

Moving, columns, information store status items 23

MSExchangeCCMC object 94

MSExchangeDS object 90

MSExchangeIMC object 92

MSExchangeISPriv object 91

MSExchangeISPub object 91

MSExchangeMSMI object 92

- MSExchangeMTA Connections object 90
 - MSExchangeMTA object 90
 - MSExchangePCMTA object 92
 - MSMI, diagnostics logging 120
 - MTA
 - connection problems 194
 - connections object ID 162
 - diagnostics logging
 - APDU logs 114
 - categories 205
 - changing level 113
 - interoperability logs 113
 - overview 21, 112
 - directory synchronization problems 177
 - enabling message tracking 126
 - events 107
 - messages 21
 - Microsoft Mail (Appletalk), diagnostics logging 120
 - Microsoft Mail (PC), diagnostics logging 120
 - monitoring 90
 - MTACHECK
 - interpreting output 155
 - overview 154
 - running 155
 - searching message logs 156
 - object ID 161
 - overview 19
 - problems 184
 - queues
 - changing message order 144
 - deleting messages 145
 - overview 21, 142
 - problems 175
 - refreshing property page 144
 - secured 142, 144
 - unsecured 142, 144
 - viewing message detail 143
 - routing table
 - overview 20
 - rebuilding 21
 - MTACHECK
 - interpreting output 155
 - overview 154
 - running 155
 - searching message logs 156
 - MTS-IN queue 147
 - MTS-OUT queue 147
 - Multiple
 - connections
 - Internet Mail Service, diagnostics logging 117–120
 - problems 101
 - mailboxes, cleaning 35
 - Multiple (*continued*)
 - PCMTAs 121
 - servers, logging levels 110
 - Multivalued properties, quoting behavior 47
- ## N
- Names
 - directory
 - Link Monitor 51
 - Server Monitor 69
 - display
 - Link Monitor 51
 - problems 177
 - Server Monitor 69
 - Link Monitor log file 101
 - MTA interoperability logs 113
 - server, restoring information store 17
 - NDRs
 - addressing problems 169
 - Link Monitor 61
 - non-existent recipients 49
 - troubleshooting 187
 - Needs, organizational, evaluating 3
 - Netstat 165
 - Network
 - alerts
 - Link Monitor 58
 - Server Monitor 74
 - map, Link Monitor display 100
 - topology maps 165
 - Network Analyzer 165
 - Network News Transfer Protocol *See* NNTP
 - Newsgroups, replication, problems 191
 - NNTP, diagnostics logging 197, 207
 - Non-deliverable mail, problems 184
 - Non-delivery reports *See* NDRs
 - Non-existent recipients 49, 61
 - Normal
 - backups 10
 - messages 37
 - Notifications
 - Link Monitor
 - applications 55
 - mail messages 57
 - modifying 59
 - network alerts 58
 - outstanding 65
 - overview 54
 - removing 59

Notifications (*continued*)

Server Monitor

- applications 72
- escalation actions 76
- mail messages 73
- modifying 74
- network alerts 74
- overview 70
- removing 75
- server 83

Numbers, event, tracking log 139

O

Object IDs, Microsoft Exchange Server 161

Objects, modification problems 171

Offline backup

- performing 14
- restoring from 18

OLE attachments, problems 184

Online backup, starting 13

Opening servers, problems 171

Order, message, MTA queues 144

Organization

Link Monitor

- outside 61
- within 59

message tracking, outside 133

Server Monitor, within 75

Organizational needs, evaluating 3

Outstanding notification, Link Monitor 65

P

PAB

- addressing problems 169
- message tracking 128

Pager programs, notification applications

- Link Monitor 55
- Server Monitor 72

Parameters, command-line batch files, backup 14

Patch mode 157, 158

Paths

- escalation 54, 71
- Link Monitor log file 101

Pausing monitors 87

PCMTA, diagnostics logging 120

Perf2mib.exe 160

Performance

- APDU logs affect on 114
- information store maintenance schedule 31
- Microsoft Exchange Server, troubleshooting 183
- monitoring, overview 2
- write-ahead transaction log files 8

Performance Monitor *See* Windows NT, Performance Monitor

Performing

- backups 4
- message tracking 128
- system maintenance 2
- timely backups 11
- trend analysis 3

Permissions

- Link Monitor 52
- Server Monitor 70

Personal

- address book (PAB), message tracking 128
- messages 37

PING 165

Ping messages

- defined 49
- Link Monitor display 100
- nonreturning 101
- notification process 54
- outside organization 61
- source 103
- warning and alert durations 53
- within organization 59

Ping-1 165

Pipes, names 175

Planning

- backup 8–12
- disaster recovery 4
- system maintenance 2

.pma file 97

Polling intervals

- Link Monitor 52
- Server Monitor 70

POP3

- diagnostics logging 207
- problems 191

Port 25, Telnet to 165

Prevention, disaster recovery 6

Priority, message, MTA queues 144

Private information store

- diagnostics logging 199
- events
 - changing logging level 116
 - list of 107
 - overview 115

Private information store (*continued*)

ISINTEG

checking tables 157

overview 157

patching 158

offline backup, performing 14

overview 22

restoring deleted items 18

restoring to different server 17

restoring to same server 16

status information

modifying columns 23

overview 22

viewing logons 24

viewing mailbox resources 25

viewing server replication status 29

Private messages 37

Problems

See also troubleshooting, specific problems

connection, Link Monitor 101

correcting 3

diagnosing 3

Process object 89

Processor object 89

Property separator 40, 47

Protocol logs, SMTP 117

Public folders

deleting expired indexes 31

information store

overview 22

replication, viewing status 27

viewing resources 28

viewing server replication status 29

mailbox cleaning 35

replication, information store events 115

restoring information store to different servers 17

troubleshooting 189

validating information store backups 15

Public information store

diagnostics logging 199

events

changing logging level 116

list of 107

overview 115

ISINTEG

checking tables 157

overview 157

patching 158

offline backup, performing 14

overview 22

restoring to different server 17

restoring to same server 16

Public information store (*continued*)

status information

modifying columns 23

overview 22

viewing folder replication status 27

viewing logons 24

viewing public folder resources 28

PView 165

Q

Queues

message

Internet Mail Service 146–150

Microsoft Mail Connector 151–154

MTA 142–145

overview 141

MTA 21, 175

MTACHECK

interpreting output 155

overview 154

running 155

searching message logs 156

troubleshooting 101

Quote separator 40, 47

Quoting behavior 47

R

RawMode option 46

Read levels, messages 37

Rebuilding MTA routing table 21

Recipients

addressing problems 169

custom

mailbox cleaning 35

problems 177

NDRs 187

non-existent 49, 61

removing, problems 171

sending mail, problems 191

Reconstruction, database, transaction log files 8

Recovering

MTACHECK removed objects 154

Recovery, disaster

dedicated recovery systems 5

design to prevent 6

overview 4

performing backups 4

planning 4

recovery toolkit 6

training administrators 6

Redirector object 89

Refresh

- information store 22

- Internet Mail Service property page 149

- Microsoft Mail Connector queue 153

- MTA message queues property page 144

Registry *See* Windows NT, Registry

Remote procedure calls *See* RPCs

Removing

- columns, information store status items 23

- notifications

 - Link Monitor 59

 - Server Monitor 75

- recipients, problems 171

- servers from Link Monitor 60, 76

- services, monitoring 85

Repairs, pausing monitors 87

Replication

- bridgehead servers, MTA message queues 142

- directory

 - problems 176

 - resynchronizing information 35

 - verifying consistency 34

- folder, viewing status 27

- newsgroups, problems 191

- public folder, information store events 115

- public folders, problems 189

- server, viewing status 29

Reports, non-delivery *See* NDRs

Requirements, dedicated recovery systems 5

Resources, additional 165, 166

Response, slow 183

Restart delay, Server Monitor 77

Restoring servers

- after catastrophe 18

- data for user 18

- from offline backup 18

- information store to different server 17

- information store to same server 16

- overview 7, 15

Results, message tracking 137

Resynchronizing replicated directory information 35

Retention period, deleted items 18

Retry, forcing, Internet Mail Service 150

Returning messages, Microsoft Mail Connector 153

RFC 1566 159

Rich text format, problems 194

Rotations, backup 11

Routines, backup 10

Routing

- messages, maps 165

- table, MTA

 - overview 20

 - rebuilding 21

Roving users, Link Monitor 57

RPC Ping 165

RPCs 67

Running

- ISINTEG 157

- MTACHECK 155

S

Saving Administrator window contents 39

Schedule+ Free/Busy Connector *See* Microsoft Schedule+ Free/Busy Connector

Scheduling

- backup, command-line batch files 14

- directory consistency 34

- information store maintenance 31

Searching

- messages *See* Message tracking

- MTACHECK message logs 156

Secured queues, MTA 142, 144

Security, events 107

Sensitivity levels, messages 37

Separators

- Administrator window contents 40

- directory import and export 47

- embedded 47

Sequential transaction log file 8

Server Monitor

- configuration

 - clock synchronization 78

 - component status 81

 - creating log files 69

 - directory name 69

 - display name 69

 - escalation actions 76

 - general properties 69–70

 - mail messages 73

 - maintenance status 84

 - modifying notifications 74

 - network alerts 74

 - notification 83

 - notification applications 72

 - notification process 70

 - overview 68

 - permissions 70

 - polling intervals 70

 - removing notifications 75

 - restart delay 77

 - server clock synchronization 81

 - server status 80

 - services, monitoring 84

 - within organization 75

- Server Monitor (*continued*)
 - interpreting display 105
 - logs 106
 - overview 67, 104
 - server status 105
 - starting automatically 96
 - starting, manual 86
 - stopping, manual 86
- Servers
 - See also* KM Server
 - backup
 - automating 14
 - command-line batch files 14
 - offline, performing 14
 - online, starting 13
 - overview 12
 - restoring 15–18
 - starting services 19
 - validating information store 15
 - components, events 107
 - connection problems 171, 173, 184, 191
 - dedicated recovery systems 5
 - design to prevent disasters 6
 - KM, diagnostics logging 205
 - Link Monitor *See* Link Monitor
 - message tracking 128
 - Microsoft Exchange Server Computer, diagnostics
 - logging 124
 - MTA message queues 142
 - opening problems 171
 - replication, viewing status 29
 - restoring
 - after catastrophe 18
 - data for user 18
 - from offline backup 18
 - information store to different server 17
 - information store to same server 16
 - overview 15
 - same, problems 191
 - sending mail, problems 191
 - Server Monitor *See* Server Monitor
 - viewing problems 171
 - within site, directory information problems 176
- Services
 - events 107
 - problems starting 184
 - Server Monitor, monitoring 84
 - starting with Backup program 19
- Settings, backing up 12
- Setup, Microsoft Exchange Server *See* Microsoft Exchange Server, Setup
- Shutdown, monitors, manual 86
- Simple Network Management Protocol *See* SNMP
- Single mailboxes, cleaning 35
- Sites
 - connection problems 184
 - connectors, MTA message queues 142
 - different
 - addressing problems 169
 - directory information problems 176
 - mail problems 175
 - recipients, problems 191
 - online backup, starting 13
 - same
 - addressing problems 169
 - mail problems 175
 - server directory information problems 176
 - users, problems 191
 - viewing problems 171
- Size, log files 8
- slash (/) 87
- SMTP
 - message archive 117, 120
 - protocol logs
 - interpreting 119
 - logging information 119
 - overview 117
- SNMP monitoring agents
 - MIB
 - installation 160
 - overview 159
 - viewing 161
 - overview 159
 - Windows NT Performance Monitor counters 89
- Snmputil utility 162
- Starting
 - Internet Mail Service, problems 179
 - Link Monitor 96, 103
 - message tracking 129
 - Server Monitor 96
 - services with Backup program 19
 - services, problems 184
 - Windows NT Performance Monitor
 - automatically 97
- Startup
 - Link Monitor 96
 - monitors, manual 86
 - Server Monitor 96
 - Windows NT Performance Monitor 97
- Status
 - information, information store
 - modifying columns 23
 - overview 22
 - viewing folder replication status 27

Status (*continued*)

- information, information store (*continued*)
 - viewing logons 24
 - viewing mailbox resources 25
 - viewing public folder resources 28
 - viewing server replication status 29

- link 63

- maintenance, Link Monitor 66

Stopping monitors, manual 86

Storage devices, backup 9, 12

Store, information

- diagnostics logging 199
- enabling message tracking 126
- events
 - changing logging level 116
 - list of 107
 - overview 115

ISINTEG

- checking tables 157
- overview 157
- patching 158

maintenance schedule 31

monitoring 91

MTS-IN queue 147

MTS-OUT queue 147

offline backup, performing 14

online backup, starting 13

overview 22

restoring

- deleted items 18
- different server, to 17
- offline backup, from 18
- same server, to 16

status information

- modifying columns 23
- overview 22
- viewing folder replication status 27
- viewing logons 24
- viewing mailbox resources 25
- viewing public folder resources 28
- viewing server replication status 29

transaction log files 8

validating backups 15

Subcomponents

information store events 115

Microsoft Exchange Server Computer, logging levels 125

Microsoft Mail Connector, diagnostics logging 120

Subjects, returning 63

Subscription service, Microsoft TechNet 166

Support, Technical, Microsoft 166

Synchronization

- clock, Server Monitor 78
- directory *See* Directory, synchronization

System

- attendant, events 107
- clock 103
- information store, diagnostics logging 199

System maintenance

Administrator window contents

- character sets 40
- options 39
- overview 38
- saving 39
- separators 40

backup

- archiving 12
- automating 14
- circular logging 9
- command-line batch files 14
- Copy option 12
- devices 9
- documenting 12
- offline, performing 14
- online, starting 13
- overview 7
- planning 8–12
- restoring servers 15–18
- routine 10
- servers 12–15
- starting services 19
- timely 11
- transaction log files 8
- validating 12
- validating information store 15
- verifying 12

concepts, overview 1

correcting problems 3

designing 1

diagnosing problems 3

directory

- consistency 34
- diagnostics logging 35
- overview 33
- resynchronizing replicated information 35

directory export

- command-line options 43
- overview 41, 42
- separators 47

directory import

- command-line options 45
- overview 41, 44
- separators 47

System maintenance (*continued*)

- disaster recovery
 - dedicated recovery systems 5
 - design to prevent 6
 - overview 4
 - performing backups 4
 - planning 4
 - recovery toolkit 6
 - training administrators 6
- evaluating organizational needs 3
- information store
 - maintenance schedule 31
 - overview 22
 - status information 22–29
- mailboxes
 - action level 38
 - age limits 36
 - deleting information 38
 - overview 35
 - read levels 37
 - sensitivity levels 37
- Microsoft Mail Connector 22
- MTA
 - diagnostics logging 21
 - messages 21
 - overview 19
 - queues 21
 - routing table 20
- overview 1, 7
- performance, monitoring 2
- performing, overview 2
- planning 2
- restore 7
- trend analysis 3

T

- Tables, checking 157
- Tape drive, backing up to 12
- Tasks, system maintenance 2
- TechNet, Microsoft 166
- Technical Support, Microsoft 166
- Telnet to Port 25 165
- Test messages 101
- Text
 - garbled 179
 - logs, MTA 113
- Time zones, clock synchronization 79
- Time, expired, NDRs 187
- Timely backups 11
- Toolkit, recovery 6

- Tools, additional 165
- Topology maps, network 165
- Tracing messages *See* Message tracking
- Tracking log
 - interpreting events 139
 - interpreting fields 138
 - overview 137
- Tracking, historical
 - Link Monitor 57
 - Server Monitor 73
- Tracking, message *See* Message tracking
- Training administrators, disaster recovery 6
- Transaction log files 8
- Trend analysis 3
- Troubleshooting
 - addressing 169
 - Administrator program 171, 179, 183
 - clients 173
 - directory replication 176
 - directory synchronization 177
 - Internet Mail Service 179
 - Internet News Service 191
 - Microsoft Exchange Server connections 175
 - Microsoft Exchange Server performance 183
 - Microsoft Exchange Server Setup 184
 - Microsoft Mail Connector 184
 - NDRs 187
 - public folders 189
 - utilities 154–159
 - X.400 connections 194

U

- Unicode separator 40
- Unread messages, deleting 37
- Unsecured queues, MTA 142, 144
- Updates
 - Microsoft Mail (Appletalk), problems 177
 - Microsoft Mail (PC), problems 177
- Users
 - mail, problems 173
 - problems 191
 - restoring data 18
 - roving, Link Monitor 57
 - sending mail to, problems 179
- Utilities
 - ISINTEG 157–159
 - MTACHECK 154–157
 - snmputil 162

V

Validating backups 12, 15

Verifying

- backups 12
- directory consistency 34

Viewing

- bounce mail details 64
- folder replication status 27
- information store logons 24
- Internet Mail Service message detail 148
- mailbox resources, information store 25
- maintenance status details 67
- MTA message queues, message detail 143
- public folder resources 28
- public folders, problems 189
- server replication status 29
- servers, problems 171
- sites, problems 171

W

Warning

- durations, Link Monitor 52
- state

 Link Monitor 54

 Server Monitor 70

Web site, Microsoft Exchange Server 166

Window, Link Monitor 103

Windows NT

 accounts

 Link Monitor permissions 52

 Server Monitor 70

 application event log, changing level 112

 Backup

 overview 7

 planning 8–12

 starting services with 19

 Control Panel 165

 Diagnostics 165

 Event Log 21, 35

 Event Viewer

 Link Monitor 101

 overview 107

 General Performance Monitor counters 89

 Macintosh Services, problems 184

 Performance Monitor

 chart file 101

 counters 88–94, 163

 overview 88, 106

 starting automatically 97

 trend analysis, overview 3

Registry

Windows NT (*continued*)

 Performance Monitor (*continued*)

 backing up 11

 ISINTEG 158

 Server

 automatic logon 95

 backup 12–15

 MIB installation 160

 services, monitoring 84

 SNMP monitoring agent 160

 Server Manager 101, 165

Write-ahead transaction log files 8

X

X.400

 connectors, MTA message queues 142

 protocol messages, text log 113

 service, APDU logs 114