Operations

Microsoft Exchange Server

Version 5.5

Microsoft Corporation

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. 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.

© 1997 Microsoft Corporation. All rights reserved.

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

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

Macintosh is a registered trademark of Apple Computer, Inc.

All other companies and product names are trademarks or registered trademarks of their respective holders.

Document No. X03-40140

Printed in Ireland 03

Contents

Before You Begin xxv
Microsoft Exchange Server Documentation xxv
About This Guide xxvii
Document Conventions xxvii

PART 1 Customizing Microsoft Exchange Server Features 1

Chapter 1 Distribution Lists and Custom Recipients 3
Distribution Lists 3
Creating Distribution Lists 3
General Properties for a Distribution List 4
Entering New Distribution List Name Information 5
Specifying an Expansion Server 5
Adding Members to a Distribution List 5
Adding an Owner to a Distribution List 6
Removing Members from a Distribution List 6
Deleting an Owner from a Distribution List 6
Advanced Properties for a Distribution List 6
Changing the Simple Display Name 7
Setting a Limit for Message Transfer 7
Setting the Distribution List Options 8
Setting a Trust Level for Directory Synchronization 8
Custom Recipients 9
Creating Custom Recipients 9
General Properties for a Custom Recipient 9
Entering User Name Information 10
Entering Address Information 11
Entering Company Information 11
Creating or Modifying a Custom Recipient's E-mail Address 11
Advanced Properties for a Custom Recipient 12
Specifying On-Line Listings Information for Microsoft NetMeeting 13
Setting a Message Size Limit 13
Allowing Rich Text in Messages 14
Hiding a Recipient from the Address Book 14
Organization Information for a Custom Recipient 14
Phone Numbers for a Custom Recipient 15

Common Properties for Recipients 16
E-mail Addresses for Recipients 16
Distribution List Membership for Recipients 16
Adding Recipients to a Distribution List 17
Removing Recipients from a Distribution List 17
Delivery Restrictions for Recipients 17
Accepting or Rejecting Messages from Specific Senders 18
Delivery Options for Recipients 19
Specifying an Alternate Recipient for Incoming Messages 20
Specifying Who Can Send Messages on Behalf of a Recipient 21
Custom Attributes for Recipients 21
Renaming the Custom Attribute Fields 22

Chapter 2 Address Books 23
Understanding Address Book Views 23
Creating Address Book Views 24
General Properties 26
Defining the Directory and Display Name 26
Group By Properties 26
Setting Group By Values 27
Configuring Address Book Views 27
Permissions 28
Restricting Address Book Views 28
Restricting Access to Offline Address Book Views 28
Advanced Properties 29
Promoting Entries in the Address Book 30
Showing Views in the Address Book 31
Removing Empty Containers 31
Working with Address Book Views 31
Moving Recipient Objects Between Address Book View Containers 32
Adding a New Item to an Address Book View Container 32
Customizing an Address Book View Hierarchy 32
Changing the Address Book View Display Name 33
Exporting Recipients from Address Book View Containers 33
Restricting Address Book Views for Anonymous Users 33
Deleting an Address Book View 34
Setting Up Large Address Book Views 34
Details Templates 35
Changing Template Display Names 36
Selecting Template Help Files 37

Template Modification 37
Creating a New Template Control 38
Editing or Removing a Template Control 38
Changing the Order of Template Controls 39
Testing the Appearance of a Template 39
Reverting to Original Template Settings 39
One-off Address Templates 39
Foreign Language Details and Addressing Templates 40
Installing a Template on a Microsoft Exchange Server Computer 41

Chapter 3 Advanced Security 43
KM Server Installation 44
KM Server Configuration 44
Starting the KM Server 45
Advanced Security Configuration 45
Administrators Properties 47
Adding and Removing Advanced Security Administrators 48
Changing Your Advanced Security Administrator Password 48
Passwords Properties 49
Setting Multiple Administrator Passwords 50
Enrollment Properties 51
Transmitting Temporary Keys to Users 52
Editing the Enrollment Welcome Message 52
Enabling Advanced Security for Users in Bulk 53
Issuing Certificates for Compatibility 54
Certificate Trust List 55
Importing Certificates 56
Untrusting and Removing Certificates 57
Viewing Certificates 58
General Properties 59
Defining the Display Name 60
CA Permissions 60
Site Security 60
General Properties for the Site 62
Defining the Display Name 62
Choosing a Site 62
Site Permissions 63
Algorithms 63
Selecting an Encryption Algorithm 64
Selecting a Preferred Security Message Format 65

Mailbox Security Tasks 65
Enabling Advanced Security for a Mailbox 66
Revoking Advanced Security for a Mailbox 68
Recovering Advanced Security Keys 69
Viewing Mailbox Security Information 69
Additional Advanced Security Tasks 70
Enabling Additional Sites to Use the KM Server 70
Enabling Security for Users in Remote Sites 72
Backing Up and Restoring Advanced Security Data 72
Viewing the Security Log 73
Moving Users from One KM Server to Another 73
Moving the KM Server from One Site to Another 74

PART 2 Setting Up Connectors 77

Chapter 4 Address Spaces 79
Address Space Configuration 79
Address Space General Properties 80
X.400 Address Spaces 80
Internet (SMTP) Address Spaces 81
Microsoft Mail Address Spaces 82
Other Address Spaces 83
Restrictions Properties 84

Chapter 5 Internet Mail Service 87
Before You Begin 87
Installing the Internet Mail Service 88
Installing and Configuring TCP/IP 88
Adding the Internet Mail Service Computer to DNS 89
Updating the Hosts File When Not Using DNS 90
Testing the Connection 90
Customizing the Internet Mail Service 91
Internet Mail Properties 92
Assigning an Administrator's Mailbox 92
Setting Up Non-Delivery Report (NDR) Notifications 92
Specifying the Default Attachment Content Format 93
Specifying the Default Character Sets 94
Enabling Rich Text for Outbound Messages 95
Disabling Out-Of-Office Responses 96
Disabling Automatic Replies to the Internet 96
Disabling Display Names for Outbound Messages 96

Specifying Message Content by E-mail Domain 97
Specifying a Fixed-width Font 98
Disabling Client S/MIME Support 98
Connections Properties 99
Specifying Inbound and Outbound Transfer Modes 100
Defining the Maximum Number of Connections and Messages Sent 100
Delivering Messages Using DNS 101
Delivering All Messages to a Single Host 102
Delivering Messages by E-mail Domain 102
Accepting Connections from All Hosts 103
Accepting Connections from Secure Hosts 103
Accepting Connections from Specific Hosts 104
Setting the Retry Interval 105
Specifying Message Time-out Values 105
Controlling Notifications for Queued Mail 106
Connected Sites Properties 107
Creating a New Connected Site 107
Specifying the Routing Address for Connected Sites 107
Address Spaces 109
Specifying an Address Space 110
Using Routing Addresses for Address Space Entries 110
Delivery Restrictions 111
Accepting or Rejecting Messages from Specific Senders 111
General Properties 112
Specifying the Maximum Message Size 112
Permissions 113
Queues Properties 113
Diagnostics Logging Properties 113
Dial-up Connections Properties 114
Viewing and Modifying the Available Connections 114
Adding Connections 115
Specifying Mail Retrieval Options 115
Specifying a Time-out Period 116
Specifying Logon Information 117
Setting a Schedule 117
Routing Properties 118
Choosing a Routing Method 120
Specifying Routing Destinations 120
Adding Routing Addresses 121

Modifying a Routing Address 121
Removing a Routing Address 121
Using a Custom Routing Program 122
Security Properties 122
Enabling Security for Outbound Connections 122
MIME Types 123
Internet Mail Service and Macintosh File Attachments 123
Adding Additional Internet Mail Services 123
Removing the Internet Mail Service 124
Advanced Internet Mail Service Configuration 125
Reverse Resolution 125
Disabling Reverse Resolution 126
User Name Resolution 126
Disabling User Name Resolution 126
Enabling Loopback Detection 127
Verify Request (VRFY) 127
Enabling VRFY 128
Disabling Text Quoting 128
Message Tracking on the Internet Mail Service 129
How a Message is Tracked 129
ESMTP Support 130
How ESMTP Works 130
Disabling ETRN Support 131
Disabling ESMTP Support 132

Chapter 6 Site Connector and Dynamic RAS Connector 133
Site Connector 133
Site Connector Installation 134
Site Connector Configuration 134
General Properties 135
Specifying the Connector Name 136
Assigning a Routing Cost 136
Setting a Messaging Bridgehead Server in the Local Site 136
Address Space Properties 137
Defining Address Spaces 137
Assigning an Address Space Cost 137
Target Servers Properties 138
Adding and Removing Target Servers 139
Assigning a Target Server Cost 139
Override Properties 140

Connecting Using a Different Account 140
Dynamic RAS Connector 141
MTA Transport Stack Installation 141
General Properties 143
Permissions 144
Defined RAS Connectors 144
Dynamic RAS Connector Installation 145
Dynamic RAS Connector Configuration 145
General Properties 147
Specifying the Connector Name 147
Specifying the Name of the Remote Server 147
Specifying the MTA Transport Stack 147
Specifying the Phone Book Entry 148
Specifying the Message Size 148
Schedule Properties 149
Setting a Schedule for the Dynamic RAS Connector 150
RAS Override Properties 150
Setting RAS Override Properties 151
Setting RAS Phone Numbers 152
MTA Override Properties 152
Setting Override RTS Values 153
Setting Override Connection Retry Values 153
Setting Override Association Parameters 154
Setting Override Transfer Time-outs 154
Resetting Override Default Values 155
Delivery Restrictions 155
Accepting or Rejecting Messages from Specific Senders 156
Address Space Properties 157
Defining Address Spaces 158
Assigning an Address Space Cost 158
Connected Sites 158
Adding or Changing Connected Sites 159
Assigning the Routing Address and Cost for an Indirectly Connected Site 160
Removing a Connected Site 161
Permissions 161

Chapter 7 X.400 Connector 163
MTA Transport Stack 164
MTA Transport Stack Installation 165
Installing a TCP/IP MTA Transport Stack 166
Installing an X.25 MTA Transport Stack 167
Installing a TP4 MTA Transport Stack 168
Using the MTA Transport Stack Permissions Property Page 169
Using the MTA Transport Stack Connectors Property Page 169
X.400 Connector 171
Adding an X.400 Connector 173
General Properties 173
Specifying the Connector Name 174
Adding or Modifying the Remote MTA Name and Password 174
Specifying the Remote MTA Transport Stack 175
Configuring Message Text Word-wrap 175
Enabling Rich Text for MAPI Client Recipients 176
Schedule Properties 177
Setting the Connection Schedule 178
Stack Properties 178
Connecting to a Site or Foreign System Using TCP/IP 179
Connecting to a Site or Foreign System Using X.25 180
Connecting to a Site or Foreign System Using TP4 182
Override Properties 183
Overriding the Local MTA Name and Password 184
Setting Override RTS Values 185
Setting Override Connection Retry Values 186
Setting Override Association Parameters 186
Setting Override Transfer Timeouts 187
Resetting Override Default Values 187
Address Space Properties 187
Specifying the X.400 Connector Address Space 189
Connected Sites 189
Adding or Changing a Connected Site 189
Removing Connected Sites 190
Assigning the Routing Address and Cost for a Connected Site 190
Delivery Restrictions 192
Accepting or Rejecting Messages from Specific Senders 193
Advanced Properties 194
Configuring MTA Conformance 195

Specifying X.400 Body Parts 195
Specifying X.400 Link Options 196
Setting the Message Size 196
Configuring the Remote Global Domain Identifier 197
Permissions 197
Foreign X.400 System Configuration 197
Testing X.400 Connections to Foreign Sites 198
Testing Connections to Another Site 199
Removing X.400 Connectors 200

Chapter 8 Microsoft Exchange Connector for Lotus cc:Mail 201
Lotus cc:Mail Requirements 201
Connector Installation 202
Connector Setup 202
Quick Start 202
Connector for Lotus cc:Mail Configuration 204
Post Office 205
Assigning an Administrator's Mailbox 205
Specifying the Connected cc:Mail Post Office 206
Specifying Versions of Import/Export 206
Specifying a Post Office Language 207
Configuring Other Post Office Options 207
General Properties 208
Specifying Message Size Limits 209
Export Containers 209
Selecting Export Containers 210
Removing Export Containers 211
Import Container 211
Selecting an Import Container 213
Configuring the Import Container Filter 214
Running Directory Synchronization 214
Setting Alias and Display Name Rules for Directory Import 215
Directory Synchronization Schedule 216
Setting the Directory Exchange Server Schedule 217
Address Space 218
Configuring the Address Space 219
Removing an Address Space 219
Modifying the Address Generator Format 220
Connector for cc:Mail Queues 221
Viewing Message Queue Details 222

Refreshing the Queues Property Page 222
Deleting Messages 222
Diagnostics Logging 222
Setting up Diagnostics Logging 223
Delivery Restrictions Properties 223
Connecting to a Post Office on a Novell NetWare Server 224
Test the Connection 225
Testing from the Microsoft Exchange Server 225
Testing from a cc:Mail Client 226
How the Connector Manages Attached Objects 227
Sending Attachments 227
Sending Shortcuts and Links 227
Moving the Connector for cc:Mail 228
Relocating the Connector for cc:Mail 228
Relocating a Connector to Another Site 229
Relocating a Connector Within a Site 229
Relocating the Import Container Within a Site 230
Public Folders and cc:Mail Bulletin Boards 230
Modifying E-mail Addresses 231
Propagating Messages Between cc:Mail Bulletin Boards and Public Folders 231
Propagating Public Folder Messages into cc:Mail Bulletin Boards 232

Chapter 9 Microsoft Mail for AppleTalk Networks 235
Microsoft Mail Connector Requirements 236
Microsoft Exchange Connection Requirements 237
Microsoft Mail Connector Setup 237
Quick Start 238
Macintosh-Accessible Volume 238
Creating a Macintosh-Accessible Volume 239
Setting Permissions for a Volume 240
Microsoft Mail Connector Interchange 241
Assigning an Administrator's Mailbox 242
Enabling Message Tracking 243
Setting Up the Microsoft Mail Connector (AppleTalk) MTA 243
Local Postoffice Properties 244
Modifying Local Postoffice Name and Password 245
Connections Properties 247
Viewing the MS Mail (AppleTalk) Message Queue 248
General Properties 249

Defining Message Size Limits 250
Address Space Properties 250
Defining Additional Addressing and Routing Information 252
Editing an Address Space 253
Removing an Address Space 253
Diagnostics Logging 253
Setting Up Connector Diagnostic Logging 254
Microsoft Exchange Connection Setup 254
Connecting to the Microsoft Mail Connector Postoffice 255
Installing Microsoft Exchange Connection Files 257
Installing the Microsoft Exchange Connection Gateway 257
Microsoft Exchange Connection Configuration 259
Specifying the Postoffice Location 259
Setting Gateway Options 261
Setting the Gateway Connection Times 262
Access Connection Gateway Installation 263
Extracting the Access Connection Gateway 263
Installing the Access Connection Gateway 264
Microsoft Mail for AppleTalk Networks Connection Gateway 265
Installing Microsoft Mail for AppleTalk Networks Connection Gateway 266
Microsoft Exchange Server and Quarterdeck Mail Server Connections 266
Installing the Macproxy.dll 267
Test the Connections 268
Sending Messages from the Microsoft Exchange Server Computer 268
Using the MS Mail (AppleTalk) Client 268

Chapter 10 Microsoft Mail for PC Networks 271

Microsoft Mail Connector Setup 272
Quick Start 273
Microsoft Mail Connector Configuration 274
Interchange Properties 275
Assigning an Administrator's Mailbox 275
Specifying the Primary Language for Clients 276
Configuring MS Mail 3.*x* Client Compatibility 277
Enabling Message Tracking 277
General Properties 277
Defining the Computer Name 278
Specifying Message Size Limits 279
LAN Connection to MS Mail 279
LAN Connection Setup 279

Creating a LAN Connection 280
Confirming Connection Changes 281
Removing Connections 282
MTA Configuration for a LAN-Connected Postoffice 282
Setting Up a Microsoft Mail Connector (PC) MTA for LAN Connections 284
Configuring Connector (PC) MTA Options 286
Removing a Connector MTA Service 288
Setting Up Service to LAN-Connected Postoffices 288
Setting LAN Postoffice MTA Options 289
MS Mail (PC) Postoffice Configuration 290
Modifying Local Postoffice Properties 291
Test the Connection 293
Using the MS Mail (PC) Client 293
Diagnostics Logging 294
Setting Up Diagnostics Logging 294
Asynchronous and X.25 MS Mail Postoffice Connections 295
Asynchronous and X.25 Setup 295
Setting Up an Asynchronous or X.25 Connection 296
Setting Options for an Asynchronous or X.25 Connection 298
Asynchronous and X.25 MTA Configuration 299
Asynchronous and X.25 MTA Services 299
Setting Up an MTA for an Asynchronous Connection 301
Setting Up an MTA for an X.25 Connection 302
Modifying an MTA for an X.25 Connection 303
MS Mail (PC) Postoffice Configuration 304
Testing an Asynchronous or X.25 Connection 304
Indirect Connections to MS Mail Postoffices 305
Indirect Connection Setup 305
Uploading Indirect Routing Information 305
Manually Creating Indirect Routing Information 307
Testing an Indirect Connection 308
MS Mail Gateway on Microsoft Exchange Server 308
MS Mail Gateway on the Connector Postoffice 308
Installing an MS Mail (PC) Gateway 309
Viewing the Gateway Postoffice Queue 310
MS Mail (PC) Gateway Access Component 311
Installing a Gateway Access Component 311
Microsoft Mail Connector (PC) Address Space 312

Address Space Configuration 312
Configuring Address Spaces for Foreign Systems 314
Modifying the Address Space 315
Removing an Address Space Listing 315

Chapter 11 Directory Synchronization for Microsoft Mail 317
Dirsync Requestor Installation 319
General Dirsync Requestor Properties 322
Setting General Requestor Properties 322
Import Container Properties 324
Selecting a Requestor Import Container 324
Export Container Properties 325
Selecting Requestor Export Containers 326
Removing Export Containers 326
Settings Properties 327
Configuring Dirsync Requestor Settings 328
Schedule Properties 329
Setting the Requestor Schedule 330
Configuring an MS Mail Directory Server 330
Dirsync Server Installation 331
General Dirsync Server Properties 332
Setting General Dirsync Server Properties 333
Schedule Properties 334
Setting the Directory Exchange Server Schedule 334
Remote Dirsync Requestor Installation 335
General Remote Dirsync Requestor Properties 336
Setting General Remote Dirsync Requestor Properties 337
Import Container Properties 339
Selecting a Remote Dirsync Requestor Import Container 340
Export Container Properties 341
Selecting Remote Dirsync Requestor Export Containers 342
Removing Export Containers 342
Permissions Properties 343
Remote Directory Requestor Configuration 343
MS Mail 3.*x* Directory Synchronization Requestor Setup 343
MS Mail (AppleTalk) Directory Exchange Requestor Setup 344
Directory Exchange Requestor 345
Configuring Requestor Settings 346
Selecting a Gateway 348
Setting Address Filters 349

Starting the Directory Exchange Requestor 350
Making the Directory Exchange Requestor a Startup Item 351
Viewing Directory Synchronization Updates 351
Importing Address Changes Manually 351
Exporting Address Changes Manually 352
Exporting a World List to a Text File Manually 352
Removing MS Mail (AppleTalk) Addresses 353
Removing Microsoft Exchange Server Addresses 354
Resynchronizing Address Information 354
Foreign Directory Exchange Requestors 355
Directory Synchronization Configuration 355
General Properties 356
E-mail Addresses for Directory Synchronization 357
Creating Directory Synchronization E-mail Addresses 358
Modifying Directory Synchronization E-Mail Addresses 358
Removing Directory Synchronization E-mail Addresses 359
Delivery Restrictions 359
Setting Restrictions for Message Reception 361
Setting Restrictions for Message Rejection 362
Incoming Template 362
Configuring Incoming Template Mappings 363
Modifying Incoming Template Mappings 364
Removing Incoming Template Mappings 364
Outgoing Templates 364
Configuring Outgoing Template Mappings 365
Modifying Outgoing Template Mappings 365
Removing Outgoing Template Mappings 366
Diagnostics Logging 366
Starting and Stopping Directory Synchronization 366
Starting Directory Synchronization 366
Stopping Directory Synchronization 367
Deleting Dirsync Requestors and Servers 367
Deleting a Dirsync Requestor 367
Deleting a Dirsync Server 367
Manual Directory Synchronization 368
Importing the Directory Synchronization Master List Manually 369
Editing the Windows NT Registry 369
Restarting the Microsoft Exchange Directory Synchronization Service 370

Copying the Resync.glb File to an External Storage Device 370
Importing the Resync.glb File to the Remote Directory Synchronization Requestor 370

Chapter 12 Microsoft Schedule+ Free/Busy Connector for Microsoft Mail 373
Schedule+ Free/Busy Connector Setup 374
Installing Microsoft Mail Connector 374
Assigning AdminSch Accounts 375
Installing Schedule+ Program Files 375
Installing the Schedule+ Administrator Program 375
Configuring Schdist.exe 375
Schedule+ Free/Busy Connector Configuration 376
Schedule+ Free/Busy Connector Options Configuration 377
Assigning an Administrator's Mailbox 377
Assigning a Schedule+ Distribution List 377
Exporting the Schedule+ Distribution List 378
Setting the Schedule+ Free/Busy Connector Update Frequency 378
Exporting Free and Busy Updates for the Microsoft Exchange Server Site Only 378
Setting the Schedule+ Free/Busy Connector Logging Level 379
General Properties 379
Specifying the Display Name and Alias Name 380
Unresolved Schedule+ Messages 381

PART 3 Setting Up Internet Protocols 383

Chapter 13 Internet Protocols 385
Configuring Site and Server Properties 385
General Properties 387
Defining a Display Name 388
Using the Site Defaults 388
Permissions 389
Connections 389
Accepting or Rejecting Connections 390
Adding a Rule 391
Removing a Rule 391
Moving a Rule Up or Down 392
Editing a Rule 392
MIME Types 393
Creating a New MIME Type 394
Removing a MIME Type 394

Moving a MIME Type Up or Down 394
Mailbox and Custom Recipient Configuration 395

Chapter 14 POP3 397

POP3 Site and Server Properties Configuration 397
General Properties 398
Defining a Display Name 399
Using the Site Defaults 399
Enabling or Disabling POP3 399
Authentication 399
Setting Authentication Methods 401
Message Format Properties 402
Enabling Rich Text Format 403
Specifying Message Format Options 404
Idle Time-out 406
Setting Idle Time-out Connections 406
Diagnostics Logging 407
POP3 Mailbox Configuration 407
Enabling POP3 for a Mailbox 408
Specifying POP3 Settings for Message Encoding 409
Internet Mail Service Configuration 410
Configuring the Internet Mail Service 411
POP3 Client Configuration 411
POP3 Account Name 412
POP3 E-mail Address 413
POP3 Server Name 413
SMTP Server Name 413
Sample POP3 Client Configuration 414

Chapter 15 IMAP4 415

IMAP4 Site and Server Properties Configuration 415
General Properties 417
Defining a Display Name 417
Using the Site Defaults 417
Enabling or Disabling IMAP4 418
Disabling Public Folder Listings for the Site or Server 418
Disabling Fast Message Retrieval 418
Authentication 418
Setting Authentication Methods 420
Anonymous Connections 421

Setting Anonymous Access 422
Message Format Properties 423
Specifying Message Format Options 424
Idle Time-out 425
Setting Idle Time-out Connections 426
Diagnostics Logging 426
IMAP4 Mailbox Configuration 426
Enabling IMAP4 for a Mailbox 427
Specifying IMAP4 Settings for Message Encoding 428
Disabling Public Folder Listings for a Mailbox 428
Enabling an IMAP4 Delegate User to View Another User's Folders 429
Internet Mail Service Configuration 429
Configuring the Internet Mail Service 430
IMAP4 Client Configuration 431
IMAP4 Account Name 431
IMAP4 E-mail Address 432
IMAP4 Server Name 432
SMTP Server Name 433
Sample IMAP4 Client Configuration 433

Chapter 16 LDAP 435

LDAP Site and Server Property Configuration 435
General Properties 436
Defining a Display Name 437
Using the Site Defaults 437
Enabling or Disabling LDAP 438
Permissions 438
Authentication 438
Setting Authentication Methods 439
Anonymous Connections 440
Setting Anonymous Access 441
Searches 441
Specify Substring Searches 443
Referrals 443
Adding a Referral 444
Setting a Default Referral 445
Modifying a Referral 445
Removing a Referral 445
Idle Time-out 445
Setting Idle Time-out Options 446

Chapter 17 NNTP 447
How the Internet News Service Works 447
Newsfeeds 448
Newsgroup Public Folders 450
Naming Newsgroup Public Folders 451
Using Moderated Newsgroups 451
Using the Internet News Service 452
Managing Newsgroup Public Folders 452
Understanding Control Messages 452
Catching Up to Current Newsfeeds 453
Contacting Your Newsfeed Provider 454
Internet News Service and Newsfeeds 455
Typical Configuration Scenarios 455
Scenario 1 455
Scenario 2 456
Scenario 3 456
Configuring an NNTP Newsfeed 456
Configuring Newsfeed Properties 458
General Properties 459
Defining a Display Name 459
Enabling a Newsfeed 459
Assigning an Administrator's Mailbox 459
Message Size Limits 460
Setting a Message Size Limit 460
Hosts 461
Connecting to the Remote USENET Site 461
Specifying the Remote USENET Host 462
Setting Up Additional Inbound Hosts 462
Removing an Inbound Connection 462
Connection 463
Configuring the Newsfeed to Use a LAN Connection 463
Configuring the Newsfeed to Use a Dial-up Connection 464
Security 464
Requiring Secure SSL Connections 465
Setting Up an Account and Password for Outbound Connections 466
Setting Up a Mailbox or Custom Recipient for Inbound Connections 467
Schedule 468
Setting the Connection Schedule 469
Inbound Pull Newsfeeds 470

Adding a Newsgroup to an Inbound Pull Feed 471
Removing a Newsgroup from an Inbound Pull Feed 471
Specifying a New Active File for Creating Newsgroup Public Folders in an Inbound Pull Feed 472
Inbound Push Newsfeeds 472
Configuring a Newsgroup to Accept Items in an Inbound Push Feed 473
Configuring a Newsgroup to Reject Items in an Inbound Push Feed 474
Creating Newsgroup Public Folders 474
Specifying a New Active File for an Inbound Push Feed 474
Outbound Newsfeeds 475
Adding a Newsgroup to an Outbound Feed 475
Removing a Newsgroup from an Outbound Feed 476
Advanced 476
Flushing Queued Messages 477
Setting Up Newsgroup Hierarchies 477
Defining a Newsgroup Public Folder as a Hierarchy 478
Removing a Newsgroup Public Folder from the Hierarchy 478
Setting Up Properties for NNTP 479
General Properties 480
Defining a Display Name 480
Enabling NNTP for the Site 480
Enabling Client Access for the Site 480
Using the Site Defaults 481
Permissions 481
Newsfeed Properties 482
Viewing Newsfeed Properties 482
Changing the USENET Site Name 483
Creating an Active File of Newsgroup Public Folders 483
Control Messages Properties 484
Processing Queued Control Messages 485
Authentication 485
Setting Authentication Methods 486
Message Format Properties 487
Specifying Message Format Options 489
Enabling Client S/MIME Signature Support 489
Idle Time-out 490
Setting Idle Time-out Connections 491
Anonymous Connections 491
Setting Anonymous Access 492

Diagnostics Logging 493
NNTP Mailbox and Custom Recipient Configuration 493
Enabling NNTP for a Mailbox or Custom Recipient 494
Specifying NNTP Settings for Message Encoding 495
Setting Properties on Newsgroup Public Folders 496
Changing the Default Character Sets 497
Configuring NNTP Clients 498
NNTP Account 498
NNTP Server 499
SSL Connections 499
Sample NNTP Client Configuration 500

Chapter 18 Microsoft Outlook Web Access 501
Outlook Web Access Installation 501
How Outlook Web Access Works 502
Authentication 503
Security Levels 503
Validated User 503
Anonymous User 504
Outlook Web Access Configuration 504
General Properties 505
Defining the Display Name 506
Enabling HTTP 506
Enabling Web Browser Access 506
Setting Anonymous Access 507
Permissions 507
Published Public Folders 508
Working with Public Folder Shortcuts 509
Setting Public Folder Anonymous Permissions 509
Advanced Properties 510
Setting the Number of Address Book Entries Returned 511

PART 4 Appendixes 513

Appendix A Setting Up Windows NT Server for RAS Connectivity 515
RAS Server Configuration 515
Configuring the Modem and Port 516
Enabling TCP/IP 516
Creating a Pool of TCP/IP Addresses for RAS 516
TCP/IP Configuration 517
Lmhosts File 518

Enabling Lmhosts Lookup Functionality 518
Modifying Lmhosts Files 518
Guidelines for Working with Lmhosts Files 519
Verifying the Lmhosts File 519
RAS Client Configuration 520
Windows NT RAS Authentication 520
Using Credentials Defined by the Service Account 520
Using Credentials Supplied by the User 521
Creating Override Accounts 521

Index 523

Before You Begin

Microsoft® Exchange Server consists of services that provide your company with advanced messaging and information management tools. While *Microsoft Exchange Server Concepts and Planning* helps administrators plan their Microsoft Exchange Server organization, this manual helps implement their plan. It 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 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 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 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 the 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 divided into four parts to provide you with complete, task-oriented information about administering, setting up, and modifying your Microsoft Exchange Server organization.

Part 1 "Customizing Microsoft Exchange Server Features" Describes how to set up distribution lists and custom recipients, use Address Books, and set up advanced security.

Part 2 "Setting Up Connectors" Describes how to connect sites within your organization and how to connect to foreign systems.

Part 3 "Setting Up Internet Protocols" Provides an overview of each Internet protocol that Microsoft Exchange Server supports. Describes how to configure each protocol using the Microsoft Exchange Server Administrator program.

Part 4 "Appendixes" Contains supplementary information about setting up Windows NT Server for RAS connectivity.

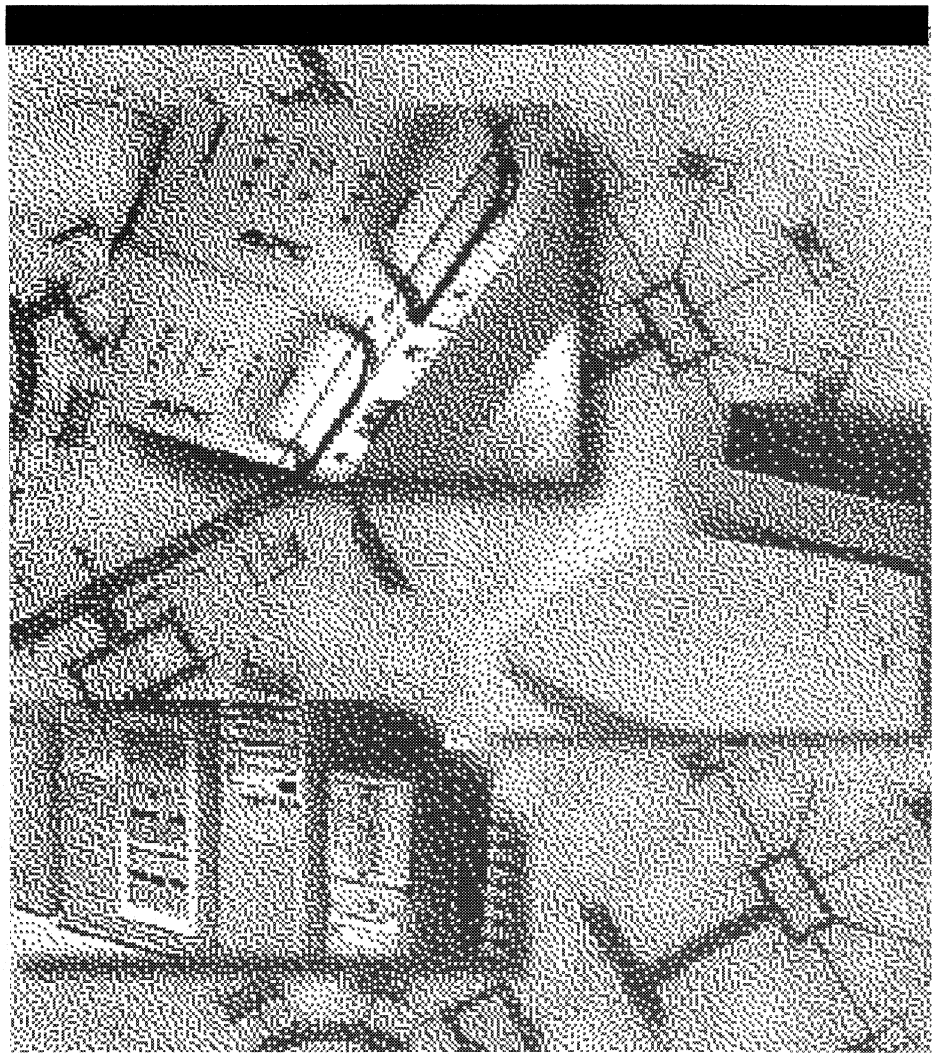
Document Conventions

To help you locate and interpret information easily, *Microsoft Exchange Server Operations* 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.
Italic	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.

PART 1

Customizing Microsoft Exchange Server Features



CHAPTER 1

Distribution Lists and Custom Recipients



Microsoft Exchange Server receives messages and information through objects known as *recipients*. Recipients can be:

- Mailboxes
- Distribution lists
- Custom recipients
- Public folders
- Mailbox agents

This chapter describes how to define or modify the properties for distribution lists and custom recipients. For detailed information on how to create, define, or modify the properties for mailboxes and public folders, see *Microsoft Exchange Server Getting Started.* For information on creating a mailbox agent, see the *Microsoft Exchange Server Programmer's Reference*, available separately from Microsoft.

Distribution Lists

A distribution list is a group of recipients created to expedite mass mailing of messages and other information. When a message is sent to a distribution list, all members of the distribution list receive a copy.

Creating Distribution Lists

You can create new distribution lists when you want to send the same information to a group of recipients rather than addressing each individual separately.

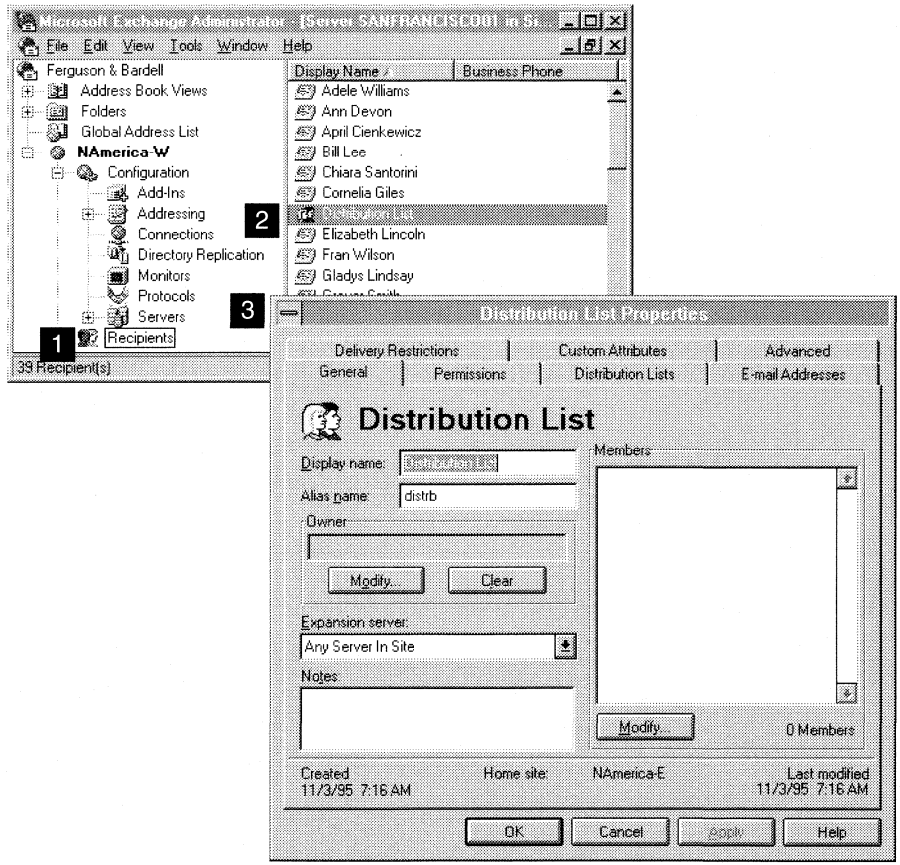
1. In the Administrator window, choose a recipients container or an Address Book view container.
2. From the **File** menu, choose **New Distribution List**.

General Properties for a Distribution List

Use the distribution list **General** property page to specify a new distribution list, modify the distribution list name or owner, and to add and delete members.

Getting to the distribution list General property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the distribution list you want to configure.
3. Select the **General** tab.



Entering New Distribution List Name Information

After the distribution list is created, you can specify the display name, alias name, expansion server, and members.

1. Select the **General** tab.
2. Type the display name and alias name for the distribution list.

Option	Description
Display name	The name (up to 256 characters) that appears in the Administrator window and the Address Book.
Alias name	Another identifier for this distribution list. The limit is 64 characters.

Specifying an Expansion Server

When a user in your site sends a message to a distribution list, Microsoft Exchange Server must expand the list, resolve the names of all recipients in the list, and determine the most efficient routing for the message. For large distribution lists, expanding the list can create a significant load on the server. You can force the distribution list to be expanded on a specific server.

1. Select the **General** tab.
2. Select an expansion server.

Option	Description
Any Server In Site	This is the default setting. Expands the distribution list on any server in your organization.

Adding Members to a Distribution List

You can add a member to an existing distribution list. All distribution list members, which can include mailboxes, custom recipients, public folders, and other distribution lists, receive messages sent to the distribution list.

1. Select the **General** tab.
2. In the **Members** box, choose **Modify**.
3. Select a recipient, and then choose **Add**.

Adding an Owner to a Distribution List

The owner of a distribution list is the primary contact person for that list. The owner can change the name of the distribution lists in Microsoft Outlook®. The owner also receives any notifications about the distribution list such as non-delivery reports (NDRs).

The owner of the distribution list can modify distribution list members in Microsoft Outlook. Typically, only an administrator with permissions can modify distribution list members using the Administrator program.

1. Select the **General** tab.
2. In the **Owner** box, choose **Modify**.
3. Select a recipient, and then choose **OK**.

Removing Members from a Distribution List

Use the **General** property page to remove members from a distribution list.

1. Select the **General** tab.
2. In the **Members** box, choose **Modify**.
3. Select a member to remove, and then press DELETE.

Deleting an Owner from a Distribution List

Use the **General** property page to delete an owner from a distribution list.

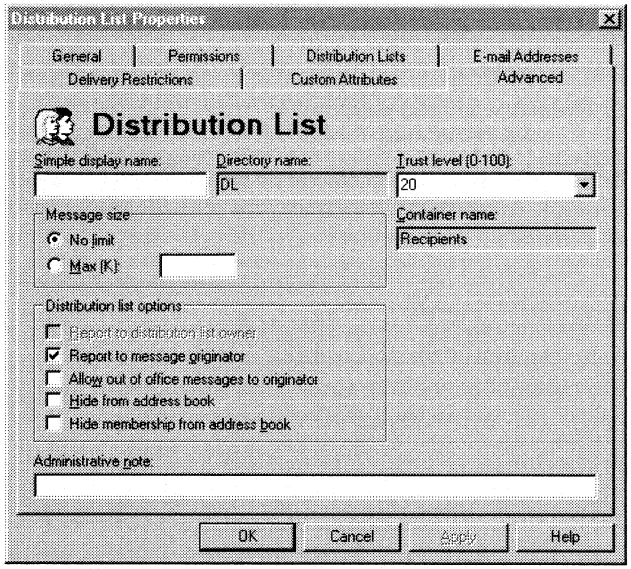
1. Select the **General** tab.
2. In the **Owner** box, choose **Clear**.

Advanced Properties for a Distribution List

Use the **Advanced** property page to provide a simple display name, set message transfer limits, set a trust level for directory synchronization, and determine whether the distribution list appears in the Address Book.

Getting to the Advanced property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the distribution list you want to configure.
3. Select the **Advanced** tab.



Changing the Simple Display Name

The display name of a distribution list can contain non-ANSI characters. Use the **Advanced** property page to change the display name.

1. Select the **Advanced** tab.
2. In the **Simple display name** box, type a name to be used by systems that cannot interpret all the characters in the normal display name.

Setting a Limit for Message Transfer

You can set a size limit for messages that can be sent to and from this distribution list.

1. Select the **Advanced** tab.
2. Under **Message size**, select an option.

Option	Description
No limit	Messages of any size can be sent or received by this distribution list. This is the default.
Max (K)	The largest message this distribution list can send or receive is specified when this option is selected.

Setting the Distribution List Options

There are several distribution list options you can set such as enabling out-of-office messages or hiding the distribution list from the Address Book.

Note Even if a distribution list is hidden from the Address Book, you can still send mail to the distribution list if you know its e-mail address and explicitly enter it in the **To** box of a message.

1. Select the **Advanced** tab.
2. Under **Distribution list options**, select an option.

Option	Description
Report to distribution list owner	Sends notification reports to the distribution list owner when a message sent to the distribution list has requested delivery notification or is undeliverable.
Report to message originator	Sends notification reports to the message originator that indicate the delivery status for each member of the list when a message sent to the distribution list has requested delivery notification or is undeliverable. When this option is not selected, the message originator receives reports from the list, not notification for each member.
Allow out of office messages to originator	Sends out-of-office messages from members of the distribution list to the originator. You may not want to select this option for large distribution lists.
Hide from address book	Indicates that you do not want this distribution list to appear in the Address Book.
Hide membership from address book	Indicates that you do not want the list of recipients that are members of the distribution list to appear in the Address Book.

Setting a Trust Level for Directory Synchronization

The trust level determines whether information about a distribution list is replicated to other sites during directory synchronization. If the trust level exceeds the trust level you specified for the directory synchronization requestor, information about the distribution list is not replicated during directory synchronization.

1. Select the **Advanced** tab.
2. In the **Trust level** box, select a trust level.

For more information on trust levels, see *Microsoft Exchange Server Concepts and Planning*.

Custom Recipients

A custom recipient is a recipient outside the messaging site, local post office, or organization, such as an Internet recipient with an SMTP address. When you create a custom recipient, it appears in the site Address Book and can receive messages. You can use the Administrator program to create a custom recipient or you can use the directory import feature to import custom recipients from other messaging systems.

Creating Custom Recipients

Use the following procedure to create custom recipients.

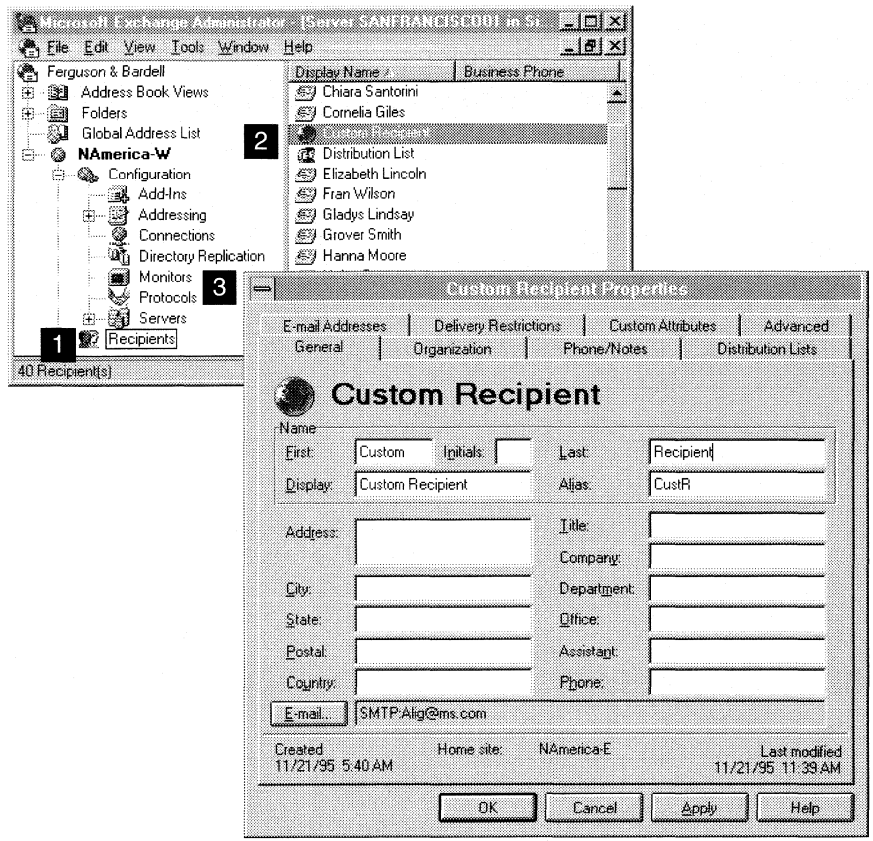
1. From the **File** menu in the Administrator window, choose **New Custom Recipient**.
2. In the **Select an e-mail address type** box, select the type of e-mail address you want to create, and then choose **OK**.
3. Type the user's e-mail address.

General Properties for a Custom Recipient

Use the **General** property page to record basic information, such as name, location, and e-mail address.

Getting to the custom recipient General property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the custom recipient you want to configure.
3. Select the **General** tab.



Entering User Name Information

User name information identifies the user associated with this custom recipient. Provide a first name, middle initial, and last name, as well as a display name and an alias name.

You can configure Microsoft Exchange Server to generate the display name and alias name automatically as you type the first name, middle initial, and last name for the mailbox. Access the **Auto Naming** property page using **Options** on the **Tools** menu.

1. Select the **General** tab.
2. In the appropriate boxes, type the user name information.

Option	Description
First	The optional first name (up to 64 characters) for the mailbox user.
Initials	The optional middle initial (up to 6 characters) for the mailbox user.
Last	The optional last name (up to 64 characters) for the mailbox user.
Display	The name (up to 256 characters) that appears in the Administrator window and the Address Book.
Alias	Another identifier for this custom recipient. The limit is 64 characters.

Entering Address Information

Address information identifies the user's postal address.

1. Select the **General** tab.
2. In the appropriate boxes, specify the mailbox owner's address information, including address, city, state, postal, and country.

Entering Company Information

Company information specifies the mailbox owner's contact details.

1. Select the **General** tab.
2. In the appropriate boxes, specify the mailbox owner's company information, including title, company, department, office, assistant, and phone.

Creating or Modifying a Custom Recipient's E-mail Address

When you create a new custom recipient, you specify the type of e-mail address the custom recipient has and provide detailed e-mail address information. You can modify this e-mail address information in the **General** property page. For example, if you created a custom recipient with an X.400 address and the private management domain (PRMD) information changes, you can update that information in the **General** property page.

1. Select the **General** tab.
2. Choose **E-mail**, and then select an option.

Option	Description
Modify existing e-mail address	Displays the e-mail address properties for the custom recipient. Make changes to the existing e-mail address, and then choose **OK**.
Create new e-mail address	Displays the e-mail address type dialog box. After selecting an e-mail address type, enter the new e-mail address for the custom recipient, and then choose **OK**.

For more information, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

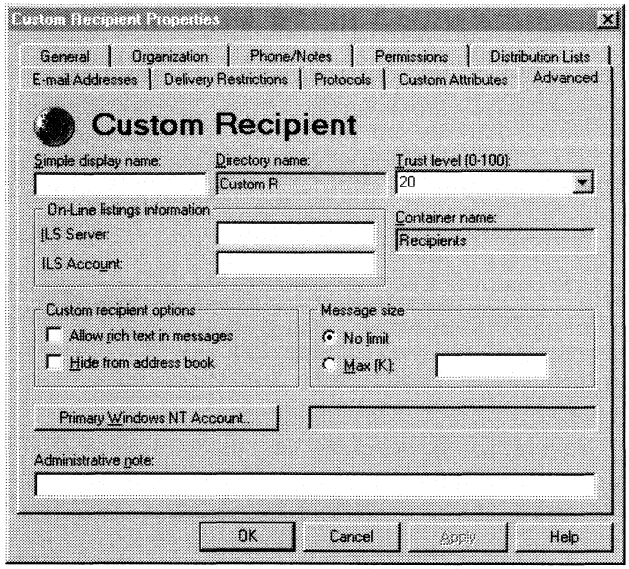
Advanced Properties for a Custom Recipient

Use the **Advanced** property page to provide a simple display name, set message limits, set a trust level for directory synchronization, and determine whether the recipient appears in the Address Book.

The trust level determines whether information about a custom recipient is replicated to other sites during directory synchronization. If the trust level exceeds the trust level you specified for the directory synchronization requestor, information about the recipient is not replicated during directory synchronization.

Getting to the Advanced property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the custom recipient you want to configure.
3. Select the **Advanced** tab.



Specifying On-Line Listings Information for Microsoft NetMeeting

If your organization is using Microsoft NetMeeting™, you can specify Microsoft Internet Locator Server (ILS) information for custom recipients. This enables other NetMeeting users to locate the recipient and set up an online meeting.

1. Select the **Advanced** tab.
2. Type the names of the recipient's ILS server and ILS account.

Setting a Message Size Limit

You can set a message size limit that indicates the size of messages that can be sent to this custom recipient.

1. Select the **Advanced** tab.
2. Under **Message size**, select **No limit**.

Option	Description
No limit	Sends messages of any size. This is the default.
Max (K)	Sets a message size.

Allowing Rich Text in Messages

Rich text in messages allows the use of characters such as bold, color, and italic. Rich text also provides the ability to position attachments. The client must support rich text format to see rich text attributes in messages.

1. Select the **Advanced** tab.
2. Under **Custom recipient options**, select **Allow rich text in messages**.

Hiding a Recipient from the Address Book

You can hide a custom recipient if you don't want it to appear in the Address Book.

Note Even if custom recipients are hidden from the Address Book in the client, you can still send them mail if you know the e-mail address and enter it in the **To** box of a message.

---

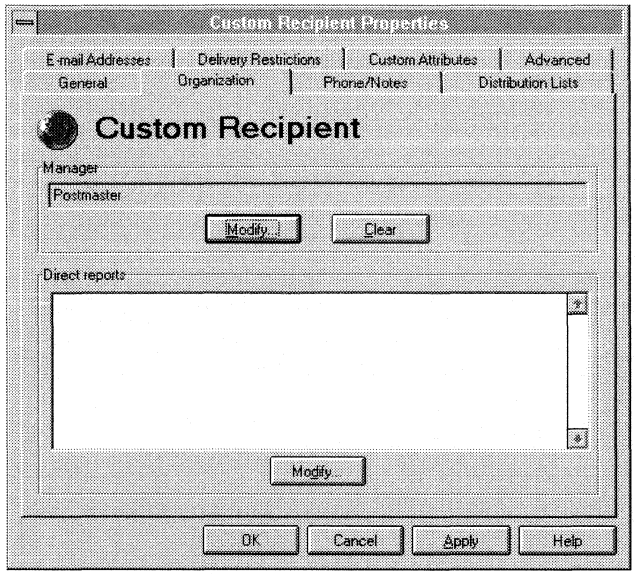
1. Select the **Advanced** tab.
2. Under **Custom recipient options**, select **Hide from address book**.

Organization Information for a Custom Recipient

Use the **Organization** property page to record information about the custom recipient, such as the name of the manager and individuals who report to the manager. The information in the **Organization** property page is optional.

Getting to the custom recipient Organization property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the custom recipient you want to configure.
3. Select the **Organization** tab.



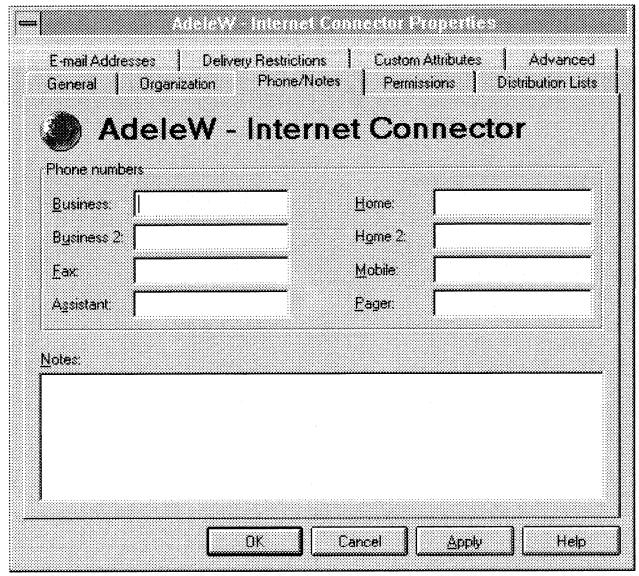
Phone Numbers for a Custom Recipient

Use the **Phone/Notes** property page to enter detailed phone number information and optional notes for a custom recipient. All the information in the **Phone/Notes** property page is optional.

For information on adding detailed phone number information, see *Microsoft Exchange Server Getting Started.*

Getting to the custom recipient Phone/Notes property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the custom recipient you want to configure.
3. Select the **Phone/Notes** tab.



Common Properties for Recipients

There are several properties common to most recipients, including:

- E-mail addresses
- Distribution list membership
- Delivery restrictions
- Delivery options
- Custom attributes

E-mail Addresses for Recipients

E-mail addresses identify recipients to the gateways and connectors that connect Microsoft Exchange Server with other messaging systems. Use the **E-mail Addresses** property page to create, modify, or remove e-mail addresses.

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

Distribution List Membership for Recipients

A distribution list is a collection of recipients that are grouped together and addressed as a single recipient. Individual recipients can be members of several distribution lists. The set of distribution lists to which a recipient belongs is called the recipient's distribution list membership.

You can use the **Distribution Lists** property page to specify the distribution list membership for a recipient.

Getting to the mailbox Distribution Lists property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the mailbox, custom recipient, or public folder you want to configure.
3. Select the **Distribution Lists** tab.

Adding Recipients to a Distribution List

You can add recipients to distribution lists.

1. Select the **Distribution Lists** tab.
2. Choose **Modify**, and then select a distribution list that you want to add this recipient to.
3. Choose **Add**, and then choose **OK**.

Removing Recipients from a Distribution List

You can remove recipients from distribution lists.

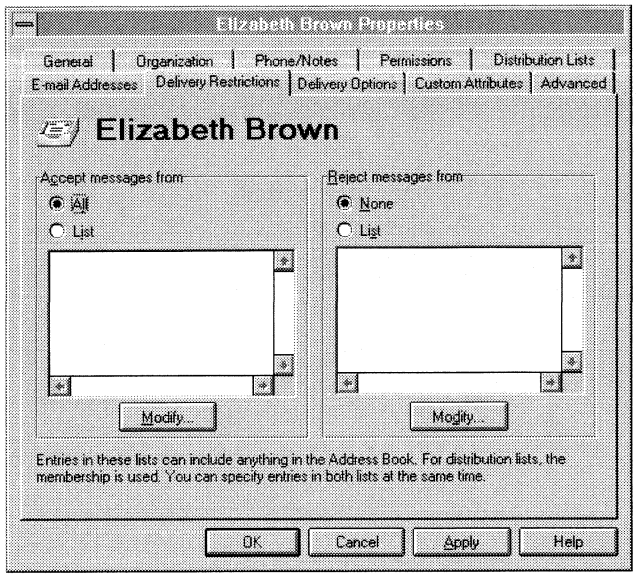
1. Select the **Distribution Lists** tab.
2. Choose **Modify**.
3. In the **Distribution List Members** box, select a recipient to remove, and then press DELETE.
4. Choose **OK**.

Delivery Restrictions for Recipients

You can specify which recipients a mailbox, distribution list, or custom recipient will accept messages from (not available for public folders). All rejected messages are returned to the originator.

Getting to the recipient Delivery Restrictions property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the recipient you want to configure.
3. Select the Delivery Restrictions tab.



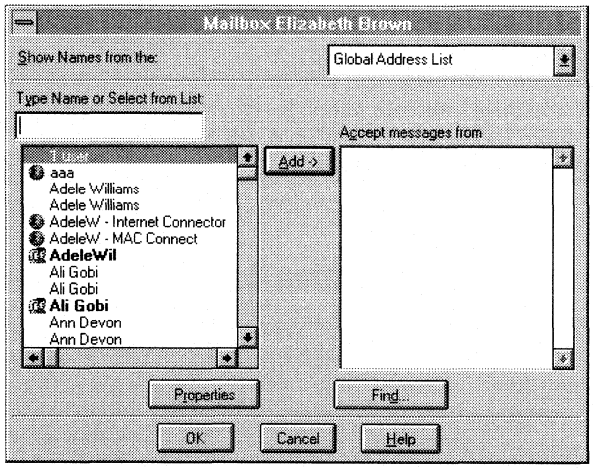
Accepting or Rejecting Messages from Specific Senders

You can accept or reject messages from any sender listed in the directory. Delivery restrictions are optional and do not affect incoming messages. The default is to accept messages from all senders and reject messages from none. If you specify even one name in the **Accept messages from** box, messages from all other senders who are not listed in the box are rejected.

Note If a distribution list is specified, the members of the distribution list are used for the restriction, not the distribution list itself.

---

1. Select the **Delivery Restrictions** tab.
2. Under either **Accept messages from** or **Reject messages from**, select **List**.
3. Choose **Modify** to open the Address Book so you can select from a list of recipients.

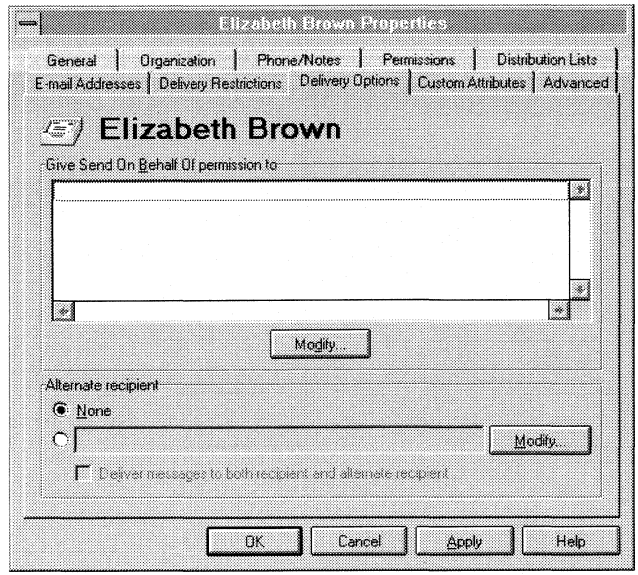


Delivery Options for Recipients

You can specify delivery options for a recipient who will receive all messages intended for the primary recipient, or a recipient who has permissions to send messages on behalf of the primary recipient. This option is not available for public folders or custom recipients.

Getting to the recipient Delivery Options property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the recipient you want to configure.
3. Select the **Delivery Options** tab.



Specifying an Alternate Recipient for Incoming Messages

You can specify an alternate recipient when you want another recipient to receive incoming messages intended for a mailbox or distribution list. For example, if you are going out of town on business, you can specify a team member to receive all your messages.

1. Select the **Delivery Options** tab.
2. Under **Alternate recipient**, choose **Modify**.
3. Select a recipient, and then choose **OK** to confirm your selection.
4. Select or clear Deliver messages to both recipient and alternate recipient.

Option	Description
Alternate recipient	Specifies an alternate recipient to receive any incoming messages intended for this mailbox or distribution list.
None	When selected, specifies that you do not want an alternate recipient.
Deliver messages to both recipient and alternate recipient	When selected, messages are delivered to both the recipient and alternate recipient. When cleared, messages are delivered to the alternate recipient only.

Specifying Who Can Send Messages on Behalf of a Recipient

You can give another recipient the authority to send messages on behalf of a mailbox or custom recipient (not available for a distribution list or public folder). For example, if you give Adele Williams Send On Behalf Of permission for Ali Gobi's mailbox, Adele can compose a message and send it on behalf of Ali Gobi. When the recipient gets the message, the message heading indicates that the message was sent by Adele Williams on behalf of Ali Gobi. This is different from Send As permission, which does not indicate in the message heading the actual sender. Use the mailbox **Permissions** property page to give Send As permission.

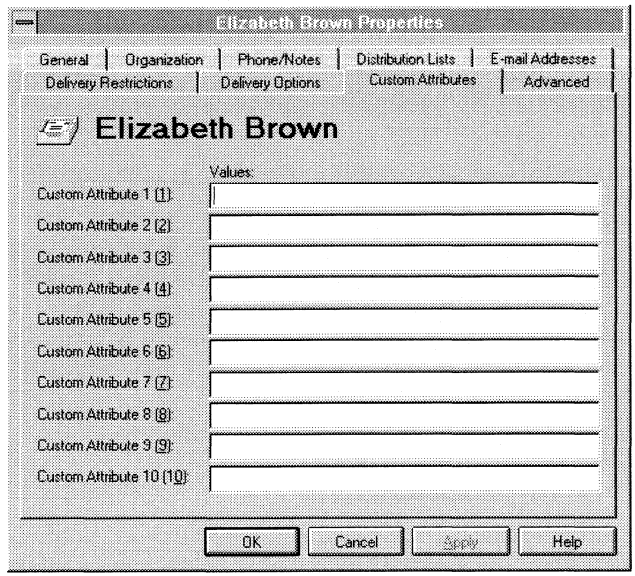
1. Select the **Delivery Options** tab.
2. Under **Give Send On Behalf Of permission to**, choose **Modify**.
3. In the Address Book, select a recipient, and then choose **Add**.

Custom Attributes for Recipients

The **Custom Attributes** property page contains 10 unique custom attribute fields that you customize to track information about the recipients in your site. For example, suppose your company uses an employee ID numbering system. If your company defines a custom attribute field called Employee ID# in the **Custom Attributes** property page of the DS Site Configuration object, then that field automatically appears in the **Custom Attributes** property page for every recipient. By default, the fields are called Custom Attributes 1 through 10.

Getting to the Custom Attributes property page

1. In the Administrator window, choose a recipients container or an Address Book view container.
2. Double-click the mailbox, distribution list, custom recipient, or public folder you want to configure.
3. Select the **Custom Attributes** tab.



Renaming the Custom Attribute Fields

You can rename custom attribute fields to track information about the recipients in your site.

1. In the Administrator window, choose **Configuration**.
2. Double-click DS Site Configuration.
3. Select Custom Attributes.
4. Type the new names in **Custom Attribute** boxes 1 through 10.
5. Select **Apply**, and then choose **OK**.

This information appears in the **Custom Attributes** property page of every recipient in your site.

CHAPTER 2

Address Books



The Microsoft Exchange Server Address Book allows you to address messages and look up locations or phone numbers. It displays recipient names that can be organized into various lists containing mailboxes, distribution lists, custom recipients, and public folders.

You can use Address Book views to group recipients by a common attribute, such as employee number. Microsoft Exchange Server also provides several types of templates you can use to customize how information appears in the Address Book.

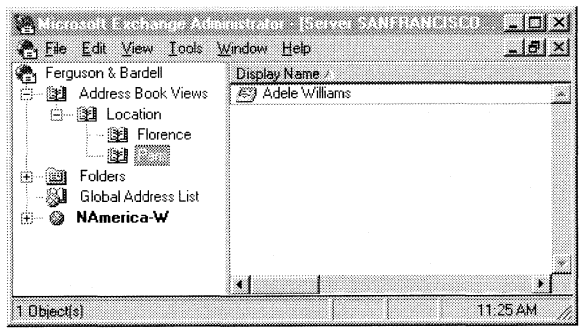
Understanding Address Book Views

Typically, you use Address Book views to organize mailboxes and custom recipients. Address Book views are automatically created based on the values of attributes on recipient objects. Address Book view containers are displayed in the Microsoft Outlook Address Book, similar to the way recipient containers are displayed in the Microsoft Exchange Server Administrator program.

For example, you can create an individual Address Book View container for each city in which your company has an office. Company X has offices in several cities so it creates an Address Book view called Offices, with a grouping based on the city attribute. For every recipient value of the city attribute, a new Address Book view container is created. User A, whose city attribute is Denver, appears in an Address Book view container called Denver, while user B, whose city attribute is Tucson, appears in an Address Book view container called Tucson. Address Book view containers are created automatically, so if user C with a city attribute of Flagstaff is added, the user appears in a new Address Book view container called Flagstaff.

As more offices are added, company X may organize its Address Book view by state as well as by city. An Address Book view grouping can be based on more than one attribute. Company X can modify the Offices Address Book view so that it is grouped first by the state attribute, and then grouped by the city attribute. Once the state information is added to all the recipients, a new set of Address Book view containers is automatically created with a container for Arizona, and subcontainers for Tucson and Flagstaff.

Each Address Book view has one or more groupings of recipients that correspond to attributes on recipient objects. Any recipient with attributes that match the Address Book view grouping appear in a container under that Address Book view in the Microsoft Exchange Server Administrator program. Address Book views are also available in the **Show Names from the** box in the Outlook Address Book. For example, you create an Address Book view called Location with a grouping for city. If the city attribute in Adele's mailbox is set to Paris, Adele's mailbox appears in the Paris Address Book View container under the Location Address Book view, as shown in the following illustration.



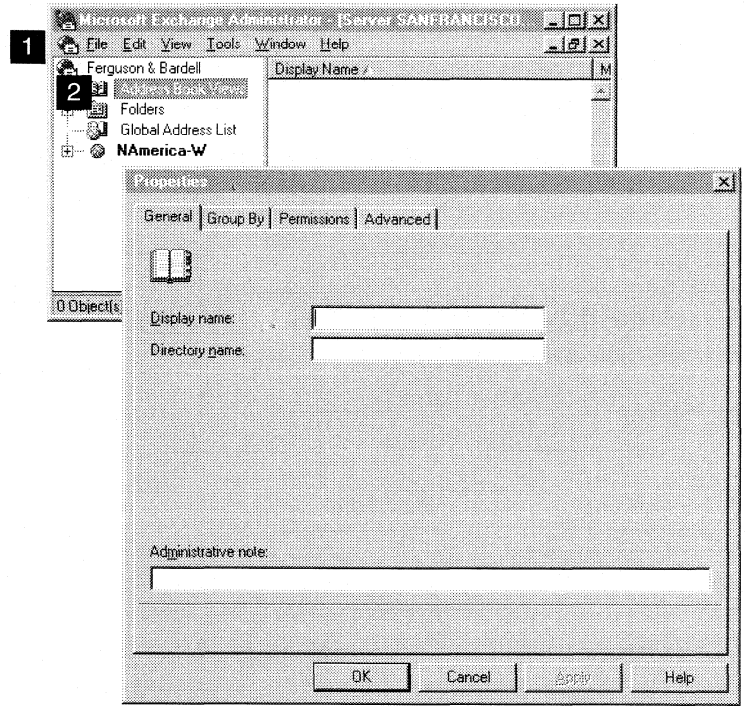
After you create an Address Book view, recipients appear in that Address Book view. You can group the containers into larger views, such as state or country, or move recipient objects between Address Book View containers by changing their attributes. Alternatively, you can use the Administrator program to move recipients to another Address Book View container.

Creating Address Book Views

To create an Address Book view, you must specify an Address Book view name and define the attributes that will be used to create the containers (groupings that you want to put recipient objects in). You must complete the **General** property page, and then select at least one attribute from the **Group By** property page to create an Address Book view.

Complete the following procedure to create the Address Book view.

1. From the **File** menu in the Administrator window, choose **New Other**.
2. Choose Address Book Views.



3. In the **General** property page, type a name in the **Display name** box.
4. In the **Directory name** box, type a name.
5. Select the **Group By** tab.
6. Select an attribute from the **Group items by** box that you want to group recipient objects by.
7. Choose **Apply**, and then choose **OK**.

Option	Description
Display name	Type a maximum of 256 alphanumeric characters, which can include spaces and special characters. If no name is provided, the system prompts for a value.
Directory name	Type a maximum of 64 characters.

General Properties

Use the **General** property page for the Address Book view to modify the display name. The directory name can be modified only if you are creating a new Address Book view.

Getting to the General property page

1. In the Administrator window, double-click **Address Book Views**.
2. Select an Address Book view.
3. From the **File** menu, choose **Properties**.
4. Select the **General** tab.

Defining the Directory and Display Name

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

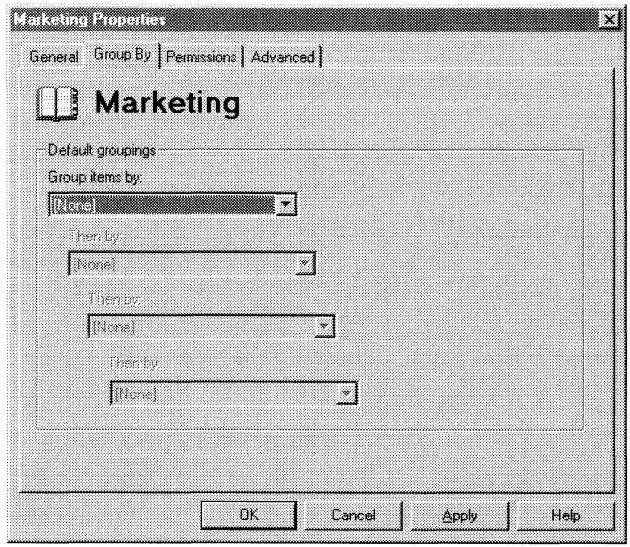
Option	Description
Display name	Type a maximum of 256 alphanumeric characters, which can include spaces and special characters. If no name is provided, the system prompts for a value.
Directory name	Type a maximum of 64 characters.

Group By Properties

Use the **Group By** property page to group recipient objects in the Address Book view. You can group recipient objects using any of the attributes that appear in the **Group items by** box. You must complete the **General** property page before you can access the **Group By** property page.

Getting to the Group By property page

1. In the Administrator window, double-click **Address Book Views**.
2. Select an Address Book view.
3. From the **File** menu, choose **Properties**.
4. Select the **Group By** tab.



Setting Group By Values

1. Select the **Group By** tab.
2. In the **Group items by** box, select an attribute you want to use to group items.
3. In the **Then by** box, select additional attributes.

Configuring Address Book Views

After creating an Address Book view, you can assign permissions and configure advanced properties for Address Book view recipient objects.

Before you can configure Address Book views, you must complete the **General** property page, and then select at least one attribute from the **Group by** property page. For more information, see "Creating Address Book Views" earlier in this chapter.

Permissions

You can assign permissions on Address Book views for Microsoft Windows NT accounts. For information on permissions, see *Microsoft Exchange Server Getting Started.*

Restricting Address Book Views

You can use search control restrictions on the **Permissions** property page to control which Address Book views users see. For example, if you are hosting multiple companies on a single Microsoft Exchange Server, you can prevent users of one company from viewing the Address Book views of another company. You do this by creating a Windows NT group for each company you are hosting and setting the Search role for each Windows NT group.

1. In the Administrator window, double-click Address Book Views.
2. Select the Address Book View container that you want to assign Search permission to.
3. From the **File** menu, choose **Properties**.
4. Select the **Permissions** tab.
5. Under the **Windows NT accounts with permissions** box, choose **Add**.
6. Select the Windows NT user or the group associated with the specified Address Book View container that you want to assign Search permission to.
7. Choose **Add**, and then choose **OK**.
8. In the **Roles** box, choose **Search**.

Note After a mailbox is created, you must add the Windows NT user account associated with the mailbox to the Windows NT group associated with the Address Book View container.

Restricting Access to Offline Address Book Views

Offline address books are files generated and stored on an offline Address Book server. When remote users connect to the Microsoft Exchange Server computer, they can download offline Address Books to their laptops or portable computers to get information about other users in the organization. You can restrict the offline Address Books that a user can download by imposing search control restrictions on the Address Book View container.

Note Users can download only the offline Address Book that they are a member of; they can't download any other offline Address Book View containers.

Complete the following procedure to restrict an Address Book view for anonymous access:

1. In the Administrator window, double-click Address Book Views.
2. Select the Address Book View container that you want to allow users to access.
3. From the **File** menu, choose **Properties**.
4. Select the **Permissions** tab.
5. Under the **Windows NT accounts with permissions** box, choose **Add**.
6. Select the Windows NT user or the group associated with the specified Address Book View container that you want to assign Search permission to.
7. Choose **Add**, and then choose **OK**.
8. In the **Roles** box, choose **Search**.

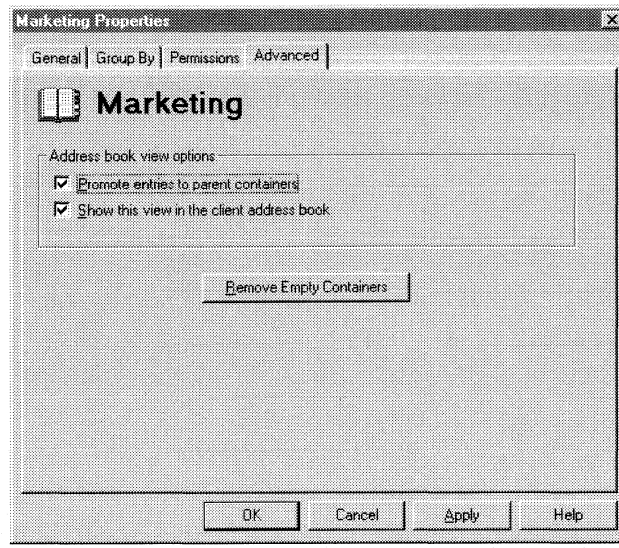
For information on downloading offline Address Books, see *Microsoft Exchange Server Getting Started.*

Advanced Properties

Use the **Advanced** property page to determine whether recipient objects should appear in one or more parent containers and which Address Book View containers will be shown in the Address Book. You can also delete empty containers within an Address Book view.

Getting to the Advanced property page

1. In the Administrator window, double-click **Address Book Views**.
2. Select an Address Book view.
3. From the **File** menu, choose **Properties**.
4. Select the **Advanced** tab.



Promoting Entries in the Address Book

Use the **Advanced** property page to determine if recipient objects are included in the parent Address Book View containers. For example, if you have containers that group mailboxes by country (USA), state (California), and city (Los Angeles), you must determine whether to include the mailbox under only the city container (Los Angeles) or under all of the containers (USA, California, and Los Angeles).

If you select the **Promote entries to parent containers** option, recipient objects appear in all containers that match the container's attributes, regardless of how the containers are related or arranged. If you do not select this option, recipient objects appear only in the lowest level container. In this case, the recipient objects would appear in only the city container and not in the state or country containers.

1. Select the **Advanced** tab.
2. Select the **Promote entries to parent containers** check box.

   If selected, recipient objects appear in all containers that match the container's attributes.

Showing Views in the Address Book

Use the **Advanced** property page to specify whether views should appear in the Address Book. Some Address Book views are visible only from the Administrator program.

1. Select the **Advanced** tab.
2. Select or clear the **Show this view in the client address book** check box.

   If selected, the Address Book view and all its containers appear in the Address Book.

Removing Empty Containers

Empty containers are not removed automatically. Use the **Advanced** property page to remove all empty containers from the Address Book view. If you move all recipient objects from one container to another, the empty container remains until you delete it.

1. Select the **Advanced** tab.
2. Choose **Remove Empty Containers**.

Note You can also remove empty containers by selecting the **Group By** tab and modifying the Group Items By attributes so that the empty containers are not needed. The Administrator program deletes the containers when the Address Book view is redefined.

You can also remove the empty Address Book View containers individually by selecting **Delete** from the **File** menu in the Administrator program.

The membership of an Address Book View is automatically recalculated when the grouping attribute for the Address Book view is changed. During recalculation, the old Address Book view containers are lost, and new containers are created based on the new grouping attributes.

Working with Address Book Views

After you set up Address Book views and their corresponding containers, you can move recipient objects between containers, change the properties of the Address Book view, delete Address Book views and their containers, and search Address Book views and their containers.

Moving Recipient Objects Between Address Book View Containers

When you move recipient objects between containers, the attribute that defined the recipient object in the original container is changed to the value of the attribute of the new container.

1. In the Administrator window, select one or more recipient objects that you want to move.
2. From the Tools menu, choose Add to Address Book View.
3. In the **Add** dialog box, select the container that you want to move the recipient object to, or choose **New Container** to add a new empty container.
4. Choose **OK**.

Adding a New Item to an Address Book View Container

You can add new recipient objects to an Address Book View container by changing the attribute value for that item. For example, if you have a container that groups items, and the Title attribute has a value of Mister, you can add a mailbox to that container by changing the Title attribute of any mailbox to Mister.

1. In the Administrator window, choose **Recipients**.
2. Double-click the recipient object you want to configure.
3. Select the **General** tab.
4. Change the attribute.

Customizing an Address Book View Hierarchy

You may want to change the way subcontainers are grouped for certain Address Book views. For example, if you have a container that groups items by country and subcontainers that group items by state and city, you may not want a state grouping in certain situations. For example, the country, state, and city groups work well for countries that have states, such as USA, Washington, Seattle. However, for countries, such as Greece, that do not have states, you would want only the city grouping. You can remove the state grouping in this instance so that Greece contains only a city grouping.

Note Changing or deleting a container or subcontainer does not delete the recipient objects in that container. It removes only the container.

Use the following procedure to customize an address book view hierarchy.

1. In the Administrator window, choose the Address Book View container you want to customize.
2. From the **File** menu, choose **Properties**.
3. Select the **Group by** tab.
4. In the **Sub-containers** box, select an attribute.

Changing the Address Book View Display Name

You can change the display name of an Address Book view container. For example, if you have an Address Book view grouped by department name and one of your departments is called Human Resources, you may want the abbreviated name, HR, to appear in the Address Book.

1. In the Administrator window, choose the Address Book View container for which you want to change properties.
2. From the **File** menu, choose **Properties**.
3. Select the **General** tab.
4. Type a new display name.

Exporting Recipients from Address Book View Containers

You can export recipients from Address Book View containers by using the **Directory Export** command from the **Tools** menu in the Administrator window. However, the default set of attributes that are exported do not include the attributes that were used to create the Address Book view. To preserve Address Book view memberships when recipients are exported and then reimported, check the header line of your export .Csv file to verify that all Address Book view grouping attributes are included.

For more information on importing and exporting files, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

Restricting Address Book Views for Anonymous Users

If your Microsoft Exchange Server allows anonymous user access, you can use Address Book views to choose which addresses anonymous users can see. For example, if you are hosting multiple companies on a single Microsoft Exchange Server, you can create a fictitious company called Help, and make only the Help container accessible to anonymous users.

Before you can restrict Address Book Views for anonymous users, you must enable a Microsoft Windows NT account for anonymous access in your site.

Complete the following procedures to enable a Microsoft Windows NT account for anonymous access:

1. In the Administrator window, choose the Address Book View container that you want to assign anonymous Search permission to, and then choose **Configuration**.
2. Double-click DS Site Configuration.
3. Select the **General** tab, and then choose **Anonymous Account**.

Complete the following procedures to restrict an Address Book view for anonymous access:

1. In the Administrator window, double-click Address Book Views.
2. Select the Address Book View container that you want to allow anonymous users to access.
3. From the **File** menu, choose **Properties**.
4. Select the **Permissions** tab.
5. Under the **Windows NT accounts with permissions** box, choose **Add**.
6. Select the Windows NT user or the group associated with the specified Address Book View container that you want to assign anonymous Search permission to.
7. Choose **Add**, and then choose **OK**.
8. In the **Roles** box, choose **Search**.

Deleting an Address Book View

You can delete an Address Book view even if the Address Book View containers still contain recipient objects. Only the Address Book view is deleted, not the items that appear in the Address Book View containers.

1. In the Administrator window, choose the Address Book view that you want to delete.
2. From the **Edit** menu, choose **Delete**.

Setting Up Large Address Book Views

Calculating the membership for an Address Book view with a large number of containers (more than 1,000) puts a heavy load on the server. You can improve server performance during these calculations by limiting the number of new containers created during each stage of the calculation. You do this by adding the following REG_DWORD key to the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeDS\Parameters\ABV max new containers

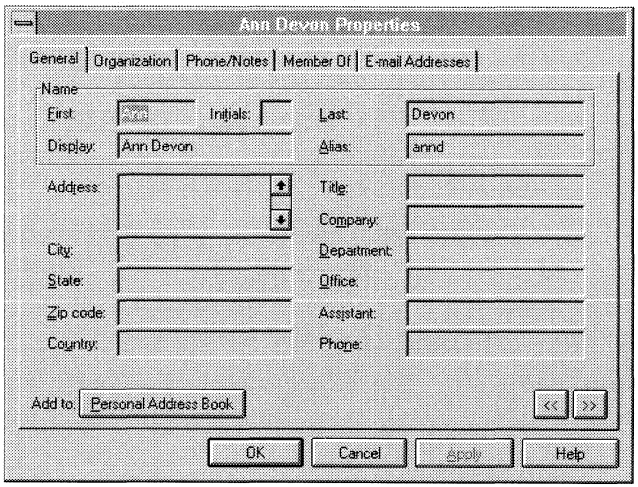
Calculation stops for five minutes after creating the specified number of new Address Book view containers. The default is 500.

Note Address Book views with large numbers of Address Book View containers can cause Windows® 16-bit e-mail clients to stop responding because they do not have enough memory to cache the entire Address Book View container hierarchy.

Details Templates

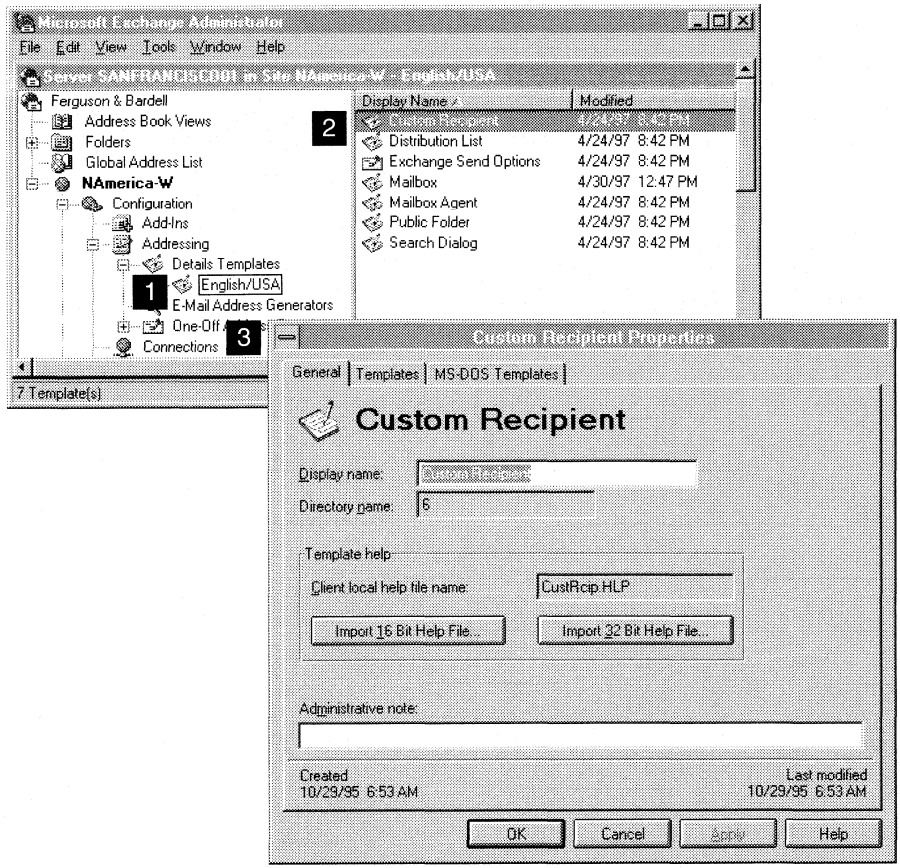
You can use the Administrator program to modify *details templates*. Details templates allow you to customize the way information about recipients appears when a user requests to see recipient properties in the Address Book. For example, you can remove the **Address** box if you do not want to publicize information about recipient addresses.

The following is an example of a details template.



Getting to the details templates General property page

1. In the Administrator window, choose **Configuration**, choose **Details Templates**, and then select one of the language containers.
2. Double-click the template you want to modify.
3. Select the **General** tab.



Changing Template Display Names

A template's display name is the name that appears in the Administrator window. Use the **General** property page to change the template display name.

1. Select the **General** tab.
2. In the **Display name** box, type the name as you want it to appear in the Administrator window.

Selecting Template Help Files

If you customize details and addressing templates, you can create and import custom template Help files. Information from these files appears when a user chooses **Help** or presses F1 while viewing information that is displayed using a details or addressing template. Template Help files are stored as attributes in the directory and are downloaded to a temporary directory on a client computer only when a user attempts to access Help from a template. Client Local Help File Name is the name of the template Help file that is created on client computers, regardless of the name of the Help file you choose to import and associate with this template.

Note Importing a new template Help file permanently overwrites previously defined template Help files. You should access all details and one-off address templates from a client computer, which creates copies of the associated Help files in the Temp directory of that computer. You can then save the Help files and import them as needed.

---

1. Select the **General** tab.
2. Under **Template help**, choose an option.

Option	Description
Import 16 Bit Help File	Opens the **Microsoft Exchange Administrator** dialog box where you can select the Help file that will be displayed on computers using Windows 16-bit operating systems.
Import 32 Bit Help File	Opens the **Microsoft Exchange Administrator** dialog box where you can select the Help file that will be displayed on computers using Windows 32-bit operating systems.

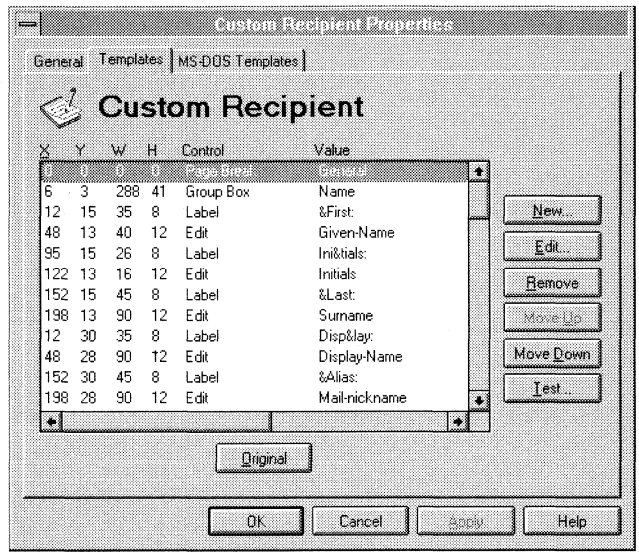
Template Modification

You can modify any template by changing one or more of the template's controls, which are attributes, such as group boxes and edit boxes, that make up a Microsoft Exchange Server dialog box.

Note The **MS-DOS Templates** property page is used in the same way as the **Templates** property page, except that the **MS-DOS Templates** property page applies to the MS-DOS® Client.

Getting to the Templates property page

1. In the Administrator window, choose **Details Templates**, and then select one of the language containers.
2. Double-click the template you want to modify.
3. Select the **Templates** tab.



Creating a New Template Control

Use the **Templates** property page to create a new template control and add a function to an existing details template. For example, you may decide to add the Employee ID attribute to the mailbox details template.

1. Select the **Templates** tab.
2. Choose **New**.

For more information, see Microsoft Exchange Server Help.

Editing or Removing a Template Control

You can edit or remove any control in a template. For example, depending on the type of control you have selected, you can change its name, value, location, size, or function.

1. Select the **Templates** tab.
2. Select the control you want to change, and then choose **Edit**.

Changing the Order of Template Controls

You can change the order in which the template controls are listed. This allows you to organize the controls in a logical way.

1. Select the **Templates** tab.
2. Select the control you want to move up or down in the list of controls, and then choose **Move Up** or **Move Down**.

Testing the Appearance of a Template

After you modify a template, or while you are making changes, you can test the appearance of a template to determine if the changes appear as you intended.

1. Select the **Templates** tab.
2. Choose **Test**.

Reverting to Original Template Settings

After you change the appearance of a template by either adding, removing, or modifying controls, you can return to the original template. Reverting to the original template permanently overwrites any changes you or another administrator made to this template. The template will appear as it did when you first installed Microsoft Exchange Server.

1. Select the **Templates** tab.
2. Choose **Original**.

One-off Address Templates

Use *one-off address templates* to address messages to mailboxes that are not in your global address list or personal address book (PAB). They are called one-off because they are often used to send one piece of mail off to an address and are not used again. (However, you can use this template to send mail and then add the addressee to your PAB.)

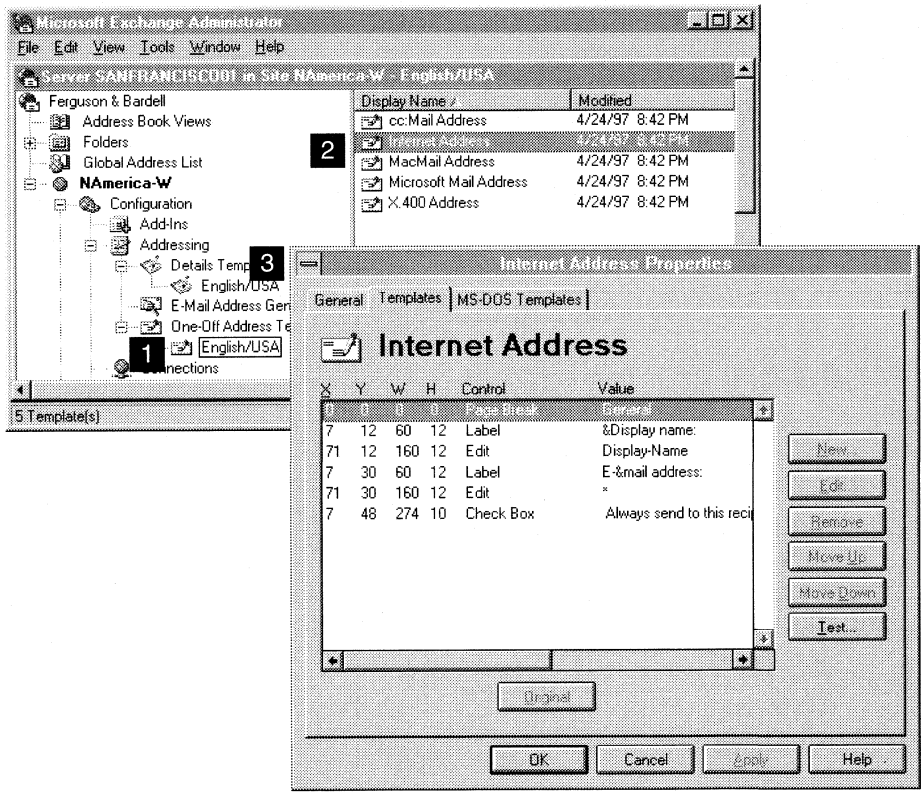
You can access one-off address templates in Outlook:

- By opening the Address Book, choosing **New Entry** from the **File** menu, selecting an address type, and then choosing **OK**.
- By composing a new message, choosing **To**, choosing **New** in the Address Book, selecting an address type, and then choosing **OK**.

You can view one-off address templates in the Administrator window, but you cannot modify them.

Getting to the one-off Address Templates property page

1. In the Administrator window, choose **Configuration**, choose **One-Off Address Templates**, and then select one of the language containers.
2. Double-click the specific template you want to view.
3. Select the **Templates** tab.



To add a Help file to one-off address templates, see "Selecting Template Help Files" earlier in this chapter.

Foreign Language Details and Addressing Templates

Microsoft Exchange Server supports multiple foreign language clients. During Setup, Microsoft Exchange Server installs details and addressing templates for the server's language. To support clients that don't use the same language as the server, you must enable the address detail display for the additional client languages.

Foreign language templates are provided on the Outlook compact disc for the client's language.

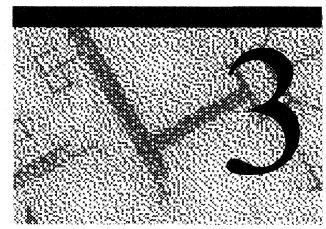
Installing a Template on a Microsoft Exchange Server Computer

To view address book information in the client's language, you must install the foreign language details and addressing templates on the Microsoft Exchange Server computer that is configured for the same language as the template.

1. In the Microsoft Exchange Server Administrator program, from the **Tools** menu, choose **Directory Import**.
2. Choose **Import File**.
3. In the templates directory on the Outlook compact disc for the language you want to support, select **Template.csv**.

CHAPTER 3

Advanced Security



Advanced security provides data integrity, proof of origin, and confidentiality. By using digital signatures, a person can "sign" a message so that the recipient can be sure that the message came from the indicated source and wasn't changed during transit. By using data encryption, a user can scramble data to ensure that only the intended recipient of the message can read it.

To enable advanced security features for Secure/Multipurpose Internet Mail Extension (S/MIME)-compatible clients and to use advanced security features of Microsoft Exchange Server, you can install the key management component on servers in your organization. This component is called the Key Management server (KM server). The KM server monitors all advanced security tasks.

It is recommended that you have only one KM server per organization even though you can configure advanced security on more than one server in your organization.

Setting up and maintaining advanced security involves:

- Selecting the server to manage the key management archive database.
- Installing and starting the key management component software and a Microsoft Certificate Server computer.
- Configuring advanced security on user mailboxes and the site.
- Viewing security logs.
- Backing up and maintaining the key management archive database.

KM Server Installation

The following tasks must be performed before setting up advanced security for a mailbox and a site:

- Install and start the KM server.
- Install and start the Microsoft Certificate Server computer.
- Install the Exchange policy module.

You install KM server using the **Complete/Custom** option in the Microsoft Exchange Server Setup program.

The KM server uses the Microsoft Certificate Server computer to certify public signing and encryption keys. Before installing Microsoft Certificate Server, you must have successfully installed Microsoft Internet Information Server (IIS) version 4.0 on a computer running Microsoft Windows NT Server version 4.0. Once installation of Microsoft Certificate Server is complete, you must install the Exchange policy module before the Microsoft Certificate Server computer can be used by KM server. The Exchange policy module enables the Microsoft Certificate Server computer to evaluate, accept, and issue certificate requests.

For more information on installing KM server, and setting up Microsoft Certificate Server and an Exchange policy module, see *Microsoft Exchange Server Getting Started.*

KM Server Configuration

Use the following guidelines when deciding which server to use as the KM server:

- Advanced security must be administered using the Microsoft Exchange Server Administrator program.
- The Administrator program must be running on a Microsoft Exchange Server computer that has remote procedure call (RPC) connectivity to the KM server.
- The server should be physically secure.
- The key management archive database should be backed up regularly.
- The server must be using the Microsoft Windows NT file system (NTFS) format for maximum security.

Starting the KM Server

Once you have installed the KM server, you must start the KM server to enable and configure security for individual users and the site. The KM server must be running at all times.

1. In Windows NT Control Panel, choose **Services**.
2. Double-click the Microsoft Exchange Key Management Server.
3. Under **Log On As**, select **This Account**.
4. Select the Microsoft Exchange Service account, and choose **OK**. See the service account under Microsoft Exchange Directory service if you're not sure what it is.
5. Place the disk with the password provided during Setup into the disk drive. The first time you start the KM server, the KM server password is **password**. If you did not copy the password to a disk during Setup, type the password Setup provided into the **Startup Parameters** box.
6. Select **Microsoft Exchange Key Manager**, and then choose **Start**.
7. If this is the first time you start the KM server, it is recommended that you change the advanced security administrator password as described in "Changing Your Advanced Security Administrator Password" later in this chapter.

Advanced Security Configuration

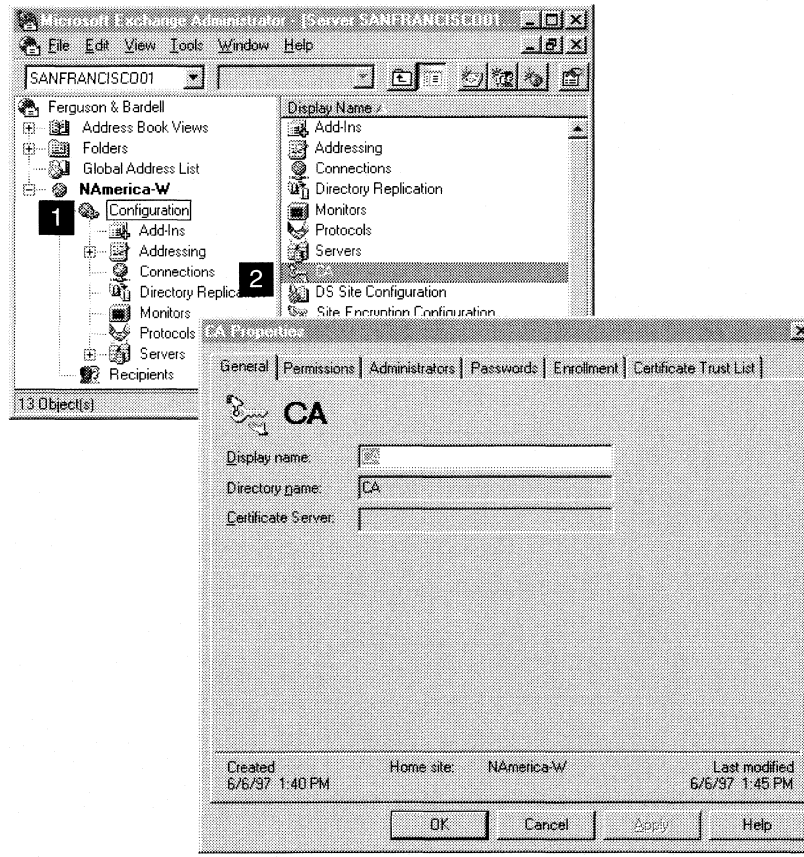
You administer advanced security for users by configuring the property pages in the CA object. You also administer advanced security for a site by configuring the property pages in the Site Encryption Configuration object. The property pages for configuring advanced security can be used to:

- View the name of the Microsoft Certificate Server computer.
- Assign permissions on the KM server for Windows NT user accounts.
- Add and remove KM server administrators, and change KM server administrator passwords.
- Set multiple password policies to recover and revoke user security keys and import or untrust another certification authority's certificate. Untrusting a certificate removes the trust placed in the certificate when it was imported.
- Enroll users in advanced security individually or in bulk.
- Issue certificates that are compatible with your environment.

- Import or untrust certificates from outside your organization that contain information necessary for digital signatures and encryption.
- View certificate trust list names, issuers, and expiration dates of outside organizations or certification authorities (CAs) that are currently certified on your Microsoft Exchange Server computer.

Getting to the CA property pages

1. In the Administrator window, choose **Configuration** in the site where the KM server is located.
2. Double-click **CA**.
3. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK** (if prompted). If this is the first time you are using KM server, the KM server password is **password**.



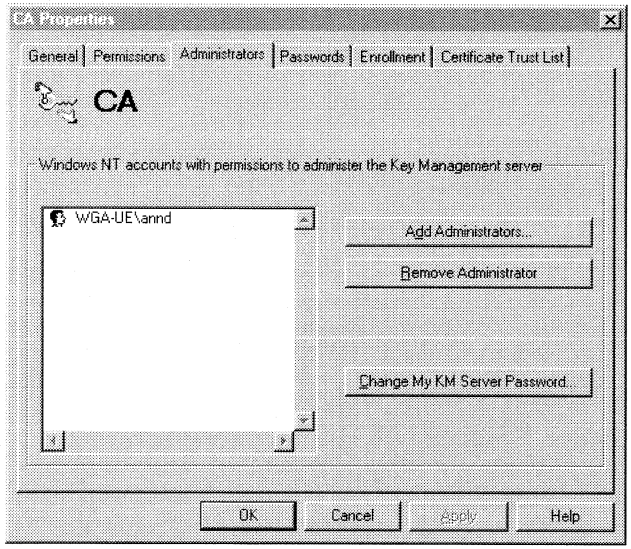
Administrators Properties

Use the **Administrators** property page to do the following tasks:

- View the Windows NT accounts that have permissions to administer the KM server.
- Add and remove administrators.
- Change an administrator's KM server password.

Getting to the Administrators property page

1. In the Administrator window, choose **Configuration** in the site where the KM server is located.
2. Double-click **CA**.
3. Select the **Administrators** tab.



Adding and Removing Advanced Security Administrators

You can make other administrators within your site advanced security administrators if you want to delegate the responsibility of setting up and maintaining advanced security to more than one person.

1. Select the **Administrators** tab.
2. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and then choose **OK**.
3. To add or remove in the list of advanced security administrators, select the name of the person.
4. Choose **Add Administrators** or **Remove Administrators**.
5. Choose **OK**, and then choose **Done**.

Changing Your Advanced Security Administrator Password

Each advanced security administrator has a password that must be entered before advanced security tasks can be performed. When you attempt to access or modify security information, the Administrator program prompts you to enter this password.

You are the only person who can change your security password. In general, it is a good idea for all security administrators to change their passwords occasionally. For example, if you suspect that your security password has been compromised, you should change it.

Note If you have never changed the password, the default password is **password**.

---

1. Select the **Administrators** tab.
2. Choose **Change My KM Server Password**.
3. Type the KM server password.
4. Type the current password and the new password, and then verify the new password.

Option	Description
Remember password for 5 minutes	Select to modify security for up to five minutes. Otherwise, you will be prompted for your password each time you try to open a user's **Security** property page or change security attributes.
Current password	Type your existing advanced security administrator password.
New password	Type your new password (case-sensitive).
Verify password	Retype the new password.

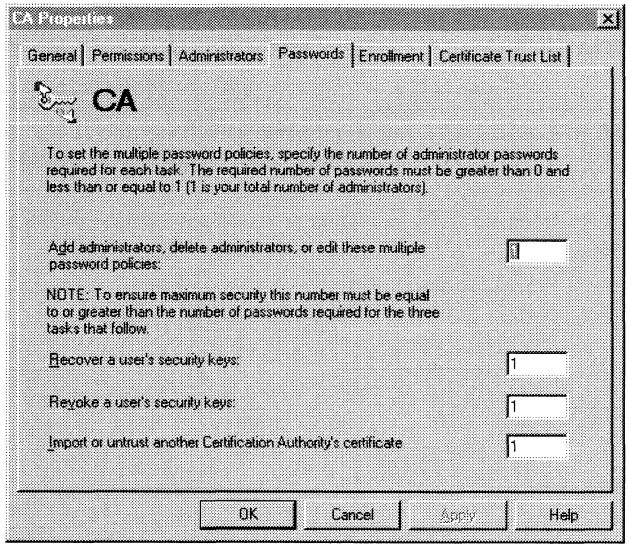
Passwords Properties

Use the **Passwords** property page to set multiple password policies. Multiple password policies prevent administrators from making changes to the KM server without the authorization of one or more other administrators. Multiple password policies enable a KM server site to specify the number of administrator passwords that are required to do the following tasks:

- Add or delete KM server administrators.
- Set multiple administrator passwords.
- Recover user security keys.
- Revoke user security keys.
- Import or untrust another certification authority's certificate.

Getting to the Passwords property page

1. In the Administrator window, choose **Configuration** in the site where the KM server is located, and double-click **CA**.
2. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK** (if prompted).
3. Select the **Passwords** tab.



Setting Multiple Administrator Passwords

You set a multiple password policy to require one or more administrators to perform certain tasks on the KM server. For example, you can set your KM server so that the cooperation of three administrators is necessary to recover or revoke a user's security key.

The first time you access the **Passwords** property page, only one administrator's password is needed. The default user name is the name of the current administrator. All user names are entered manually.

After you set the initial multiple password policies, the **Key Management Server Passwords** dialog box reflects the password policies by showing the required number of user names and administrator passwords required to perform a task. You must choose **Apply**, **OK**, or **Cancel** before leaving the **Passwords** property page to update password policies.

1. Select the **Passwords** tab.
2. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and then choose **OK** after each password.
3. Set the number of administrator passwords that must be entered for each option to perform advanced security tasks.

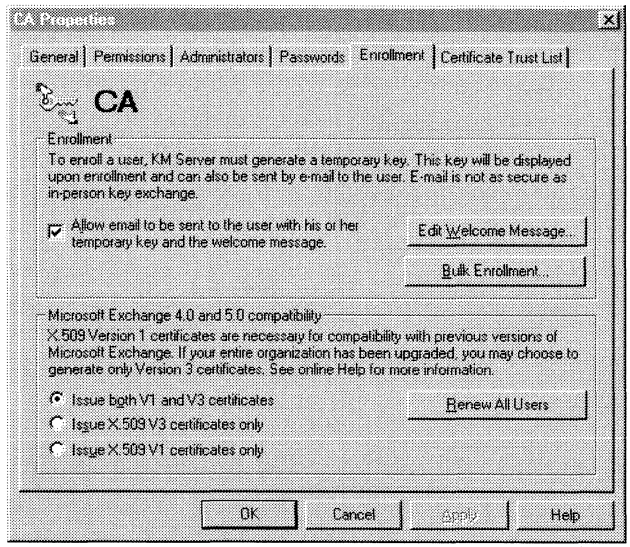
Option	Description
Add administrators, delete administrators, or edit these multiple password policies	Type the number of KM server administrators who will be required to add or delete administrators or to edit the **Passwords** property page. This number must be equal to or greater than the number of passwords required to perform the other tasks in the **Administrators** property page.
Recover a user's security keys	Type the number of KM server administrators required to recover a user's security keys.
Revoke a user's security keys	Type the number of KM server administrators required to revoke a user's security keys.
Import or untrust another Certification Authority's certificate	Type the number of KM server administrators required to import or untrust a certificate from another certification authority.

Enrollment Properties

Use the **Enrollment** property page to individually set the policies for transmitting temporary keys to users or to bulk enroll new users.

Getting to the Enrollment property page

1. In the Administrator window, choose **Configuration** in the site where the KM server is located, and double-click **CA**.
2. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK** (if prompted).
3. Select the **Enrollment** tab.



Transmitting Temporary Keys to Users

There are two ways you can transmit a temporary key to a user.

- Send the temporary key to the user through e-mail.
- Give the temporary key to the user in person.

If you choose not to send a user his or her temporary key using e-mail, you must give it to the user in person. Authenticate the user using private identification. For example, ask the user for a driver's license or social security number before giving out the temporary key.

Each time the KM server generates a temporary key, you can choose to send a message containing the temporary key.

1. Select the **Enrollment** tab.
2. In the **Key Management Server Passwords** box, type your advanced security administrator password, and then choose **OK**.
3. Select the **Allow email to be sent to the user with his or her temporary key and the welcome message** check box, and then choose **OK**.

   Selecting this check box sets the policy for allowing the temporary key to be sent to the user using e-mail. The message is sent when you enable advanced security in the **Security** property page of the user's mailbox.

For more information on enabling advanced security for users, see "Enabling Advanced Security for a Mailbox" later in this chapter.

Editing the Enrollment Welcome Message

If you selected the **Allow email to be sent to the user with his or her temporary key and the welcome message** check box in the **Enrollment** property page, then a temporary key is sent to the user in an e-mail when you enable advanced security message for that user's mailbox. You can customize the text of the enrollment welcome message. For example, you can include a description of your company's security policies.

The enrollment welcome message includes the name of the temporary key. You can delete the name of the temporary key from the message before sending the message to the user. For example, you can give users their temporary key in person. If you do so, you can send a generic message informing them that they should see the KM server administrator to obtain their temporary key.

1. Select the **Enrollment** tab.
2. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and then choose **OK**.
3. Choose **Edit Welcome Message** and modify the message appropriately. You can restore the default message by choosing **Default Settings**.

Enabling Advanced Security for Users in Bulk

Users must have security keys before they can enable advanced security on the client. You can generate security keys in bulk to save time when there are a large number of new users to enroll. You must still transmit the security keys to users individually, and each user must complete the process of enabling advanced security on the client.

Note Bulk enrollment of a large container can cause an increase in message traffic to the KM server.

---

1. Select the **Enrollment** tab.
2. In the **Key Management Server Passwords** box, type your advanced security administrator password, and then choose **OK**.
3. Choose **Bulk Enrollment**.
4. In the **Key Management Server Passwords** box, type your advanced security administrator password, and then choose **OK**.
5. Select the container and delivery option to enroll a group of users.

Option	Description
Container name	Displays the name of the container that contains the mailbox of users you want to enroll. The default is the **Recipients** container.
Modify	Selects a different container. Each container with users you want to enroll must be individually selected. Subcontainers are not included when you select a container.
Mail temporary keys to all newly enrolled users	Sends temporary keys to users through e-mail. Users who are being enrolled for the first time will receive their temporary key through e-mail.
Save results in a file	Writes information such as organization, site, and user name to a file that includes advanced security information for both new and users who were enrolled previously. This file enables you to obtain the status of a user's advanced security information quickly.

Issuing Certificates for Compatibility

Use the **Enrollment** property page to set policies for issuing certificates that are compatible with your site's client environment. A certificate is issued by a CA and binds the user's public key to the mailbox. In Microsoft Exchange Server, the CA is Microsoft Certificate Server, which issues, revokes, and renews digital certificates.

Microsoft Exchange Server supports the X.509 version 1 (V1) and the industry standard version 3 (V3) certificate formats. The certificate format you choose depends on the type of secure mail clients that your organization wants to support. You can choose to use one or both certificate formats. The V1 certificate format is necessary for compatibility with Microsoft Exchange Client versions 4.0 and 5.0, and Microsoft Outlook 8.0*x* clients. If your organization uses these clients, you must use the V1 format. If your organization uses an S/MIME-compatible client, you should also enable the V3 certificate format. If you are not using Microsoft Exchange Client versions 4.0 or 5.0, or Outlook 8.0 clients, then you can disable version 1 (V1) support.

The following describes the security formats supported for each client:

- Microsoft Exchange Client version 4.0 or 5.0 supports V1 certificates only.
- Outlook 8.0*x* client supports V1 certificates only.
- S/MIME-compatible clients support V1 or V3 certificates.

Certificates can be given a life span. This means that you can issue a certificate that expires after giving a user a certain number of days of access. The default life span of V1 and V3 certificates is 18 months. To change the life span, you must modify its span value on the Microsoft Certificate Server computer.

Note You can view the name of the Microsoft Certificate Server computer in the **General** property page of the CA object. The Microsoft Certificate Server computer name is created when the KM server is set up, and that the name cannot be modified.

---

1. Select the **Enrollment** tab.
2. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and choose **OK** after each password.
3. Choose the type of certificate you want to issue to all users.

Option	Description
Issue both V1 and V3 certificates	Issues both V1 and V3 certificates. You can issue both certificates if there are some users in your organization who are running Microsoft Exchange Client versions 4.0 and 5.0, or Outlook 8.0*x*.
Issue X.509 V3 certificates only	Issues only V3 certificates. You can use this format if all users in your organization are running an S/MIME-compatible client.
Issue X.509 V1 certificates only	Issues only V1 certificates. Choose this format if the majority of your clients are Microsoft Exchange Client version 4.0 or 5.0, or Outlook 8.0*x*, and you want to force your S/MIME-compatible clients to use only the backward-compatible mode. Choosing this format prevents S/MIME-compatible clients from choosing the S/MIME security format, which requires V3 certificates.
Renew all users	Notifies all users that they should initiate enrollment with the certificate type you have specified. You can also use this option to reset any changes you make to the security message format or the issuing of V1 and V3 certificates. For example, if you have changed the default security message format in the **Algorithms** property page, or if you have changed the type of V1 or V3 certificate to issue, you should choose **Renew all users**.

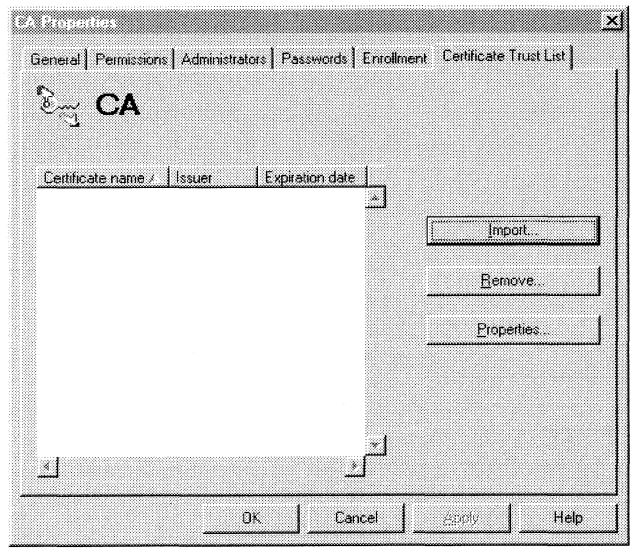
Certificate Trust List

A certificate trust list enables organizations to establish trust with other organizations so users can verify the digital signature of messages sent by users in other trusted organizations.

Use the **Certificate Trust List** property page to view other organizations that are currently certified on your Microsoft Exchange Server and to import certificates from outside of your organization. A certificate binds a public key to a particular certification authority.

Getting to the Certificate Trust List property page

1. In the Administrator window, choose **Configuration** in the site where the KM server is located.
2. Double-click **CA**.
3. Select the Certificate Trust List tab.



Importing Certificates

Importing certificates from another certification authority allows you to establish trust with another organization.

Use the **Certificate Trust List** property page to import a certificate from another organization. Importing certificates requires multiple administrator passwords if multiple password policies are set.

1. Select the **Certificate Trust List** tab.
2. Choose **Import**.
3. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and then choose **OK** after each password.
4. Select a certificate or a Certification Revocation List (CRL) to import, and then type the file name.

Option	Description
Import a certificate	Imports a certificate from another organization to the KM server. The certificate should be a .Crt file from a CA. You should have already received this certificate file from an outside organization.
Import a CRL	Imports a CRL to the KM server. The CRL contains a list of clients from a trusted organization that no longer hold valid security keys. It consists of the serial number of the certificate and the revocation date of the certificate. CRLs can be sent to you by e-mail or published on a Web page.
File name	Type the name of the file that contains the certificate or CRL you want to import.

Untrusting and Removing Certificates

A certificate from another certifying authority is trusted when you import it to your organization. You can use the **Certificate Trust List** property page to untrust or remove an imported certificate. Untrusting a certificate removes the trust placed in the certificate when it was imported. Removing a certificate deletes the certificate from your system but does not remove the trust placed in it. If you remove a certificate, you cannot untrust it later. Untrusting or removing certificates requires multiple administrator passwords if multiple password policies are set.

1. Select the **Certificate Trust List** tab.
2. Select a certificate and then choose **Remove**.
3. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and then choose **OK** after each password.
4. Select the method you want to use to remove the certificate.

Option	Description
Untrust certificate	Ensures you have a record of certificates that are untrusted from your KM server because the certificates are no longer valid.
Remove certificate	Removes the certificate from the KM server but does not add it to your CRL. Use this option with caution because a removed certificate cannot be untrusted. It is recommended that you use the **Untrust certificate** option to remove its trust, and then use the **Remove certificate** option to delete the certificate from your system.

Viewing Certificates

You can view the name, issuer, and expiration date of certificates that have been imported from other organizations and are trusted on your KM server. Use the **Certificate Trust List** property page to view the attributes of a certificate.

1. Select the **Certificate Trust** tab.
2. Select a certificate and then choose **Properties**.

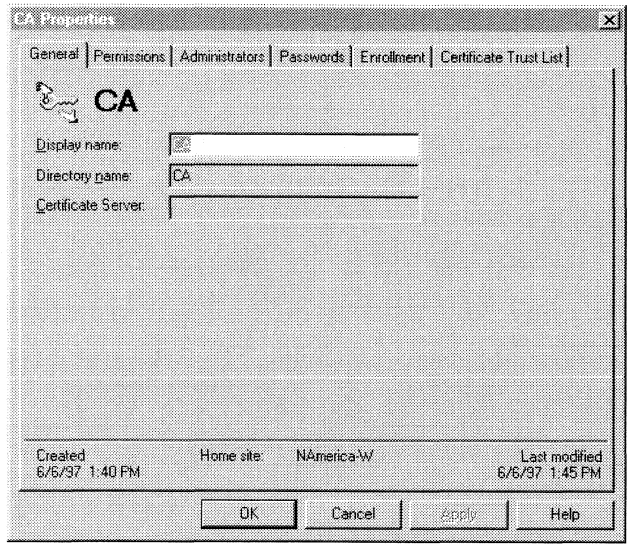
Property Page	Description
General	Shows the validity of a certificate.
Details	Shows who the certificate was issued to, the issuer, the friendly name, the creation and expiration dates, the serial number, the finger print, the algorithm, and the status.
Advanced	Shows details of the certificate's start date, expiration date, version, and intended use.

General Properties

Use the **General** property page to define the display name of the CA object that appears in the Administrator window. The directory name and the Microsoft Certificate Server computer name are created when the KM server is set up and they cannot be modified.

Getting to the General property page

1. In the Administrator window, choose **Configuration** in the site where the KM server is located, and double-click **CA**.
2. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK** (if prompted).
3. Select the **General** tab.



Defining the Display Name

Use the **General** property page to define the display name for the CA object.

1. Select the **General** tab.
2. Type the display name.

Option	Description
Display name	Type a maximum of 256 alphanumeric characters, which can include spaces and special characters. If no name is provided, the system prompts for a value.
Directory name	Displays the directory name of the CA object. This name is created during Microsoft Exchange Server Setup and cannot be modified.
Certificate Server	Displays the name of the Microsoft Certificate Server computer. This name is created during Microsoft Exchange Server Setup and cannot be modified.

CA Permissions

Use the **Permissions** property page to specify the rights that users or groups have on the CA object. You delegate permissions to a user or group by assigning them a role. Roles are sets of rights that define how much and what type of access a user or group has on an object. For the CA object, Microsoft Exchange Server provides Admin, Permissions Admin, and User default roles. You can also create custom roles.

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

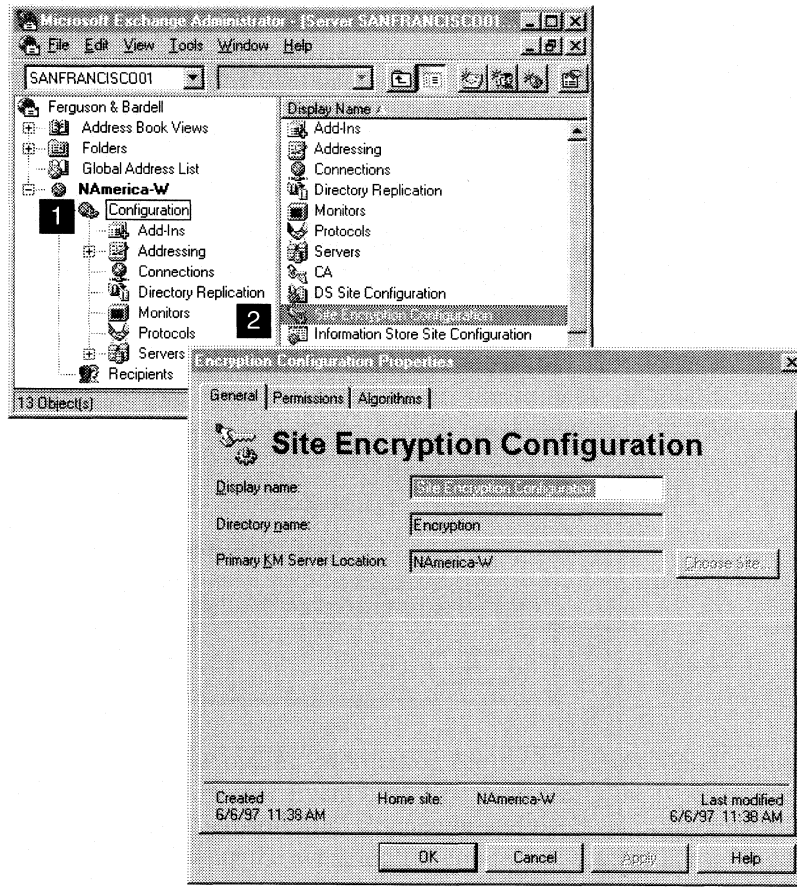
Site Security

After you have enrolled users in advanced security, you must configure security for your site. You can enable advanced security features in any site in your organization by configuring the property pages in the Site Encryption Configuration object. Use these property pages to perform the following tasks:

- View and select the KM server that you want to handle the advanced security requests for your site.
- Assign permissions on the KM server for Windows NT accounts.
- Select the type of encryption algorithms that the client will use to encrypt the contents of a message.

Getting to the Site Encryption property pages

1. In the Administrator window, choose **Configuration** in the site where the KM server is located.
2. Double-click **Site Encryption Configuration**.
3. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK** (if prompted).



General Properties for the Site

Use the **General** property page for the site to define the display name that appears in the Administrator window and to choose a site where you want to enable a KM server.

Getting to the General property page

1. In the Administrator window, choose **Configuration** in the site where the KM server is located.
2. Double-click **Site Encryption Configuration**.
3. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK** (if prompted).
4. Select the **General** tab.

Defining the Display Name

Use the **General** property page to define the display name for the Site Encryption Configuration object.

1. Select the **General** tab.
2. Type the display name.

Option	Description
Display name	Type a maximum of 256 alphanumeric characters, which can include spaces and special characters. If no name is provided, the system prompts for a value.
Directory name	Displays the directory name of the Site Encryption Configuration object. This name is created during Microsoft Exchange Server Setup and cannot be modified.
Primary KM Server Location	Displays the site location name of the KM server.

Choosing a Site

You can enable a site to use a KM server in another site.

1. Select the **General** tab.
2. Choose **Choose Site** and select a KM server to use in another site.

For more information on selecting a site to use a KM server, see "Enabling Additional Sites to Use the KM Server" later in this chapter.

Site Permissions

Use the **Permissions** property page to specify the rights that users or groups have on the Site Encryption Configuration object. You delegate permissions to a user or group by assigning them a role. Roles are sets of rights that define how much and what type of access a user or group has on an object. For the Site Encryption Configuration object, Microsoft Exchange Server provides Admin, Permissions Admin, and User default roles. You can also create custom roles.

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

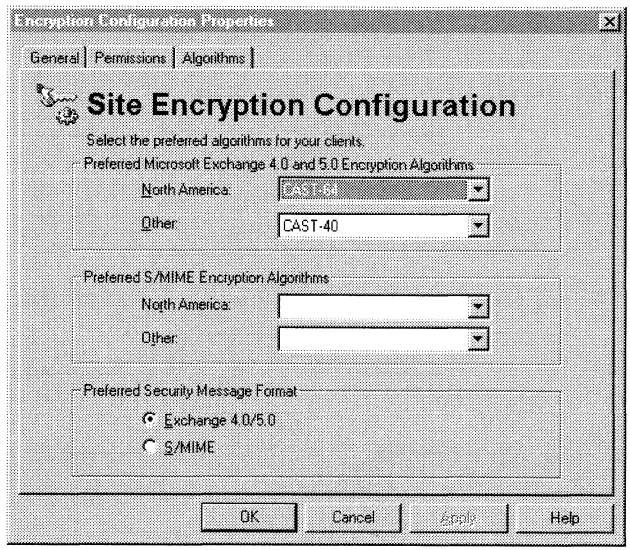
Algorithms

Use the **Algorithms** property page to specify the type of encryption algorithm and the security message format you want to use for your clients.

Note The selections you make on this property page can be modified later by users on the client.

Getting to the Algorithms property page

1. In the Administrator window, choose **Configuration** in the site where the KM server is located, and double-click **Site Encryption Configuration**.
2. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK** (if prompted).
3. Select the **Algorithms** tab.



Selecting an Encryption Algorithm

Microsoft Exchange Server supports several types of encryption algorithms for encrypting the content of messages.

Algorithms Compatible with Microsoft Exchange Server 4.0 and 5.0

Microsoft Exchange Server 4.0 and 5.0 can use one of the following encryption algorithms to encrypt the contents of a message: CAST-64, Data Encryption Standard (DES), and CAST-40. The North American version of the Microsoft Exchange Client supports all three algorithms. All other localized versions of the Microsoft Exchange Client support the CAST-40 algorithm.

Note You can change the North America preferred encryption algorithm from CAST-64 to DES and vice versa. However, you must renew all security-enabled users in the site where the change was made for the change to take effect. After you change the encryption algorithm, users can still read messages that were encrypted using the previous algorithm.

Algorithms Compatible with S/MIME

The preferred encryption algorithms that Microsoft Exchange Server can use to encrypt the content of messages using S/MIME algorithms are DES, 3DES, RC2-40, RC2-64, and RC2-128. S/MIME adds security to messages in Multipurpose Internet Mail Extensions (MIME) format. The security services offered are authentication (using digital signatures) and privacy (using encryption).

1. Select the **Algorithms** tab.
2. Under **Preferred Microsoft Exchange 4.0 and 5.0 Encryption Algorithms** or **Preferred S/MIME Encryption Algorithms**, select an encryption method for the geographic location.

Selecting a Preferred Security Message Format

Use the **Algorithms** property page to select the security message format for encrypting the content of messages. The selection of a preferred security message format is based on the configuration of clients in your site. For example, if your site primarily has computers running a client on 16-bit platforms, you can set the preferred security message format to **Exchange 4.0/5.0** so that users can read the content of encrypted messages.

Note The security message formats are default preferences for a user's mail client. Users can change the default preferences using their mail client. Set the format to the one that will be used by most clients. The profiles of other clients can be changed appropriately.

---

1. Select the **Algorithms** tab.
2. Under **Preferred Security Message Format**, select an encryption message format.

Option	Description
Exchange 4.0/5.0	Specifies the preferred security message format for your clients to be Microsoft Exchange Server 4.0 or 5.0. Select this option if your site primarily contains computers running the Microsoft Exchange Client on 16-bit platforms.
S/MIME	Specifies the preferred security message format for Outlook to be S/MIME. This option is the preferred industry standard.

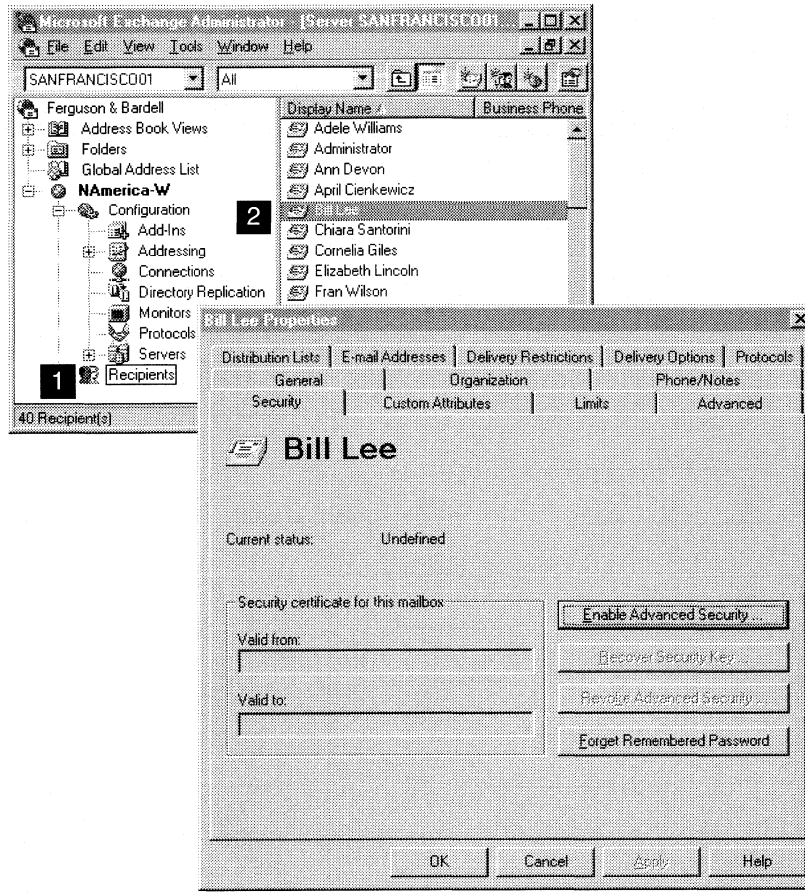
Mailbox Security Tasks

The following advanced security tasks must be performed in the **Security** property page of the user's mailbox.

- Enabling advanced security for a mailbox.
- Revoking advanced security for a mailbox.
- Recovering advanced security keys.
- Viewing mailbox security information.

Getting to the Security property page

1. In the Administrator window, choose **Recipients**.
2. Double-click a mailbox, and then select the **Security** tab.
3. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and then choose **OK** after each password.



Enabling Advanced Security for a Mailbox

When you enable advanced security for a mailbox, you give users temporary keys that are used to digitally sign and encrypt mail. A temporary key is used only once for a user to enroll in advanced security, and it secures the connection between the KM server and the client.

When you start the process of enrolling users in advanced security, an RPC is made to the KM server. The KM server generates a one-time temporary key and returns it to you. You must then transmit the temporary key to the user so the user can complete the advanced security process on the client.

A local private key file is created and can be copied to any computer that the user wants to use to digitally sign and encrypt mail.

Note The Administrator program must be running on a Microsoft Exchange Server computer that has RPC connectivity to the KM server.

1. Select the **Security** tab.
2. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and choose **OK** after each password.
3. Choose **Enable Advanced Security**.

   A dialog box appears prompting you to select the method you want to use to transmit the temporary key to the user.
4. Transmit the temporary key to the user in a secure manner.

Option	Description
Enable Advanced Security	Creates a temporary security key for users. Use a secure method to transmit temporary keys to users. Once users have this key, they must enable advanced security.
Security certificate for this mailbox	**Valid from** is the date on the client this certificate was created. **Valid to** is the date when the certificate expires. There are no tasks involved in extending certificates. After one year, users are prompted to initiate renewal of a certificate.
Send Enrollment Message	Sends an enrollment welcome message to the user through e-mail. A confirmation message showing the name of the temporary key is returned. You can select the text in the **Advanced security temporary key** box, but you cannot edit the text. You can edit the enrollment welcome message to enable you to customize the text of the message. If you delete the name of the temporary key from the enrollment welcome message, you must remember the name of the temporary key and give it to the user later. This option displays if you selected the **Allow email to be sent to the user with his or her temporary key and the welcome message** box in the **Enrollment** property page of the CA object.
Do Not Send E-mail	The temporary key is not sent to the user through e-mail. You must give the temporary key to the user in a secure manner. For example, you can give the temporary key to the user in person. This option displays if you selected the **Allow email to be sent to the user with his or her temporary key and the welcome message** box in the **Enrollment** property page of the CA object.

Revoking Advanced Security for a Mailbox

Revoking advanced security permanently disables the certificate for a mailbox. When security is revoked for a mailbox, anyone attempting to open an encrypted message previously sent from that mailbox is prompted with a warning stating that the message was secured with a revoked security certificate. The same things happens with a digital signature.

You should consider revoking advanced security when users leave their company or if users feel their security has been compromised because it appears someone is signing messages on their behalf or someone has gained access to their security file and password. You can enable security again by assigning a user another temporary key.

When you revoke security, the serial number of the certificate is added to a CRL. This list is stored in the Microsoft Exchange Server directory and the key management archive database. It is also stored on the client and is accessed each time a user attempts to verify the signature of a message. If the message is encrypted, the list is also accessed for each user in the recipient list of the encrypted message. If the originator's certificate is on the revocation list, the user is warned that the message is signed with a revoked certificate. Certificates remain on the revocation list until they expire, which is 18 months after security was first enabled for the user.

Limit the use of revocation. As the size of the revocation list increases, performance of advanced security is degraded.

1. Select the **Security** tab.
2. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and then choose **OK** after each password.
3. Choose **Revoke Advanced Security**.
4. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK**.

Option	Description
Revoke Advanced Security	Adds the serial number of the certificate to a revocation list.

Recovering Advanced Security Keys

You can reissue the security key for a mailbox if someone loses the password, or corrupts or removes the local security information for the mailbox. From the user's perspective, this process is identical to the initial task of setting up advanced security.

1. Select the **Security** tab.
2. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK**.
3. Choose **Recover Security Key**.
4. In the **Key Management Server Passwords** box, type the required number of advanced security administrator passwords, and then choose **OK** after each password.
5. Transmit the key to the user using a secure method.

   When users receive their temporary key, they should complete the advanced security process on the client.

Viewing Mailbox Security Information

You can view the status of mailbox security in the **Security** property page. It displays the status of security in the top portion of the property page for any mailbox.

1. Select the **Security** tab.
2. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK**.

Current status	Description
Undefined	Security has not been set up for this mailbox.
New	Security has been enabled for the first time, but the one-time temporary key has not been received from the client.
Active	Security has been enabled, and the one-time temporary key has been received from the client.
Disabled	Security has been disabled for this mailbox.
Key recovery in progress	A one-time temporary key has been reissued to this mailbox but not yet received, or a previously disabled mailbox is in the process of being enabled again.

Additional Advanced Security Tasks

Once you have configured advanced security for users and your site, you can also perform the following advanced security tasks:

- Enabling additional sites to use the KM server.
- Enabling security for users in remote sites.
- Backing up and restoring advanced security data.
- Viewing the security log.
- Moving users from one KM server to another.
- Moving the KM server from one site to another.

Enabling Additional Sites to Use the KM Server

You can enable advanced security in additional sites in your organization by configuring any server in the site. However, you should give careful consideration to how you configure advanced security when enabling additional KM servers in sites within your organization. Some configurations can result in the inability of users to recover their security key from the key management database.

Note The Site Encryption Configuration object can detect whether a KM server has been installed in another site based on the existence of the CA object in the Configuration container for that site. When you install the KM server, the CA object is created. Before configuring one Site Encryption Configuration object, verify that you can see the Configuration container for the other sites in your organization.

There are two scenarios that can occur when determining how to enable advanced security in additional sites:

- A KM server does not exist in the current site, and the Site Encryption Configuration object is not configured with a KM server (the **KM Server** box in the **General** property page of the Site Encryption Configuration object is blank).

  When you choose **Choose Site** in the **General** property page on the Site Encryption Configuration object, all KM servers in the organization are listed in the **Key Management Server** dialog box.

- A KM server does not exist in the current site, but the Site Encryption Configuration object has been configured with a KM server and you want to configure the Site Encryption Configuration object to point to another KM server.

  When you choose **Choose Site** in the **General** property page on the Site Encryption Configuration object, all KM servers in the organization are listed in the **Key Management Server** dialog box with the current KM server selected. If you select another KM server and choose **OK**, a message appears to warn you that security keys for existing users in your site may be unrecoverable if you configure the current site to use a different KM server.

Caution Configuring existing users in your site to use a different KM server is not recommended because security keys may be unrecoverable.

Complete the following procedure to enable advanced security in additional sites.

1. In the Administrator window, choose **Configuration** in the site where the KM server is located.
2. Double-click **Site Encryption Configuration**.
3. In the **Key Management Server Passwords** box, type the advanced security administrator password, and then choose **OK** (if prompted).
4. Select the **General** tab.
5. Choose **Choose Site**.
6. Select a site to enable a KM server.

Option	Description
Site name	Displays the name of the site where the KM server resides.
Server name	Displays the name of the KM server residing at a site in your organization.

Enabling Security for Users in Remote Sites

Because the Administrator program uses RPCs to communicate with the KM server to generate security keys, you cannot directly enable users in remote sites to use advanced security. If you are in a site without RPC connectivity to the KM server, you must contact an administrator in the site where the KM server is located and provide a list of user names that you want to enable for advanced security. In turn, the administrator at the site where the KM server is located enables each user to use advanced security (using the Administrator program). Once the security keys are generated, the administrator can either transmit them to you or directly to each user.

Note It is not necessary for each user to be in the same site as the KM server to enable advanced security on the client. Because the client and KM server communicate through e-mail, users in any site in your organization can complete the advanced security configuration process once they have a temporary key.

Backing Up and Restoring Advanced Security Data

Advanced security data is stored in the Kmsdata subdirectory where you installed the Microsoft Exchange Server. You can back up the advanced security data using the Windows NT Backup utility to back up all files and subdirectories in this directory. Stop the Microsoft Key Management Server service before performing the backup.

Caution You should periodically back up the Key Management archive database. If a user's security file is corrupted or a security logon password is forgotten, encrypted messages, including all previously encrypted messages, cannot be opened by the user. The key must be recovered as described in "Recovering Advanced Security Keys" earlier in this chapter, and the advanced security data must be current for this operation to succeed.

For more information, see your Windows NT documentation or *Microsoft Exchange Server Maintenance and Troubleshooting*.

Viewing the Security Log

Use the Windows NT Event Viewer to view an event of any significant occurrence requiring the administrator to be notified. Events for the KM server are logged in the Windows NT Event Log and include information about KM server functions.

For information about viewing security events, see *Microsoft Exchange Server Maintenance and Troubleshooting* or your Windows NT documentation.

Moving Users from One KM Server to Another

It is recommended that you do not move users from one KM Server to another because of the critical information kept in the key management database. The key management database is unique to each KM server. Moving users to another KM server can cause mail authentication and encryption errors if user security keys are lost. User security keys cannot be recovered if the user is moved to a new KM server.

The following scenarios describe the result of configuring and moving users to another KM server.

Scenario	Result
Single upgrade of a KM server in an organization and no installation of additional KM servers.	All sites continue to point to the single KM server that has been upgraded. The information kept in the key management database remains intact, so there is no risk of authentication and encryption errors occurring, or loss of user security keys.
Single upgrade of a KM server in an organization and the installation of additional KM servers in the organization.	All users in the site now point to the new KM server and must be enrolled in advanced security for the new KM server. Because the key management database is unique to each KM server and contains the security key history of all the users, the users pointing to the new KM server lose their ability to recover security keys from the KM server they were previously pointing to. This can result in mail that is encrypted with the user's previous security keys from becoming unreadable.
Clean installation of KM servers in an organization (no upgrade).	No key management databases have been established for the KM servers, so there is no potential for users to lose recovery of their security keys.
Clean installation of an extra KM server in a new site.	The site is new, so there is no need to move users.

If you want to move users to a new KM server in spite of the risk to recovering security keys, you should encourage all users moving to the new KM server to use the Bulk Advanced Security tool (Sectool.exe). This tool decrypts all mail for a user. After moving to the new KM server, users can encrypt all their mail again.

For information about enabling KM servers in additional sites, see "Enabling Additional Sites to Use the KM Server" earlier in this chapter.

For more information about using the Bulk Advanced Security tool, see Help for the Microsoft Exchange Server Resource Kit Tools (Exchtool.hlp) that is included on the *Microsoft BackOffice Resource Kit: Part One* compact disc.

Moving the KM Server from One Site to Another

It is recommended that you do not move the KM Server to another server in the same site because of the critical information kept in the key management database.

The original KM server disk is needed because it contains the 64-bit encryption key for the archive database. Because the data that is being moved was created with this encryption key, the encryption key needs to be present to issue and revoke certificates in the new location. If the original disk containing the encryption key is not used, new security keys must be issued for all users in the organization.

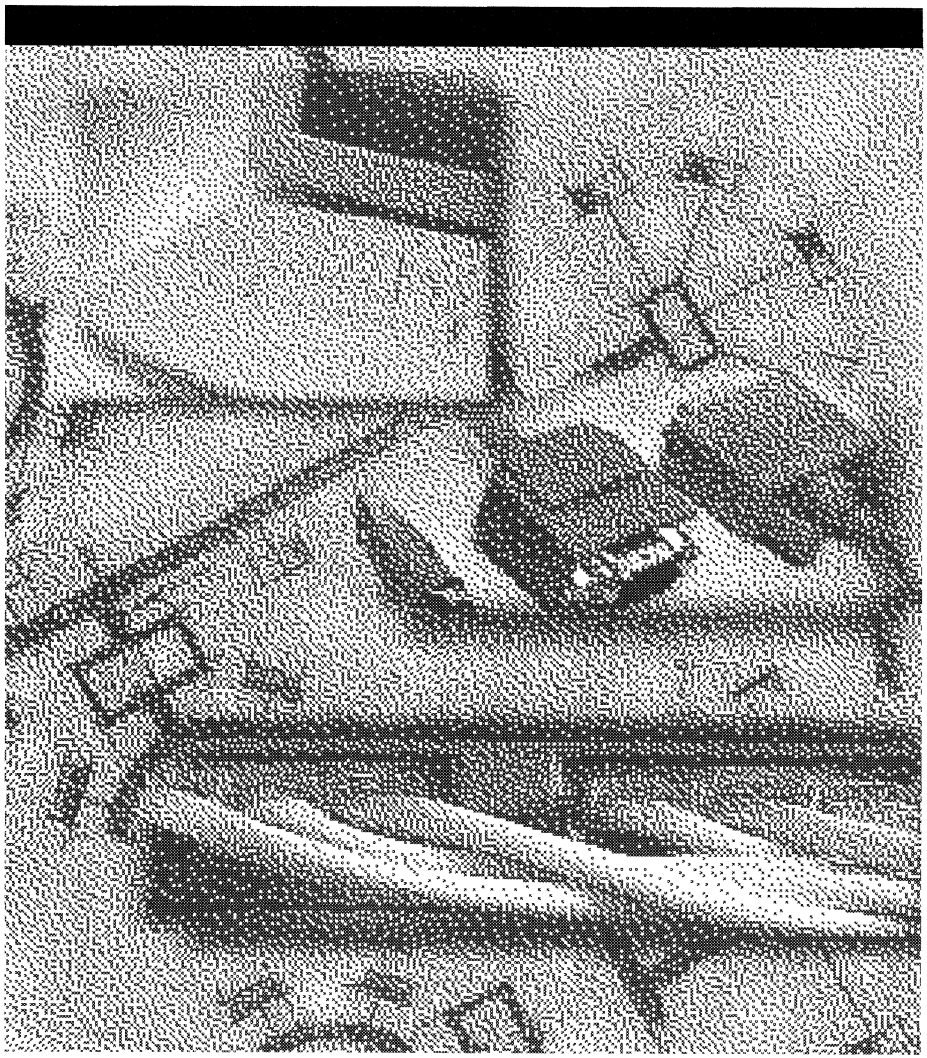
Before moving a KM server to another server, you should back up the key management database on the Microsoft Exchange Server computer that hosts the KM server. Also, you must stop the Microsoft Key Management service using the **Services** option in Control Panel. You must then complete the following procedures.

1. Run the Microsoft Exchange Server Setup program and remove the key management server component.

   This removes the KM server components, but retains the KM server directory and the key management database.
2. On the Microsoft Exchange Server computer that will host the KM server, run the Microsoft Exchange Server Setup program, and select the key management server component.
3. Use the **Services** option in **Control Panel** to stop the Microsoft Key Management service.
4. Restore the advanced security data on the server where you previously had the KM server.
5. Place the original KM server disk (from the original installation of the KM server) in the A drive and start the Microsoft Key Management service. You can also start the Key Management service from the command line.
6. After allowing for replication to occur within your organization (this could take several hours depending on your topology), configure advanced security features in the other site using the Site Encryption Configuration object.

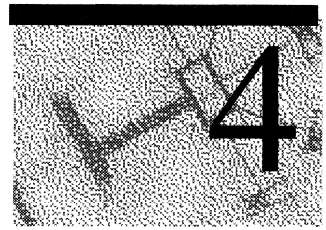
PART 2

Setting Up Connectors



CHAPTER 4

Address Spaces



Connectors and the Internet Mail Service are used to create paths for messages to be sent outside a site. These paths are represented by *address spaces.* An address space is a set of address components used by a connector or service to identify messages that it is responsible for processing.

This chapter describes how to create address spaces.

Address Space Configuration

Depending on the type of messages you are routing, you can create a corresponding address space type. This can be done in the **Address Space** property page of the connector responsible for routing messages. You can select X.400, Internet (SMTP), Microsoft Mail, or Other.

Getting to the Address Space property pages

1. In the Administrator window, choose **Connections**.
2. Double-click the connector to be modified.
3. Select the **Address Space** tab.
4. Choose **New**.
5. Choose an address type.

Depending on the address type you choose, see the appropriate section under "Address Space General Properties" later in this chapter.

For more information about addressing and routing, see *Microsoft Exchange Server Concepts and Planning.*

Address Space General Properties

The **General** property page for each address space type is a template to help you create address spaces. You can choose templates to create X.400, Internet (SMTP), Microsoft Mail, and other address spaces.

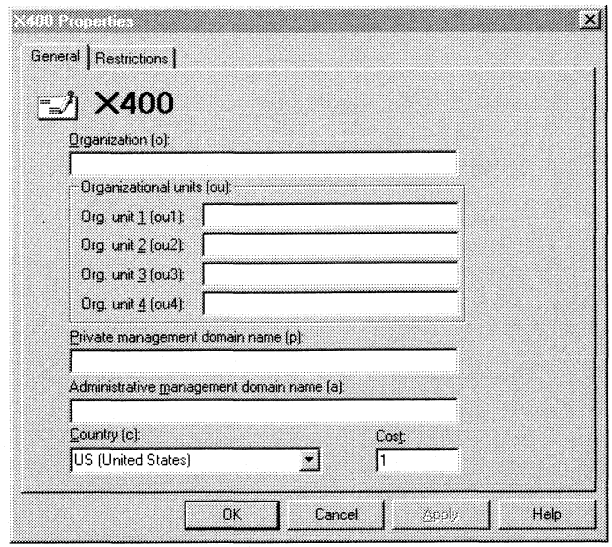
The cost associated with each address space is used to optimize outbound message routing but does not affect message reception. Routing costs range from 1 to 100. Lower cost routes take precedence over higher cost routes. If two or more routes are available with the same cost, the load placed on the routes is roughly equal.

For more information about routing costs, see *Microsoft Exchange Server Concepts and Planning*.

X.400 Address Spaces

Use the **General** property page as a template to create an X.400 address space.

Note An asterisk (*) can be used for a multicharacter wildcard in an address space. A percent symbol (%) can be used for a single character wildcard.



An X.400 address space contains the following information:

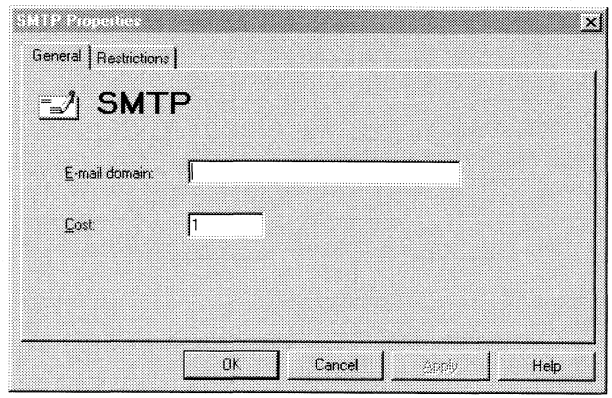
Address attribute	Description
Organization (o)	0 through 64 characters.
Org. unit 1 - 4 (ou1 - ou4)	0 through 32 characters.
Private management domain name (p)	1 through 16 characters.
Administrative management domain name (a)	1 through 16 characters.
Country (c)	2 characters or 3 digits.
Cost	A value from 1 to 100. Lower cost routes take precedence over higher cost routes.

The characters you use can vary according to the character set used by the connected system. However, characters must be printable strings. Address components are not case-sensitive, but case is preserved.

Internet (SMTP) Address Spaces

Use the **General** property page as a template to create an Internet (SMTP) address space.

Note An asterisk (*) can be used for a multicharacter wildcard in an address space. A percent symbol (%) can be used for a single character wildcard. Therefore, the percent symbol is not available for use as a character in the SMTP address.



An Internet (SMTP) address space contains the following information:

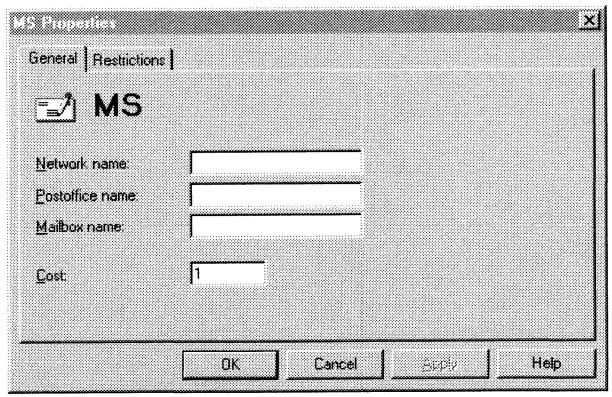
Address attribute	Description
E-mail domain	1 through 255 alphanumeric characters composed of one or more domain labels (up to 63 characters each), typically in the format *sitename.enterprisename.domain_suffix*. Use an asterisk (*) to indicate subdomains. An ending asterisk (*) is appended to the address space, but is not displayed.
Cost	A value from 1 to 100. Lower cost routes take precedence over higher cost routes.

For more information about routing costs, see *Microsoft Exchange Server Concepts and Planning*.

Microsoft Mail Address Spaces

Use the **General** property page as a template to create a Microsoft Mail address space.

Note An asterisk (*) can be used for a multicharacter wildcard in an address space. A percent symbol (%) can be used for a single character wildcard.



A Microsoft Mail address space contains the following information:

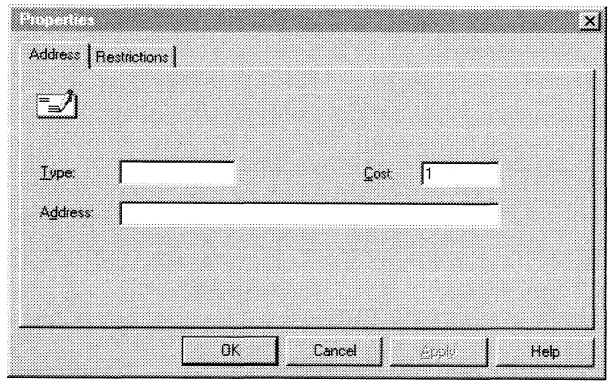
Address attribute	Description
Network name	1 through 10 capital alphanumeric characters.
Postoffice name	1 through 10 capital alphanumeric characters.
Mailbox name	The postoffice mailbox name on the remote Microsoft Mail system that you want to connect to.
Cost	A value from 1 to 100. Lower cost routes take precedence over higher cost routes.

For more information about routing costs, see *Microsoft Exchange Server Concepts and Planning*.

Other Address Spaces

You can configure an address type for which there is no template. Enter as much information as necessary to distinguish messages that should be sent through the connector.

Note An asterisk (*) can be used for a multicharacter wildcard in an address space. A percent symbol (%) can be used for a single character wildcard.



When creating a general address space entry, you should consider the following:

- A recipient address type and address space type must be identical before the address information is compared.

  For example, an e-mail address must be an SMTP type address before it is compared with an SMTP address space. In another example, a message sent with an MCIMail general address would not match an MCI general address space entry, so an e-mail type is required.

- Address information is examined from left to right and can include wildcard characters (* and ?). For example, if the address space type is fax! and an asterisk (*) is used for the address, the following address will be matched, as will any other entry that begins with fax!:

  ```
  fax!+19085551234  (/James Braun)  /delivery
  ```

The ? wildcard character specifies any single character, while the * wildcard specifies any number of characters that occur before a period (.), slash (/), colon (:), or at (@) character.

Tip Using a standard prefix (such as mcitelex: or 3com:) for the e-mail type and address space simplifies entering address information and message routing.

A general address space contains the following information:

Address attribute	Description
Type	A set of unique alphanumeric characters that identifies the system.
Address	A set of alphanumeric characters.
Cost	A value from 1 to 100. Lower cost routes take precedence over higher cost routes.

For more information about routing costs, see *Microsoft Exchange Server Concepts and Planning.*

Restrictions Properties

Use the **Restrictions** property page to control whether messages from an organization, a site, or a location can travel through the connector. Usually, address spaces are replicated to all Microsoft Exchange Servers, which allows each Microsoft Exchange Server to be aware of all connectors capable of processing messages of a specific address type. Use the **Restrictions** property page to prevent a connector from being available to the entire organization or site.

For example, an organization may have a site in Europe and a site in North America with connectors in both sites capable of transmitting messages of the Internet (SMTP) address type. Usually, when the North America server goes down, all SMTP messages are routed through the server in Europe. Using the **Restrictions** property page, you can prevent messages that originate in North America from using the connector in Europe.

You can use the location restriction to divide one site into multiple locations. For example, if North America and Europe are in the same site, you can divide the site into two geographic locations. This enables messages to be sent only to connectors within the same geographic location even though they are in the same site.

Getting to the Restrictions property page

1. In the Administrator window, choose **Connections**.
2. Double-click the connector to be modified.
3. Select the **Address Space** tab.
4. Select an address space or **New**.
5. Choose an address type.
6. Select the **Restrictions** tab.
7. Choose an option.

Option	Description
Organization	Messages of this address type that originated from any server in the organization are sent through this connector.
Site	Messages of this address type that originated from servers only in the connector server's site are sent through this connector.
Location	Messages of this address type that originated from servers only in the connector server's location are sent through this connector.

For information about defining locations, see *Microsoft Exchange Server Getting Started.*

CHAPTER 5

Internet Mail Service



Microsoft Exchange Server provides connectivity to the Internet and other systems using Simple Mail Transfer Protocol (SMTP). The connector, called the Microsoft Exchange Internet Mail Service, provides access and message exchange to and from any system that uses SMTP.

The Internet Mail Service is fully integrated with Microsoft Exchange Server and the Microsoft Windows NT Server. It is configured using the Microsoft Exchange Server Administrator program. You can administer the Internet Mail Service from any Windows NT Server that is part of your local area network (LAN).

Before You Begin

Before you install the Internet Mail Service, you should review the following list to ensure you have the environment configured correctly and you have the information needed to complete the Internet Mail wizard.

- For improved security and performance, the Internet Mail Service should be run on a Microsoft Windows NT Server using Windows NT file system (NTFS) rather than a file allocation table (FAT) file system.
- Know the addressing scheme for your organization.
- Determine the SMTP address for the site.
- Determine the address space the Internet Mail Service will service.
- Identify a recipient who will receive notifications if the Internet Mail Service fails.
- Obtain the host name and domain name of the computer on which the Internet Mail Service will be installed.
- Determine whether Domain Name System (DNS) will be used to provide host and domain name-to-Internet Protocol (IP) address resolution.
- Obtain the IP address of DNS servers or the SMTP hosts that will service the Internet Mail Service.

Installing the Internet Mail Service

To set up the Internet Mail Service for the minimum configuration requirements, use the following list of procedures in the order in which they appear.

Task	Description
Installing and configuring Transport Control Protocol/Internet Protocol (TCP/IP).	Install Windows NT TCP/IP, and specify the host and domain name. If DNS will be used, enter the IP address of the DNS servers.
Adding the Internet Mail Service computer to DNS.	If using DNS, add the host name, domain name and IP address to the DNS serving the Internet Mail Service computer.
Updating the Hosts file when not using DNS.	If not using DNS, use the Hosts file to specify the host name and IP address of the hosts to which the Internet Mail Service will forward mail.
Verifying the site address.	From the **Configuration** container in the Administrator window, select **Site Addressing**.
Running the Internet Mail wizard to install the Internet Mail Service.	From the **Connections** container in the Administrator program, choose **File**, **New Other**, and **Internet Mail Service**.
Testing the connection.	Test the connection to ensure that the Internet Mail Service is configured correctly.

Note When changes are made to the Internet Mail Service, you must stop the Internet Mail Service and then restart it for the changes to take effect.

Installing and Configuring TCP/IP

The Internet Mail Service uses Windows NT TCP/IP for its transport protocol. To use the Internet Mail Service, you must install Windows NT TCP/IP and specify the host name and domain name.

1. Select the Network icon in Control Panel.
2. Select the **Protocols** tab, choose **TCP/IP Protocol**, and then choose **Properties**.
3. Select the **DNS** tab.

4. Type the host name of the computer and the domain name where it resides. These elements create the fully qualified domain name (FQDN). You must associate the FQDN with the Internet Mail Service using an A record either in DNS or in the Hosts files of hosts that will connect to this Internet Mail Service.
5. If you are using DNS, type the IP address of one or more DNS servers in the **DNS Service Search Order** box. These are the DNS servers the Internet Mail Service queries to resolve domain names for outbound mail. Register the Internet Mail Service either with a DNS or in the Hosts file of an SMTP host.

   If DNS is not used, see "Updating the Hosts File When Not Using DNS" later in this chapter.

For information about installing TCP/IP, see your Microsoft Windows NT documentation.

Adding the Internet Mail Service Computer to DNS

You may have access to DNS through your Internet provider, or someone in your organization may be responsible for maintaining the DNS. This section will help you understand DNS terminology and how it is used with Microsoft Exchange Server.

You should be familiar with the following DNS terms:

A (address) records Contain the IP address and the FQDN of a computer, so the address in a message can be resolved and the message can be sent to the correct host. For example, if the host name in the TCP/IP configuration is *imshost*, the domain name in the TCP/IP configuration is *company.com*, and the IP address is 123.45.67.89, the A record in DNS would be:

```
imshost.company.com. IN A 123.45.67.89
```

MX (mail exchanger) records Used to point to one or more computers that will process mail for an organization or site. If the Microsoft Exchange Server SMTP site address is different from the host and domain name configured in TCP/IP, an MX record should be used to associate the address with an A record. For example, if the Microsoft Exchange Server site address is *exchange.company.com*, and the TCP/IP configuration specifies a host name of *imshost* and a domain name of *company.com*, the MX record would be:

```
exchange.company.com. IN MX 10 imshost.company.com.
```

Note Using both an A record and an MX record can result in faster name resolution.

- Add the host and domain name, and the IP address of the computer running the Internet Mail Service to DNS.

For more information about DNS, see *Microsoft Exchange Server Concepts and Planning*, your DNS administrator, Internet provider, or DNS documentation.

Updating the Hosts File When Not Using DNS

If you are not using DNS, you must use the local Hosts file to specify the IP address and the domain name of all hosts to which the Internet Mail Service will transfer messages. In addition, you must add the domain name and IP address of the Internet Mail Service computer to the Hosts file of all SMTP servers that will deliver mail to the Internet Mail Service. If the SMTP servers delivering mail to the Internet Mail Service are using DNS and the Internet Mail Service computer has entries in available DNS servers, the Hosts file does not need to be updated on those servers.

If you do not use DNS, use the **Connections** property page to list the hosts to which the Internet Mail Service will forward mail. The host names listed in the **Connections** property page must be listed in the Hosts file of the computer running the Internet Mail Service, unless you have listed hosts by IP address.

The Hosts file is located in the Winnt\System32\Drivers\Etc directory. The following is a sample entry in a Hosts file:

```
123.45.67.123      sales.fab.com
```

1. Add the IP address and the host and domain names to the local Hosts file.
2. Notify any SMTP hosts that will be forwarding mail to the Internet Mail Service so the Internet Mail Service host name, domain name, and IP address can be added to the SMTP Hosts file or to DNS.

Testing the Connection

When you finish configuring the Internet Mail Service and have started the service, you should test its operation before beginning general message transfer.

1. Send a message from your site to an SMTP server using an e-mail client.
2. Verify that the message arrives at the recipient's mailbox on the SMTP server.
3. Have someone send a message to your site from the SMTP server or reply to a message sent from you.
4. Verify that the message arrives.

If the message is delayed or does not arrive, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

Customizing the Internet Mail Service

You can customize the Internet Mail Service using various property pages. You must stop and restart the Internet Mail Service for changes to take effect.

Getting to the Internet Mail Service property pages

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.



Internet Mail Properties

Use the **Internet Mail** property page to configure the administrator's mailbox, message content, character sets, and message tracking.

Getting to the Internet Mail property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.
3. Select the **Internet Mail** tab.

Assigning an Administrator's Mailbox

Use the **Internet Mail** property page to assign an administrator's mailbox to receive error notifications and all messages delivered to the postmaster of this Internet Mail Service.

1. Select the **Internet Mail** tab.
2. Under **Administrator's Mailbox**, choose **Change**.
3. Select a recipient for the administrator's mailbox.

Option	Description
Show Names from the	Select the global address list or a container.
Type Name or Select from List	Type a name or select one from the list.
Properties	Display the properties for the recipient.
Find	Search for a name based on a specific set of criteria.

Setting Up Non-Delivery Report (NDR) Notifications

You can configure the Internet Mail Service to notify the administrator when non-delivery reports (NDRs) are generated by the Internet Mail Service. Use the **Internet Mail** property page to specify what types of NDRs will be reported to the administrator.

1. Select the **Internet Mail** tab.
2. Under **Administrator's Mailbox**, choose **Notifications**.
3. Select an option.

Option	Description
Always send notifications when non-delivery reports are generated	Select to send notifications to the administrator for all NDRs.
Send notifications for these non-delivery reports	Select to specify the types of NDRs the administrator will receive. By default, the **Multiple matches for an E-Mail address occurred** is the only option selected.

Specifying the Default Attachment Content Format

Use the **Internet Mail** property page to specify whether outbound messages with attachments will be encoded using Multipurpose Internet Mail Extensions (MIME) or uuencode. This option can be specified by e-mail domain. These settings override the default format.

Settings configured in client applications can override the default setting and the settings specified by e-mail domain. If the client specifies no content format option and no match is found in the e-mail domain options, the default setting will be used.

Note Message content should be set for **UUENCODE** when transferring messages to Microsoft Mail 3.*x* with Microsoft Mail Gateway to SMTP.

1. Select the **Internet Mail** tab.
2. Under Attachments (Outbound), select MIME or UUENCODE.
3. Choosing MIME means that all attachments will be encoded using MIME, except when the client software overrides the option. If a MIME message is delivered to a non-MIME-aware client, the attachment may not be usable.

Option	Description
Plain text	A plain text MIME body part is generated for the message. If **HTML** is also selected, Microsoft Exchange Server provides both Hypertext Markup Language (HTML) and plain text in a MIME multipart/alternative message.
HTML	A MIME body part in HTML is generated for the message. If **Plain text** is also selected, Microsoft Exchange Server provides both HTML and plain text in a MIME multipart/alternative message. HTML is an Internet standard that enables rich-text formatting such as bold, color, and italic to appear in messages.
Binhex	Renders the message body as text with any attachments encoded by the BinHex method, which is commonly used in the Macintosh operating system to encode 8-bit data transmitted on the Internet.

For more information about MIME and uuencode, see *Microsoft Exchange Server Concepts and Planning*. For more information about e-mail domain options, see "Specifying Message Content by E-mail Domain" later in this chapter.

Specifying the Default Character Sets

Use the **Internet Mail** property page to specify the default character set to be used when sending outbound and receiving inbound non-MIME messages. You can also specify the default character set for outbound MIME messages.

Note The Internet Mail Service should be configured to match remote SMTP hosts; otherwise, the characters that the recipient sees in the message may be misrepresented.

---

1. Select the **Internet Mail** tab.
2. In the **Character Sets** box, select the character set to be used with MIME and non-MIME messages.

Option	Description
MIME	For outbound messages, the setting is used only if the code page the message was composed in can map to more than one character set.
Non-MIME	For outbound messages, the setting is always used. For inbound messages, the setting is used no matter what the original character set was.

Enabling Rich Text for Outbound Messages

Use the **Internet Mail** property page to configure the Internet Mail Service to send outbound messages using Microsoft Exchange rich text character formatting such as bold, color, and italic. This option also allows preservation of attachment position and the ability to include OLE objects as message attachments.

The attachment information in uuencode mode is included in a file called Winmail.dat. In MIME mode, this information is included in a body part tagged using the MIME content type of application/ms-tnef. If the recipient is not a Messaging Application Programming Interface (MAPI) client and rich text is enabled, the recipient may complain about receiving these attachments. To avoid this situation, use one of the following methods:

- Disable rich text for the domain of non-MAPI recipients.
- Disable rich text for each custom recipient.
- Disable rich text in the sender's personal address book (PAB) entry for the recipient.
- Disable rich text for the Internet Mail Service.

When the Internet Mail Service is used as a site connector, this option should be set to **Always** or **User**. Rich text should always be enabled when transferring messages to the Microsoft Mail Gateway to SMTP.

Note To set the Microsoft Exchange rich text for custom recipients, use the **Advanced** property page for custom recipients.

---

1. Select the **Internet Mail** tab.
2. Choose **Advanced Options**.
3. In the Send Microsoft Exchange rich text formatting box, select User, Always, or Never.

Option	Description
Always	Always send Microsoft Exchange rich text regardless of how the recipient is configured in the sender's PAB or how the recipient is defined as a custom recipient.
User	Send Microsoft Exchange rich text only when enabled for the recipient. This is the default.
Never	Never send Microsoft Exchange rich text regardless of how the recipient is configured in the sender's PAB or how the recipient is defined as a custom recipient.

For information about setting these options by e-mail domain, see "Specifying Message Content by E-mail Domain" later in this chapter.

Disabling Out-Of-Office Responses

Some client applications can be configured to automatically generate replies to messages received while out of the office. You can stop out-of-office replies from being sent to the Internet.

1. Select the **Internet Mail** tab.
2. Choose **Advanced Options**.
3. Select or clear **Disable Out of Office responses to the Internet**. Select this to stop out-of-office responses to the Internet. This is the default. Clear to allow out-of-office responses to the Internet.

For information about setting these options by e-mail domain, see "Specifying Message Content by E-mail Domain" later in this chapter.

Disabling Automatic Replies to the Internet

Some client applications can be configured to automatically generate replies to messages. You can stop these messages from going to the Internet using the option in the **Internet Mail** property page.

1. Select the **Internet Mail** tab.
2. Choose **Advanced Options**.
3. Select or clear **Disable Automatic Replies to the Internet**. Select this to suppress automatic replies to messages received by the Internet Mail Service. This is the default. Clear to allow automatic replies returned to the Internet.

For information about setting these options by e-mail domain, see "Specifying Message Content by E-mail Domain" later in this chapter.

Disabling Display Names for Outbound Messages

The Internet Mail Service can be configured to send outbound messages with the sender's display name in addition to the sender's e-mail address. The display name is usually the full name of the sender. For example, Bill Lee's e-mail address might be billl@fab.com, and his display name Bill Lee.

Use the **Internet Mail** property page to enable or disable sending display names with outbound messages. To view the display name for a recipient, use the recipients container **E-mail Addresses** property page.

1. Select the **Internet Mail** tab.
2. Choose Advanced Options.
3. Select or clear **Disable sending Display names to the Internet**. Clear this to enable display names for messages sent through the Internet Mail Service. This is the default. Select to disable display names for messages sent through the Internet Mail Service.

For information about setting these options by e-mail domain, see "Specifying Message Content by E-mail Domain" later in this chapter.

Specifying Message Content by E-mail Domain

If you want to use different encoding methods, character sets, and message sizes for individual domains, use the **E-Mail Domain** option in the **Internet Mail** property page. These settings will override the default message content information and allow you to configure individual domains separately.

For example, you may want to use the MIME encoding method for the subdomain *sales.fab.com* and the uuencode encoding method for the domain *fab.com.* To do this, list the subdomain before the domain.

Note Uuencode and rich text should be specified when transferring messages to the Microsoft Mail Gateway to SMTP.

---

1. Select the **Internet Mail** tab.
2. Choose **E-Mail Domain**.
3. In the **E-Mail Domain** dialog box, choose **Add**.
4. Select the maximum message size, attachment encoding method, and character set options for this domain.

Option	Description
E-Mail Domain	Type the domain name. Subdomains and FQDNs are allowed. IP addresses and wildcard characters are not allowed. The Internet Mail Service will search the list starting at the top and will move down until a match is found. Therefore, subdomains should be listed before domains.
Maximum message size	Specify the maximum number of kilobytes (KB) for outbound messages or select **No limit**. The maximum message size specified in the **General** property page of the Internet Mail Service takes precedence if it is lower than this value.
Attachments (outbound)	Select an encoding method for message attachments. Settings chosen in the client may override this option. If the client specifies none, and a domain match is not found, the Internet Mail Service default encoding method will be used.
Advanced Options	Choose whether to specify options such as Microsoft Exchange rich text, word-wrap, and automatic replies.
Character Sets	Select the character sets that will be used for content conversion.

For more information about setting the maximum message size, see "Specifying the Maximum Message Size" later in this chapter. For more information about content format, see "Specifying the Default Attachment Content Format" earlier in this chapter. For more information about character sets, see "Specifying the Default Character Set" earlier in this chapter. For more information about rich text, see "Enabling Rich Text for Outbound Messages" earlier in this chapter. For more information about automatic replies, see "Disabling Out-of-Office Responses" and "Disabling Automatic Replies to the Internet" earlier in this chapter.

Specifying a Fixed-width Font

You can use the **Internet Mail** property page to enable inbound messages to display using fixed-width characters such as Courier. This is useful when text needs to be aligned in columns.

1. Select the **Internet Mail** tab.
2. Select **Convert inbound message to fixed-width font**.

Disabling Client S/MIME Support

You can use the **Internet Mail** property page to convert multipart/signed messages to unsigned MIME messages. This is useful when mailboxes are being accessed using client software that does not support multipart/signed message format.

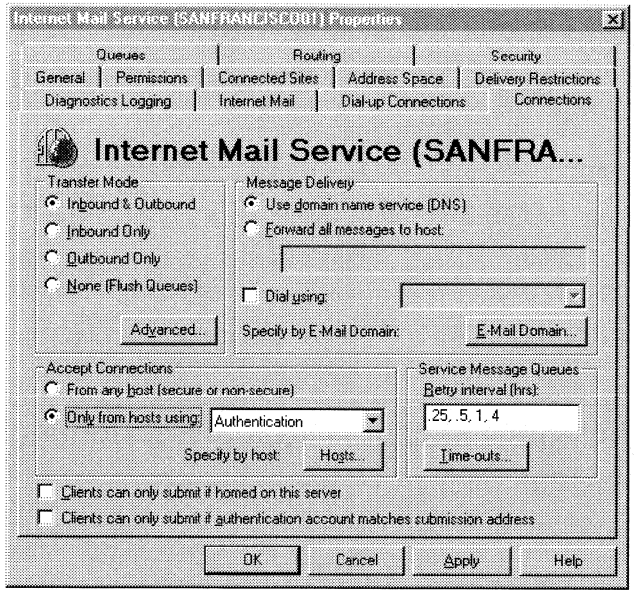
1. Select the **Internet Mail** tab.
2. Clear Clients support S/MIME signatures.

Connections Properties

Use the **Connections** property page to configure transfer mode, message delivery, connection acceptance, security, retry interval, and message time-out options for the Internet Mail Service.

Getting to the Connections property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.
3. Select the **Connections** tab.



Specifying Inbound and Outbound Transfer Modes

Use the **Connections** property page to configure the Internet Mail Service to accept inbound messages, send outbound messages, both, or neither. In an organization using one Internet Mail Service, you set the transfer mode to both send and receive messages. In an organization using multiple Internet Mail Services, you can balance responsibility for sending and receiving messages among the services. Use the **None** option when you want to suspend further message activity when preparing to remove or move the Internet Mail Service.

Note Setting the transfer mode to **Inbound Only** will not prevent outbound messages from being queued to this Internet Mail Service. To prevent outbound messages from being queued to this Internet Mail Service, remove the address spaces from the **Address Space** property page.

---

1. Select the **Connections** tab.
2. Under Transfer Mode, select Inbound & Outbound, Inbound Only, Outbound Only, or None.

Option	Description
Inbound & Outbound	Accept inbound and attempt outbound connections.
Inbound Only	Only accept inbound connections.
Outbound Only	Only attempt outbound connections.
None (Flush Queues)	Do not accept inbound connections. Pending messages are delivered.

Defining the Maximum Number of Connections and Messages Sent

Use the **Connections** property page to specify the maximum number of inbound and outbound connections the Internet Mail Service will accept and initiate respectively at one time. You can also define the maximum number of messages sent during each connection and adjust the number of connections and messages based on resources available in your environment. Some mail systems can accept only one connection at a time. The maximum number of combined inbound and outbound connections cannot exceed 1,000.

Note Setting the maximum number of inbound and outbound connections to 0 does not stop the Internet Mail Service from accepting inbound or attempting outbound connections. For more information, see "Specifying Inbound and Outbound Transfer Modes" earlier in this chapter.

If you have a server supporting Post Office Protocol version 3 (POP3) or Internet Message Access Protocol Version 4rev1 (IMAP4) clients, you may need to increase the maximum number of simultaneous SMTP connections. POP3 and IMAP4 clients need to create an SMTP connection to the Internet Mail Service to send mail, but the number of simultaneous connections required varies based on the number and type of POP3 and IMAP4 clients.

Tip Use the Windows NT Performance Monitor to view current connections.

1. Select the **Connections** tab.
2. Under Transfer Mode, choose Advanced.
3. Type a number in the appropriate box.

Option	Description
Max no. of Inbound Connections	The maximum number of inbound connections the Internet Mail Service can accept at one time.
Max no. of Outbound Connections	The maximum number of outbound connections the Internet Mail Service can make at one time.
Max no. of Connections to a single host	The maximum number of connections the Internet Mail Service can make to a single host at one time.
Max no. of Messages sent in a connection	The maximum number of messages to be sent during each outbound connection.
Reset default values	Return all options to default settings.

Delivering Messages Using DNS

Use the **Connections** property page to specify whether all outbound messages will be routed using the routing information in the DNS. This is the default. Domains specified in outbound messages will be looked up in DNS. If the domain is found in DNS, the message will be delivered to the corresponding IP address. If the domain is not found, the message will be returned to the sender with an NDR.

1. Select the **Connections** tab.
2. Under **Message Delivery**, select **Use domain name service (DNS)** to route all outbound messages using DNS queries. This also includes using a Hosts file or Windows Internet Naming System (WINS).
3. Select **Dial using** if you reach hosts by using a dial-up connection. Choose one of the dial-up connections specified on the **Dial-up Connections** property page.

For information about specifying message delivery by e-mail domain, see "Delivering Messages by E-mail Domain" later in this chapter. For more information about DNS, see *Microsoft Exchange Server Concepts and Planning*.

Delivering All Messages to a Single Host

Use the **Connections** property page to specify that all outbound messages be sent to a single host. If message delivery by e-mail domain is not specified, the message is delivered using the option specified in the **Message Delivery** section of the **Connections** property page.

Note If the domain name of a host is specified, the domain name must be defined in the local Windows NT Server Hosts file or in the DNS. Otherwise, the Internet Mail Service will not start.

---

1. Select the **Connections** tab.
2. Select **Forward all messages to host**, and then type the IP address or host and domain name of the SMTP host. Use the IP address rather than the computer name for the best performance.

   This option can be configured to process SMTP mail messages in a round-robin style. For example, you can type a comma-separated list of multiple hosts: host1,host2,host3. The first message will be sent to host1, the second message to host2, the third message to host3, the fourth message to host1, and so on.
3. Select **Dial using** if you reach the host using a dial-up connection. Choose one of the dial-up connections specified on the **Dial-up Connections** property page.

For information about specifying message delivery by e-mail domain, see "Delivering Messages by E-mail Domain" later in this chapter.

Delivering Messages by E-mail Domain

Use the **Connections** property page to define the way messages will be delivered to the destination.

Note This setting overrides the option you specified under **Message Delivery**.

---

1. Select the **Connections** tab.
2. Under Message Delivery, choose E-Mail Domain.
3. Choose **Add**.
4. Type the e-mail domain name and specify whether messages will be delivered using DNS or to a specific host.

Option	Description
E-Mail Domain	Type the domain name for which you will specify delivery options. Do not use an ending period after the FQDN.
Use DNS	Select when messages to the specified domain should be delivered using DNS queries.
Forward all messages for this domain to host	Type the host name or IP address of the SMTP host that will process messages for the specified domain. If any host name cannot be resolved, the Internet Mail Service will not start and a Windows NT Event Log message will be generated. This option can be configured to process SMTP mail messages in a round-robin style. For example, you can type a comma-separated list of multiple hosts: host1,host2,host3. The first message will be sent to host1, the second message to host2, the third message to host3, the fourth message to host1, and so on.
Dial using	Select to use a dial-up connection. Choose one of the dial-up connections specified on the **Dial-up Connections** property page.

For more information about message delivery, see "Delivering Messages Using DNS" and "Delivering All Messages to a Single Host" earlier in this chapter.

Accepting Connections from All Hosts

Use the **Connections** property page to accept connections from all secure and non-secure hosts. This is enabled by default.

1. Select the **Connections** tab.
2. Under **Accept Connections**, select **From any host (secure or non-secure)**.

Accepting Connections from Secure Hosts

Use the **Connections** property page to accept connections only from hosts using authentication or encryption.

1. Select the **Connections** tab.
2. Under **Accept Connections**, select **Only from hosts using**.
3. Choose **Authentication**, **Encryption**, or **Auth and Encrypt**.

Accepting Connections from Specific Hosts

Use the **Connections** property page to reject incoming SMTP connections from a single IP address or range of IP addresses. You can specify a range of addresses to reject and make a list of addresses that will be excluded from the restriction. To do this, specify the hosts from which you will accept mail higher in the list than the more general range of hosts from which connections will be rejected.

1. Select the **Connections** tab.
2. Under Accept Connections, choose Hosts.
3. To add or modify a host, choose **Add** or **Edit**.
4. Identify the host by entering the IP address and mask, and then choose an option. Choose **OK** to return to the **Specify Hosts** dialog box.

Option	Description
IP Address	Type the IP address of the SMTP hosts that will be accepted or rejected. Use of wildcards is accomplished using the **Mask** field. If you are specifying only a single IP address to be rejected, you do not need to use the **Mask** field.
Mask	Type the IP address mask. To control access, the IP address specified is matched against the IP address of the host that is connecting to the Internet Mail Service. The mask specifies which bits are relevant in the match. In Boolean logic, this is equivalent to exclusive-oring the addresses and then anding the result with the mask. If the result is zero, it is a match. For example: IP 192.11.154.0 Mask: 255.255.255.0 Therefore, any IP address in 192.11.154.*n* would match, where *n* = 1-254.
Accept connections from this host	Select to allow the specified host to connect to the Internet Mail Service computer.
Only accept from this host if it uses	Select to accept connections from hosts using security. Choose **Authentication**, **Encryption** or **Auth and Encrypt**.
Reject connections from this host	Select to indicate that the specified host is not allowed to connect to the Internet Mail Service computer.
This host is a relay server	Select to override client security requirements in the **Connections** property page.

5. In the **Specify Hosts** dialog box, choose an option to identify which clients can submit messages.

Option	Description
Clients can only submit if homed on this server	Select to allow clients to submit messages only if they have a mailbox on this server.
Clients can only submit if authentication account matches submission address	Select to allow clients to submit messages only if their logon account matches the address in the **From** field of the message.

Setting the Retry Interval

The Internet Mail Service can be set to wait a specified number of hours before retrying a host to which a previous connection attempt has failed. If the Internet Mail Service attempts to deliver a message to an SMTP host for which it has obtained an IP address and does not receive a response from the host, the connector attempts to reconnect after the period of time specified in the **Retry interval** box.

The first number in the list determines the time the Internet Mail Service will wait between the initial delivery attempt and the first retry. The second number is the amount of time the Internet Mail Service will wait between the first retry and the second retry, and so on. The last specified time interval will be repeated until either the connection is made or the specified time-out value has been reached.

1. Select the **Connections** tab.
2. Under **Connector Message Queues**, type the number of hours the Internet Mail Service will attempt subsequent connections.

Option	Description
Retry interval (hrs)	The number of hours to wait before retrying a connection to a host to which delivery has previously been attempted. Values are separated by commas. Periods may be used to indicate partial hours. No spaces are allowed. The default is .25, .5, 1, 4.

For more information about time-out values, see "Specifying Message Time-out Values" later in this chapter.

Specifying Message Time-out Values

Message time-out values can be specified for urgent (high importance), normal, and non-urgent (low importance) messages. If the time-out is reached before the message can be sent, the sender is notified with an NDR, and the message is not sent.

1. Select the **Connections** tab.
2. Under Service Message Queues, choose Time-outs.
3. Type message time-out values in the appropriate boxes.

Option	Description
Urgent message timeout (hrs)	The maximum amount of time the Internet Mail Service will try to send a message of high importance. The default is 24 hours. The maximum value is 999.
Normal message timeout (hrs)	The maximum amount of time the Internet Mail Service will try to send a message of normal importance. The default is 48 hours. The maximum value is 999.
Non-urgent message timeout (hrs)	The maximum amount of time the Internet Mail Service will try to send a message of low importance. The default is 72 hours. The maximum value is 999.

Controlling Notifications for Queued Mail

The Internet Mail Service notifies the sender when an outbound message has been queued beyond the time specified in the **Connections** property page. You can disable notification. The default is to notify the sender only for queued mail of high importance.

1. Select the **Connections** tab.
2. Under **Service Message Queues**, choose **Time-outs**.
3. Select **Notify sender for queued mail**, and then select the check box for the type of mail for which the sender will be notified.
4. Type the number of hours that will elapse before notification.

Option	Description
Urgent mail every (hrs)	Select to enable notification for messages of high importance. This is the default. Type a value for the number of hours before notification. The default is 4 hours.
Normal mail every (hrs)	Select to enable notification for messages of normal importance. Type a value for the number of hours before notification. When selected, the default is 12 hours.
Non-urgent mail every (hrs)	Select to enable notification for messages of low importance. Type a value for the number of hours before notification. When selected, the default is 24 hours.

Connected Sites Properties

When the Internet Mail Service is used to connect to an existing Microsoft Exchange Server site, use the **Connected Sites** property page to ensure directory replication can take place and that other connectors in the organization can be accessed.

Note Connected sites should list all sites that will receive mail through this Internet Mail Service, regardless of direct or indirect connection to the connector. Knowledge of all other sites are inherited automatically through directory replication.

Getting to the Connected Sites property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.
3. Select the **Connected Sites** tab.

Creating a New Connected Site

Use the **Connected Sites** property page to set up or modify an Internet Mail Service connection to another site.

1. Select the **Connected Sites** tab.
2. Choose **New**.
3. Type the organization name and site name.

Option	Description
Organization	The directory name of the organization.
Site	The name of the site that will be connected.

Specifying the Routing Address for Connected Sites

Use the **Routing Address** property page to provide the FQDN of the Internet Mail Service that will receive mail for the site you are currently configuring. The Internet Mail Service encapsulates the distinguished name (DN) on the message, adds an @ sign, and then appends the routing address to create an FQDN for the SMTP address.

For example, the DN might be o=FAB ou=site cn=bill. Because this is not a valid SMTP address, the Internet Mail Service encapsulates the address.

Note If you route other address types through this Internet Mail Service (for example, by using the Microsoft Mail address type), do not prefix the SMTP routing address with an at sign (@). If you do, mail to this address type is not routed.

When you add a site to the list of connected sites, messages are sent to the site that is directly connected by this Internet Mail Service. The directly connected remote site then forwards messages to the final destination (which can be several hops away).

---

1. Select the **Connected Sites** tab.
2. Choose **New** or the site to be modified.
3. Select the **Routing Address** tab.
4. Type the **Type**, **Cost**, and **Address**.

Option	Description
Type	The address type is SMTP.
Address	The details of the address that you want appended to the message. This is the domain name or FQDN of the SMTP host, or Internet Mail Service at another Microsoft Exchange Server site.
Cost	The value associated with sending to this address, connector, or SMTP host. It can be a number between 1 and 100. The default is 1.

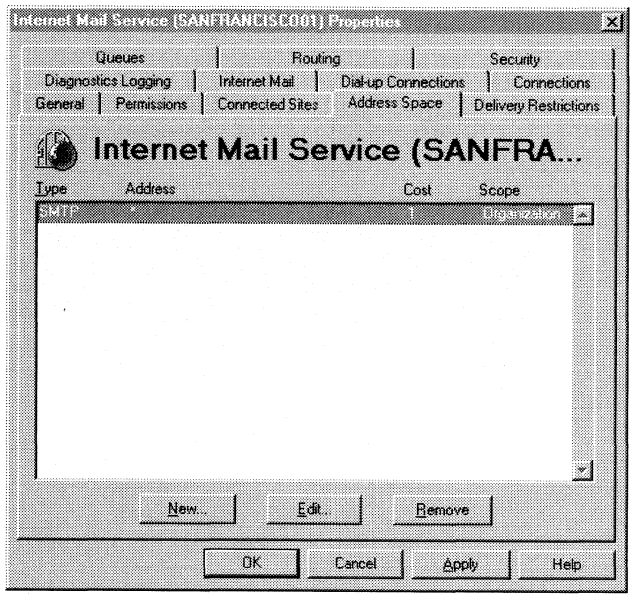
Address Spaces

Connectors are used to create paths for messages to be sent outside a site. These paths are represented by address spaces. Address spaces can be used to balance the messaging load when you use multiple Internet Mail Services. For example, if you have two Internet Mail Services, you can designate one to process messages destined for domainA and domainB, and the other to process messages destined for domainC. However, if you use two Internet Mail Services to handle a large throughput to a single domain, you can configure both to process the same addresses for equal load balancing.

Note If you have multiple routes to the same destination, the Internet Mail Service uses only the lowest cost route. If that connection is unavailable due to a communications problem, the Internet Mail Service does not use any of the higher cost routes. You can use mail exchanger (MX) records in DNS to override this and allow incoming mail to use a secondary route.

Getting to the Address Space property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.
3. Select the **Address Space** tab.



Specifying an Address Space

Use the **Address Space** property page to enter information about the addresses you want the connector to process.

1. Select the **Address Space** tab.
2. Choose **New** to create a new address space, or **Edit** to modify an existing address space.
3. To route all SMTP messages through an Internet Mail Service, choose **OK** without typing an e-mail domain. To route all messages to *company.com*, type *company.com* under **E-Mail Domain**.

For more information about addresses, see Chapter 4, "Address Spaces" or *Microsoft Exchange Server Concepts and Planning*.

Using Routing Addresses for Address Space Entries

Use the **Routing Address** property page on the address space configuration to send mail to recipients in another site when the sites do not use directory replication. To send to recipients using an address type other than SMTP, configure an address space for that address type, and use the **Routing Address** property page to specify the FQDN of the computer to which the Internet Mail Service will forward messages.

Note Only the first entry of any one type of address space will be used.

If you route other address types through the Internet Mail Service (for example, by using an Microsoft Mail address space), do not prefix the SMTP routing address in the **Routing Address** property page with an at sign (@). If you do, mail to this address type is not routed.

---

1. Select the **Address Space** tab.
2. Choose **New** and select an address type.
3. Specify an address space in the **General** property page, and then select the **Routing Address** tab.
4. Type the address type and address.

Option	Description
Type	An address type associated with recipients, such as SMTP or X.400.
Address	The FQDN of the computer to which the Internet Mail Service will forward messages.

For more information about configuring address spaces and using the **General** property page, see Chapter 4, "Address Spaces."

Delivery Restrictions

Use the **Delivery Restrictions** property page to accept or reject outbound messages from any sender listed in the Microsoft Exchange Server directory. For example, if a message is addressed to a foreign system, it is returned to the sender if the sender's address is in the **Reject messages from** box or does not appear in the **Accept messages from** box.

Note You cannot control delivery of inbound messages using the **Delivery Restrictions** property page.

Getting to the Delivery Restrictions property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.
3. Select the **Delivery Restrictions** tab.

Accepting or Rejecting Messages from Specific Senders

Delivery restrictions are optional and do not affect incoming messages. The default is to accept messages from all senders and reject messages from none. These are senders that are listed in the Microsoft Exchange Server directory.

Note If a distribution list is specified, the members of the distribution list are used for the restriction, not the distribution list itself.

---

1. Select the **Delivery Restrictions** tab.
2. Under either **Accept messages from** or **Reject messages from**, select **List**.
3. Choose **Modify** to open the Address Book so you can select from a list of recipients.

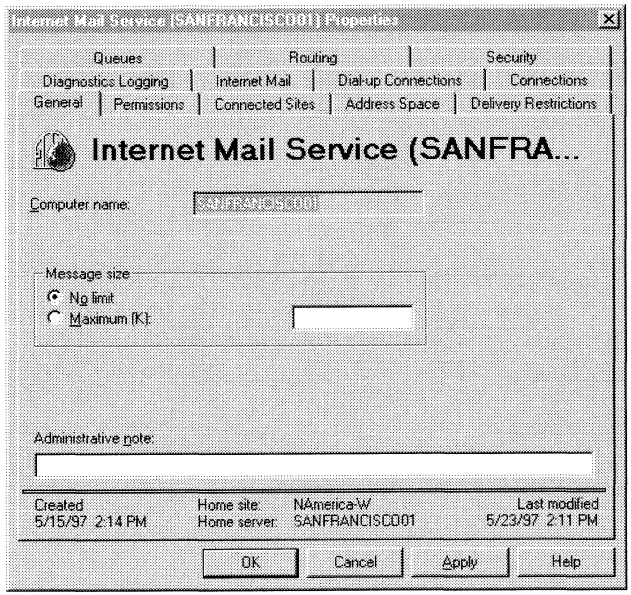
Option	Description
Show Names from the	Select the global address list or container from which to display a list of mailboxes.
Type Name or Select from List	Type or select one or more names from the list.
Add	Adds the selected names to the **Accept messages from** box.
Properties	Displays the properties of the mailbox.
Find	Opens the **Find** dialog box where you can search for any name based on a variety of properties.

General Properties

Use the **General** property page to view the computer name, specify message size, and add an administrative note.

Getting to the General property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.
3. Select the **General** tab.



Specifying the Maximum Message Size

You can configure the maximum size of messages transported through the Internet Mail Service using the **General** property page. This is useful when you do not want users sending messages with large attachments that might affect performance. This setting applies to both inbound and outbound messages. If the message size is exceeded, the message will be returned to the sender with an NDR.

You can restrict message size by e-mail domain. For outbound messages, the maximum message size in the **General** property page is applied before the maximum message size specified by the domain.

1. Select the **General** tab.
2. In the **Message size** box, select an option.

Option	Description
No limit	Send an inbound or outbound message of any size.
Maximum (K)	Specify a number between 1 and 9,999,999 KB.

For more information about setting options by e-mail domain, see "Specifying Message Content by E-mail Domain" earlier in this chapter.

Permissions

You can assign specific administrative permissions on the Internet Mail Service for Windows NT accounts. For more information on permissions, see *Microsoft Exchange Server Getting Started.*

Queues Properties

Use the Internet Mail Service **Queues** property page to view details about messages delivered to the Internet Mail Service queues.

Getting to the Queues property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.
3. Select the **Queues** tab.

For more information about using the **Queues** property page, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

Diagnostics Logging Properties

Diagnostics logging levels determine which Internet Mail Service events are written to the Windows NT Event Log and to the SMTP protocol log and message archival directories. They represent a progression of detail from recording only highly significant events, such as an application failure, through moderately important events, such as receipt of messages across a gateway, to events relevant only to debugging. Typically, you want to log only critical events. However, when problems occur, diagnostics logging lets you change the logging levels to capture more detailed events.

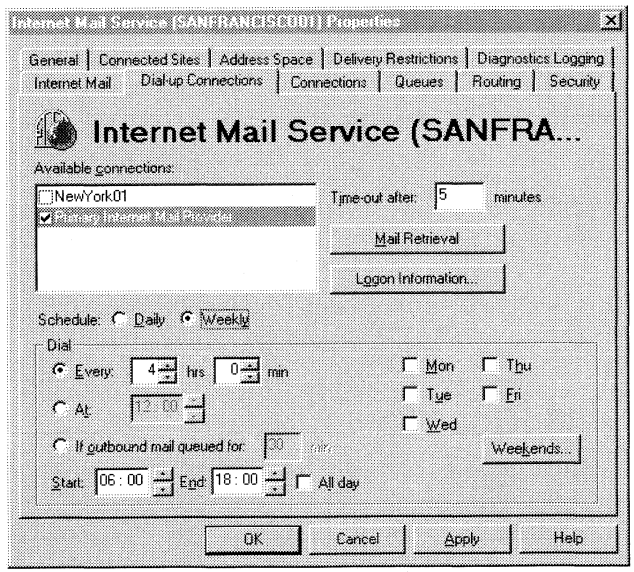
For more information about diagnostics logging, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

Dial-up Connections Properties

Use the **Dial-up Connections** property page to set connection and schedule information for using the Internet Mail Service and Remote Access Service (RAS) to connect to another site or to an Internet provider. Dial-up connections can be used when you do not want to have a permanent Internet Mail Service connection but would like to connect to an Internet service provider or a remote site at specified intervals.

Getting to the Dial-up Connections property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service to be modified.
3. Select the Dial-up Connections tab.



Viewing and Modifying the Available Connections

Use the **Dial-up Connections** property page to view and modify connections specified in the RAS phone book. You can specify commands used to retrieve mail, provide logon information, and schedule when connections will occur. The connection must be activated to modify its settings. To activate a connection, select the check box to the left of the connection name.

1. Select the **Dial-up Connections** tab.
2. Under **Available Connections**, select a connection to view or modify.

Adding Connections

You can add RAS entries using the RAS phone book. For information about how to add RAS entries, see your Windows NT Server documentation.

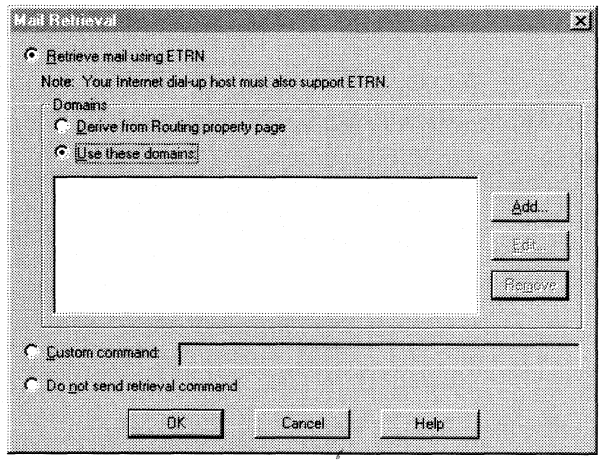
Note If you have multiple dial-up connections defined on the server and have selected the check boxes next to them in the **Dial-up Connections** property page, the Internet Mail Service dials each connection, even though only the connections selected in the **Connections** property page are used to transfer mail.

Specifying Mail Retrieval Options

Your Internet service provider may require a command that identifies you to the provider and gives notification that you are ready to receive messages. You can use ETRN, if your host supports it, or you can specify a command, such as **ping**, to run on the local computer when the connection is established. ETRN is an SMTP extension that causes the remote host to send mail to a specified domain.

Use the **Dial-up Connections** property page to specify which command will be used to retrieve mail.

1. Select the **Dial-up Connections** tab.
2. Under **Available Connections**, select a connection to view or modify.
3. Choose Mail Retrieval.



4. Choose an option.

Option	Description
Retrieve mail using ETRN	Specify whether you will use the domains specified on the **Routing** property page or create a new list of domains.
Derive from Routing property page	An @ sign is appended to the ETRN command for all domains listed on the **Routing** property page. This enables mail to be collected for all subdomains. This is the default.
Use these domains	Choose **Add**, **Edit**, and **Remove** to create, modify, and delete domain names. Precede domain names with an @ symbol to collect mail for all subdomains.
Custom Command	Choose to enter a custom command or executable file, such as **ping**. This is run on the local computer when the connection is made.
Do not send retrieval command	Disables ETRN and does not send any command.

For more information on ETRN, see *Microsoft Exchange Server Concepts and Planning*.

Specifying a Time-out Period

Use the **Dial-up Connections** property page to specify the amount of time, in minutes, to keep the RAS connection open and wait for incoming mail after the initial transfer is complete. If incoming mail is received before the time-out period expires, the mail is transferred and the time-out period begins again.

Outbound mail is sent only when a RAS connection is first established. When you set the time-out period, it should be long enough for the remote system to initiate its mail transfer but short enough that the RAS connection ends at some point and then reconnects to send outgoing mail.

1. Select the **Dial-up Connections** tab.
2. Under **Available Connections**, select a connection.
3. In the **Time-out after** box, type a value.

Specifying Logon Information

Use the **Dial-up Connections** property page to provide the logon account and password required by the remote site or Internet service provider.

1. Select the **Dial-up Connections** tab.
2. Under **Available Connections**, select a connection.
3. Choose **Logon Information**.
4. Type the user name, domain, and password.

Option	Description
User name	The name used to log on to the remote server.
Domain	The domain of the remote system (optional).
Password	The user password.
Confirm password	Verifies the password.

Setting a Schedule

Use the **Dial-up Connections** property page to specify how frequently the Internet Mail Service connects to another site or an Internet provider.

1. Select the **Dial-up Connections** tab.
2. Under **Available Connections**, select a connection.
3. Set the schedule for the connection.

Option	Description
Daily	Specifies a daily dial-up connection.
Weekly	Specifies a weekly dial-up connection.
Every	Specifies a dial-up connection at certain intervals. Type the number of hours and minutes between connection attempts. If you select this option, a connection is made when you start the Internet Mail Service and then again at the specified interval.
At	Specifies a dial-up connection at a certain time. Type the time when you want to connect to your Internet service provider or a remote site.
When mail queued, but at most every	Specifies a dial-up connection only when messages are waiting to be sent. The number of minutes you enter determines the most frequent interval at which a dial-up connection is established, regardless of how much mail is waiting. If no mail is waiting to be sent, the dial-up connection is made as soon as an outbound message is queued as long as the specified interval has passed since the last connection was made. The default is 30 minutes.

(continued)

Option	Description
Start, End	The hours during which the dial-up connection schedule takes effect. This applies only if you enter values in the **Every** or **When mail queued for** boxes. If you want the schedule to be active 24 hours a day, select the **All Day** check box.
Mon, Tue, Wed, Thu, Fri	Indicates when the Internet Mail Service dial-up schedule applies. You must select **Weekly** under **Schedule** for these options to appear.
Weekends	Specifies the dial-up connection schedule that will be used on the weekends.

Routing Properties

Use the **Routing** property page to intercept inbound messages from SMTP hosts, POP3, and IMAP4 clients, and selectively reroute those messages to other SMTP hosts before they are processed by the Internet Mail Service.

Note If the Internet Mail Service is responsible for delivering messages inbound to Microsoft Exchange Server for domains other than the domain specified in the Site Addressing object, you must add these domains to the **Routing** property page. If you do not add these additional domains, mail to these domains will generate an NDR without being delivered inbound to Microsoft Exchange Server.

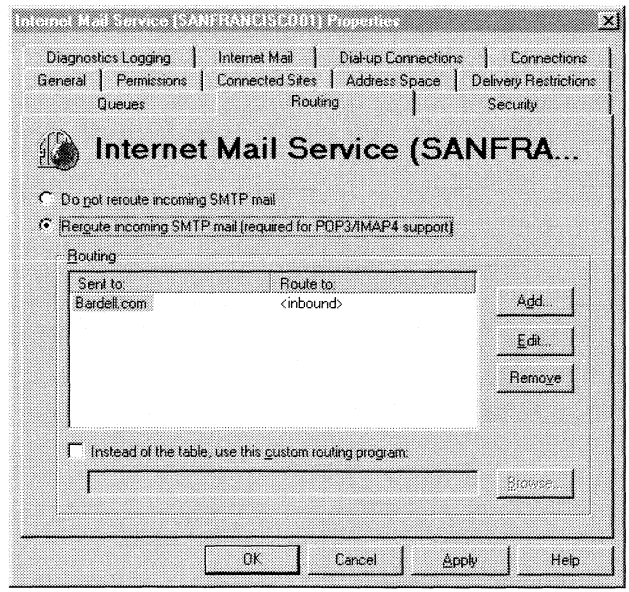
The **Routing** property page contains a list of domain names and associated SMTP hosts. For each recipient of every inbound message the Internet Mail Service receives, the **Routing** property page compares the domain name on the address to the list of domain names in the **Routing** property page. If a match is found, the message for that particular recipient is rerouted to the associated host.

The match is compared to the rightmost part of the domain name in the recipient address. Only full subdomains are compared. For example, if the domain name in the table is sea.com, it matches an address of x.sea.com as well as sea.com, but not chelsea.com. The list is searched from the most specific to the least specific match. For example, user@x.sea.com would match x.sea.com, sea.com, or .com. However, if x.sea.com is in the list, it is used because it is the most specific match. This occurs regardless of its placement in the list.

In cases where the associated SMTP host is set for **<inbound>**, domain names in the list represent names that should be handled by the Internet Mail Service. If the recipient address matches one of these domain names, the Internet Mail Service processes the recipient normally and attempts to deliver the message to the Microsoft Exchange Server computer. If no match is found, the Internet Mail Service reroutes the message outbound to the domain name in the recipient's address. For this reason, it is important to ensure that any domain names that must be routed to the Microsoft Exchange Server computer are listed in the **Routing** property page. In particular, any domain names used in SMTP addresses for Microsoft Exchange users must be defined in the **Routing** property page. Otherwise, reports and replies will not be deliverable and could cause routing loops.

Getting to the Routing property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service.
3. Select the **Routing** tab.



Choosing a Routing Method

Use the **Routing** property page to specify whether to reroute incoming mail.

Note If POP3 or IMAP4 clients are to be accessing the organization, all Internet Mail Services directly connected to the Internet or servicing POP3 or IMAP4 clients should be configured to reroute mail.

1. Select the **Routing** tab.
2. Select an option.

Option	Description
Do not reroute incoming SMTP mail	Only messages addressed to recipients listed in the Microsoft Exchange Server global address list are delivered. All other mail is returned with an NDR.
Reroute incoming SMTP mail (required for POP3/IMAP4 support)	Incoming mail is rerouted according to the entries in the **Routing** property page.

Specifying Routing Destinations

Use the **Routing** property page to specify where inbound mail will be rerouted. To receive mail addressed to the Microsoft Exchange Server organization from the Internet, you must specify at least one inbound route. By default, the **Routing** box contains the SMTP address in the Configuration container's **Site Addressing** property page and sets it to route messages inbound.

Note Mail addressed to any domain not specified is directed outbound.

1. Select the **Routing** tab.
2. Under **Routing**, choose **Add**, **Edit**, or **Remove**.

Option	Description
Add	Create new routing information.
Edit	Modify routing information.
Remove	Remove routing information.

Adding Routing Addresses

Use the **Routing** property page to determine the routing of messages bound for any domain. You may want inbound mail addressed to your domain to be received by this Internet Mail Service. To do this, you would route all mail destined for the organization to inbound, or you can configure the Internet Mail Service so it translates domain names. For example, you could specify inbound mail addressed to x.sea.com be rerouted to server1.sales.sea.com. If no routing entry is specified for a domain, mail for that domain is rerouted outbound. This allows the Internet Mail Service to forward Internet mail for other hosts.

1. Select the **Routing** tab.
2. Under **Routing**, choose **Add**.
3. Type the domain name of the mail that will be rerouted.
4. Select an option.

Option	Description
Should be accepted as "inbound"	Mail is accepted into the Microsoft Exchange Server organization.
Should be rerouted to this domain	Specify the domain name where the mail will be sent. The Internet Mail Service rewrites the address.

Modifying a Routing Address

You can edit an address specified in the **Routing** property page.

1. Select the **Routing** tab.
2. Select the routing address you want to modify.
3. Choose **Edit**.

Removing a Routing Address

You can delete an address specified in the **Routing** property page.

1. Select the **Routing** tab.
2. Select the routing address you want to delete.
3. Choose **Remove**.

Using a Custom Routing Program

Use the **Routing** property page to specify the name of a custom routing program.

1. Select the **Routing** tab.
2. Select **Instead of the table, use this custom routing program**.
3. Choose **Browse**, and select the name of the custom routing program.

For more information on custom routing files, see the *Microsoft Exchange Server Resource Guide*.

Security Properties

Use the **Security** property page to enable security on outbound connections to other systems. Messages transferred from one Microsoft Exchange Server computer to another SMTP host may be encrypted or authenticated.

Getting to the Security property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service.
3. Select the **Security** tab.

Enabling Security for Outbound Connections

You can use Simple Authentication and Security Layer (SASL), Secure Sockets Layer (SSL), or Windows NT security on connections to other systems. You can provide the account, domain, and password that is effective for all connections, or you can provide separate security information for each domain you connect to.

Note To ensure the strongest possible encryption over outbound connections, choose SSL encryption or use a Windows NT account with a non-blank password.

---

1. Select the **Security** tab.
2. Choose **Add**.
3. Type the name of the remote e-mail domain.
4. Choose a security type.

Option	Description
No authentication or encryption	No security enabled.
SASL authentication/SSL encryption	Choose **SASL/AUTH**, **SSL encryption**, or both.
SASL/AUTH clear text password authentication	Uses the AUTH LOGIN ESMTP extension to send the clear text account and password on the outbound connections.
SSL encryption	SSL encryption is enabled. The STARTTLS ESMTP extension is used.
Windows NT challenge/response authentication and encryption	Enables Windows NT security. Choose this option when the Internet Mail Service is used as a site connector and you want to encrypt data transferred over the Internet.

MIME Types

To set MIME types for inbound messages, use the **MIME Types** property page located on the site and server Protocols containers. For more information about using the **MIME Types** property page, see Chapter 13, "Internet Protocols."

Internet Mail Service and Macintosh File Attachments

File attachments from a Macintosh will be mapped to MIME-standard body parts so that MIME-compliant clients and gateways can decode these attachments. Additionally, the Internet Mail Service maps any incoming body parts to Windows or Macintosh file types.

Adding Additional Internet Mail Services

You can add an Internet Mail Service to a site that has an existing service. Only one Internet Mail Service can be installed on a single server.

You should consider adding another Internet Mail Service when:

- Backlogs regularly build up in one of the Internet Mail Service queues.
- A backup computer is required to eliminate any interruption of the mail transfer between the Microsoft Exchange Server site and the other SMTP hosts.

When your site has more than one Internet Mail Service, you should consider the following:

- If the amount of mail to specific domains on the SMTP messaging system can be divided, consider configuring each of the Internet Mail Services to process mail for specific domains only.

- You can assign a cost to the address spaces of each Internet Mail Service. This partially determines Internet Mail Service throughput and can be used to optimize Internet Mail Service performance.
- If incoming and outgoing mail to the SMTP messaging system is balanced, consider configuring one Internet Mail Service to process incoming messages and the other Internet Mail Service to process outgoing messages.

When you add a new Internet Mail Service, you may need to perform one or more of the following tasks:

- Modify the address space of existing Internet Mail Services depending upon the address space you assign to the new Internet Mail Service.
- Change the maximum number of inbound and outbound connections of existing Internet Mail Services depending upon the number of inbound and outbound connections you want to assign to the new Internet Mail Service.
- Change the DNS or Hosts file to reflect the existence of the new Internet Mail Service host.
- Change the MX records in DNS to forward mail to a new Internet Mail Service host if the primary Internet Mail Service is down or too busy.

Removing the Internet Mail Service

To remove an existing Internet Mail Service, stop new outbound messages from arriving at the Internet Mail Service, stop new inbound Internet messages from being accepted by the Internet Mail Service, monitor queues until they are empty, and then remove the Internet Mail Service.

1. Remove all address space entries for the Internet Mail Service in the **Address Space** property page. This allows message transfer agents (MTAs) to reroute messages to other Internet Mail Services servicing the same address spaces.
2. If the Internet Mail Service is used to connect Microsoft Exchange Server sites, remove all the entries in the **Connected Sites** property page. In addition, reconfigure all other Internet Mail Services that exchange messages directly with this Internet Mail Service. If the Internet Mail Service is the only one in the organization, all messages sent to the address spaces that were being serviced by the Internet Mail Service will be returned to the senders as non-deliverable.
3. Stop the Internet Mail Service.
4. In the Administrator window, select the Internet Mail Service, and then select the **Connections** tab.
5. Under **Transfer Mode**, select **None** to clear the Internet Mail Service queues.
6. Set the **Retry interval** to a short interval, such as **.25** (15 minutes).

7. Under **Service Message Queues**, choose **Time-outs** and set all time-outs for one hour.
8. Start the Internet Mail Service.
9. Select the **Queues** property page to monitor all the queues.
10. When the queues are empty, stop the Internet Mail Service.
11. Remove the Internet Mail Service by deleting the object from the Connections container.

For more information about connected sites, see "Connected Sites Properties" earlier in this chapter. For more information about address spaces, see "Address Spaces" earlier in this chapter. For more information about using the **Internet Mail** property page, see "Internet Mail Properties" earlier in this chapter. For more information about using the Internet Mail Service as a site connector, see *Microsoft Exchange Server Concepts and Planning*.

Advanced Internet Mail Service Configuration

You can increase the Internet Mail Service performance by editing the registry for the Windows NT Server hosting your Microsoft Exchange Server.

For information on SMTP commands and headers, see Request for Comments (RFC) 821, "Simple Mail Transfer Protocol" and RFC 822, "Standard for the Format of ARPA Internet Text Messages."

Reverse Resolution

You can disable reverse resolution lookup for SMTP mail sent to the Internet Mail Service. Reverse resolution is when the name of the host that delivered an incoming SMTP message is resolved and placed into the message header by the Internet Mail Service.

When an SMTP message is received, the host address is contained in the message header. The header describes the path of the message as it traveled from the host that sent the message to the host that received the message. The following is a sample SMTP message header with return path and time stamps.

```
Received: from GHI.COM by JKL.COM ; 27 Oct 96 15:27:39 PST
Received: from DEF.COM by GHI.COM ; 27 Oct 96 15:15:13 PST
Received: from ABC.COM by DEF.COM ; 27 Oct 96 15:01:59 PST
Date: 27 Oct 96 15:01:01 PST
From: JOE@ABC.COM
Subject: Upgraded Mail System
To: SAM@JKL.COM
```

Disabling Reverse Resolution

You can increase Internet Mail Service performance by disabling reverse resolution. When reverse resolution is disabled, the Internet Mail Service will not resolve the host name in the upper most Received From portion of the SMTP message header. If the address is in Internet Protocol (IP) form, the address will remain as such.

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and then choose **New DWORD Value**. If you are using Regedt32.exe, choose **Edit**, and then choose **Add Value**.
4. If you are using Regedit.exe, type **DisableReverseResolve**; under **Value data**, type 1. If you are using Regedt32.exe, type **DisableReverseResolve**; under **Data Type**, choose **REG_DWORD.**
5. If you are using Regedt32.exe, under **Data**, type 1.

User Name Resolution

When the Internet Mail Service receives an SMTP message, it attempts to resolve the user name in the header against the Microsoft Exchange Server global address list. A *user name* is the name associated with an SMTP address. If the user exists in the global address list, the SMTP address associated with the user is replaced by the display name for the user's account. Otherwise, the name displays as the SMTP address.

Disabling User Name Resolution

When an SMTP message is received, the Internet Mail Service attempts to resolve the user name in the To, From, and Cc fields from the SMTP addresses. You can increase the performance of the Internet Mail Service by disabling user name resolution.

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and then choose **New DWORD Value**. If you are using Regedt32.exe, choose **Edit**, and then choose **Add Value**.

4. If you are using Regedit.exe, type **ResolveP2**; under **Value data**, type 0. If you are using Regedt32.exe, type **ResolveP2**; under **Data Type,** choose **REG_DWORD**.
5. If you are using Regedt32.exe, under **Data**, type 0.

Enabling Loopback Detection

The Internet Mail Service allows configurations where SMTP connections are made to itself. There are cases where this is appropriate, such as when a user sends a message to another user on the same server using an SMTP proxy. However, this can also allow loopbacks and inefficient configurations. You can configure the Internet Mail Service so that it will not initiate SMTP connections if the destination host's IP address matches its own. Instead, it creates an NDR for the message.

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and then choose **New DWORD Value**. If you are using Regedt32.exe, choose **Edit**, and then choose **Add Value**.
4. If you are using Regedit.exe, type **DisableLoopbackConnection**; under **Value data**, type 1. If you are using Regedt32.exe, type **DisableLoopbackConnection**; under **Data Type,** choose **REG_DWORD**.
5. If you are using Regedt32.exe, under **Data**, type 1.

Verify Request (VRFY)

When the Internet Mail Service communicates with an SMTP host, it may be asked to identify a user. This is done with the SMTP verify command (VRFY). The verify command asks the receiver to identify whether a user can be reached through the receiving host. The response will include the mailbox of the user and a full name.

The following is an example of a verify request for the user "smith." The response is the full name and the SMTP address for the user Renee Smith.

```
Send: VRFY smith
Received: 250 Renee Smith <renees@abcd.COM>
```

Enabling VRFY

The verify request for the Internet Mail Service is disabled by default. Disabling the VRFY command is of interest to mail administrators concerned with spoofing. The VRFY command is one method of querying a server for valid SMTP addresses.

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and then choose **New DWORD Value**. If you are using Regedt32.exe, choose **Edit**, and then choose **Add Value**.
4. If you are using Regedit.exe, type **EnableVRFY**; under **Value data**, type 1. If you are using Regedt32.exe, type **EnableVRFY**; under **Data Type**, choose **REG_DWORD.**
5. If you are using Regedt32.exe, under **Data**, type 1.

Disabling Text Quoting

You can disable the Internet Mail Service *text quoting* in outgoing messages that are not sent with rich text formatting by setting the UseRTFText registry value to 0. By default, text quoting behavior is enabled and applies Internet-style quoting to reply-and-forward text by inserting a greater than (>) character before each line.

Quoting is also applied to text that is cut and pasted from a message into a compose note. When sending a message with a command to a list server, it is important to make sure the text is not quoted; otherwise, the list server cannot interpret the command. You can type the command manually. Alternatively, you can use the **Paste Special** command to paste the plain text. Do not paste the formatted text.

Note UseRTFText also affects word-wrap. If enabled, text lines in all non-TNEF messages are wrapped at a fixed column. The word-wrap setting for non-MIME messages on the Internet Mail Service properties in the Microsoft Exchange Server Administrator program is ignored.

You can disable quoting using the Windows NT registry.

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and then choose **New DWORD Value**. If you are using Regedt32.exe, choose **Edit**, and then choose **Add Value**.
4. If you are using Regedit.exe, type **UseRTFText**; under **Value data**, type 0. If you are using Regedt32.exe, type **UseRTFText**; under **Data Type**, choose **REG_DWORD.**
5. If you are using Regedt32.exe, under **Data**, type 0.

Message Tracking on the Internet Mail Service

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 unaccounted mail.
- Track an unauthorized message and remove it from the system.

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 each component receives, processes, and delivers it to the next component. The tracking logs are stored in \Exchsrvr\Tracking.Log.

For more information on message tracking, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

How a Message is Tracked

When a message is passed from the Microsoft Exchange Server computer to the Internet, multiple events are logged in the tracking log. Each log records one day's activities on the server. The tracking log can be displayed by using the Microsoft Exchange Server Message Tracking Center.

The following table defines the Internet Mail Service activity in the tracking logs.

Field Name	Description
SMTP transfer out	The message is received by the Internet Mail Service from the Microsoft Exchange Server information store.
SMTP inbound received	The message is received by the Internet Mail Service from the Internet.
SMTP transfer in	The message is received by the Microsoft Exchange Server information store from the Internet Mail Service.
SMTP message rerouted	The message was received by the Internet Mail Service and rerouted to another domain.

For information on rerouting, see "Routing Properties" earlier in this chapter.

ESMTP Support

The Internet Mail Service supports SMTP Service Extensions (ESMTP). ESMTP defines a method for extending SMTP whereby an SMTP server can inform an SMTP client of the extensions it supports. ESMTP does not require modification of existing SMTP client or server configuration.

How ESMTP Works

An SMTP client supporting ESMTP starts an SMTP session by issuing the EHLO command instead of the HELO command. A successful response issues a list of SMTP extensions the server supports. If the server does not support ESMTP, an error is generated.

The following is an example of a successful response to the EHLO command from the server abc.def.ghi.com as requested by the client rst.uvw.xyz.com.

```
Server: 220 abc.def.ghi.com ESMTP Server (Microsoft Exchange Internet
Mail Service) ready
Client: EHLO rst.uvw.xyz.com
Server: 250-abc.def.ghi.com supports the following extensions:
Server: 250-XEXCH50 [Exchange to Exchange data transfer]
Server: 250-HELP
Server: 250-VRFY
Server: 250-SIZE 0
Server: 250-ETRN
Server: 250 DSN
Server: 250 AUTH=LOGIN [SASL clear text password authentication]
Server: 250 TLS [transport level security]
```

For more information on ESMTP, see RFC 1869, "SMTP Service Extensions" and RFC 1870, "SMTP Service Extension for Message Size Declaration."

Disabling ETRN Support

Microsoft Exchange Server supports the use of an SMTP extension called ETRN for dial-up connections using RAS. After the client host submits the ETRN command to the server host, a new connection is established from the server host to the client host, and mail to the client host domain is retried immediately.

You can disable ETRN using the Windows NT registry.

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and then choose **New DWORD Value**. If you are using Regedt32.exe, choose **Edit**, and then choose **Add Value**.
4. If you are using Regedit.exe, type **DisableETRN**; under **Value data**, type 1. If you are using Regedt32.exe, type **DisableETRN**; under **Data Type**, choose **REG_DWORD.**
5. If you are using Regedt32.exe, under **Data**, type 1.

For more information about using ETRN, see *Microsoft Exchange Server Concepts and Planning*, and RFC 1985, "SMTP Service Extension for Remote Message Queue Starting."

Disabling ESMTP Support

You can disable ESMTP, which prevents the Microsoft Exchange Server computer from responding to an EHLO command with a list of supported ESMTP commands. You disable ESMTP when you want clients to stop issuing ESMTP commands.

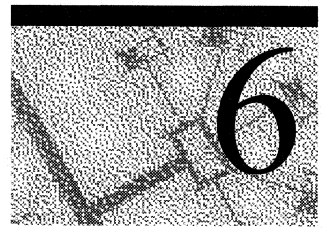
You can disable ESMTP using the Windows NT registry.

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and then choose **New DWORD Value**. If you are using Regedt32.exe, choose **Edit**, and then choose **Add Value**.
4. If you are using Regedit.exe, type **AdvertiseSMTPExtensions**; under **Value data**, type 0. If you are using Regedt32.exe, type **AdvertiseSMTPExtensions**; under **Data Type**, choose **REG_DWORD.**
5. If you are using Regedt32.exe, under **Data**, type 0.

CHAPTER 6

Site Connector and Dynamic RAS Connector



Microsoft Exchange Server provides several connectors to link sites in your organization. Each connector uses different transport protocols for message exchange. You can use a combination of connectors or install multiple connectors of the same type.

You can use the following connectors to connect sites:

Site Connector Connects two sites on the same physical local area network (LAN) using synchronous remote procedure calls (RPCs).

Dynamic RAS Connector Connects two sites using the asynchronous Remote Access Service (RAS) function provided with Windows NT Server.

Internet Mail Service Connects two sites using the Internet Mail Service.

X.400 Connector Connects two sites using X.400 transport protocols. An X.400 Connector is also used to connect Microsoft Exchange Server sites to foreign systems.

For information about using the Internet Mail Service, see Chapter 5, "Internet Mail Service." For information about using X.400, see Chapter 7, "X.400 Connector."

Site Connector

When you set up a Site Connector, you specify a server in the remote or target site to provide site-to-site message transfer.

Before you begin, you need the following:

- A logical map of your network.
- The name of at least one server in the target site.
- A LAN protocol capable of using RPC.

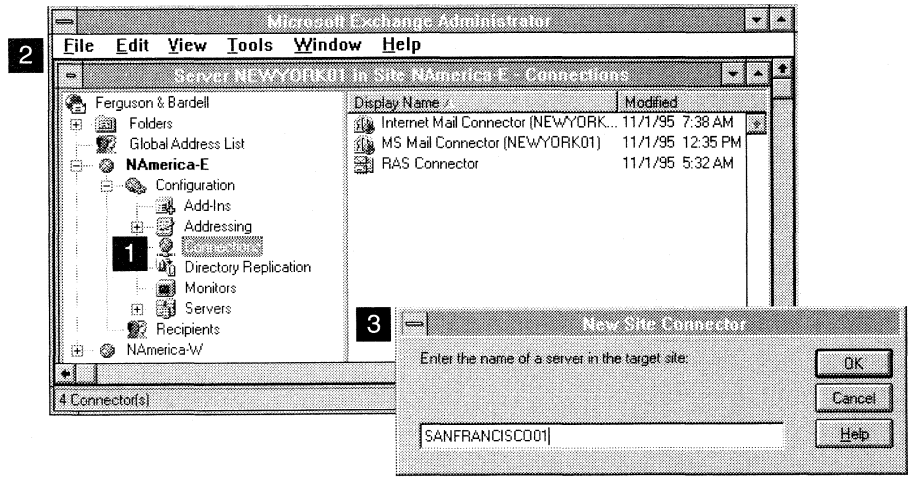
- Administrator permissions on both the local and target sites.
- Decide which servers in the remote site you want to use for message transfer. These will be the target servers displayed in the *target server list.*

Site Connector Installation

These procedures enable message transfer from the local site to the remote site. When you finish configuring the Site Connector, you create a Site Connector in the remote site, provided you have the appropriate permissions. To install a new Site Connector, you need to specify a server in the remote site.

1. In the Administrator window, choose **Connections**.
2. From the **File** menu, choose **New Other**, and then choose **Site Connector**.
3. Type the name of the server in the target site, and choose **OK**.

   The name of the server in the target site can contain up to 15 alphanumeric characters.

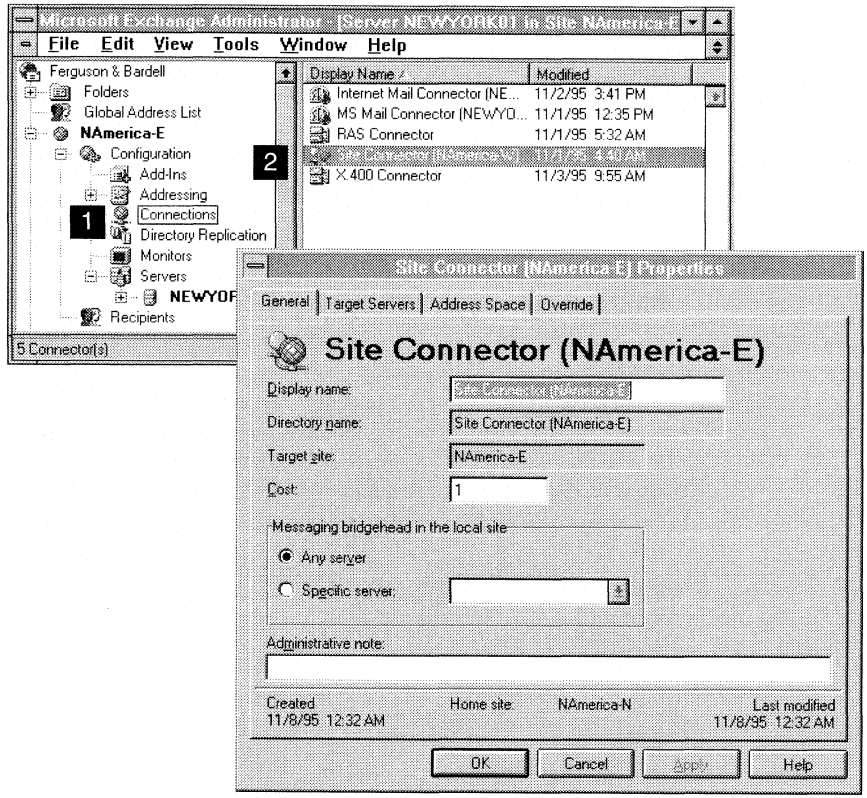


Site Connector Configuration

You configure the Site Connector using property pages to specify target servers, address spaces, override account information, permissions, and the name and cost of the connector.

Getting to the Site Connector property pages

1. In the Administrator window, choose **Connections**.
2. Double-click the Site Connector to be configured.



General Properties

Use the **General** property page to provide a name for the connector, specify the cost of the connector, and specify the messaging bridgehead server in the local site.

Note If you are installing a new Site Connector, the **General** property page appears automatically after you choose **New Other** from the **File** menu, and then choose **Site Connector**.

Getting to the General property page

1. In the Administrator window, choose **Connections**.
2. Double-click the Site Connector to be modified.
3. Select the **General** tab.

Specifying the Connector Name

Use the **General** property page to define a name for the Site Connector. The directory name cannot be changed once it is entered.

1. Select the **General** tab.
2. Type the directory name and the display name.

Option	Description
Display name	Type the name (up to 256 alphanumeric characters) that will be displayed in the Administrator window. This name is not case-sensitive.
Directory name	Type an informative and descriptive name (up to 64 alphanumeric characters). This permanent name identifies the Site Connector in the directory and is used in event log messages. You can modify this name only when creating a Site Connector. This name is not case-sensitive.

Assigning a Routing Cost

You can set a routing cost of the message transfer from the local site to the remote site.

1. Select the **General** tab.
2. Specify the **Cost**.

Option	Description
Cost	Type a cost between 1 and 100. The lowest cost of all active connections is chosen. The default is 1.

For more information about setting costs, see *Microsoft Exchange Server Concepts and Planning*.

Setting a Messaging Bridgehead Server in the Local Site

You can select one server that is dedicated to sending messages to remote sites.

1. Select the **General** tab.
2. Select **Any server** or select **Specific server**, and type the name of the server.

Option	Description
Any server	Any server in the local site can send messages to the remote site. This is the default setting.
Specific server	Select a specific server in the local site to send messages to the remote site.

Address Space Properties

You can define the type and format of addresses used to identify messages sent to another site. Each entry is called an *address space* and contains only as much of the address as necessary to distinguish messages that should be sent through this connector. You need to specify only the address space options that uniquely identify the route to the site. The X.400 address of the remote site is automatically entered in the **Address Space** property page when the Site Connector is created.

Getting to the Address Space property page

1. In the Administrator window, choose **Connections**.
2. Double-click the Site Connector to be modified.
3. Select the **Address Space** tab.

Defining Address Spaces

Specify only as much of the address information as necessary to distinguish messages that should be routed to the connected site. For example, if you want to route every message with a Simple Mail Transfer Protocol (SMTP) address to the remote site, you should create a new Internet entry with an asterisk (*) in the address field. This matches all messages with a non-local SMTP address type and routes each to the remote site.

Note You can use an asterisk (*) for a multicharacter wildcard in an address space. A percent symbol (%) can be used for a single character wildcard.

---

1. Select the **Address Space** tab.
2. Choose **New** to create a new address space or **Edit** to modify an existing address space.

For more information about address spaces, see Chapter 4, "Address Spaces," or see *Microsoft Exchange Server Concepts and Planning*.

Assigning an Address Space Cost

Address space costs determine the preference between multiple routes to a remote site. The cost associated with each address space is used to optimize message routing to the foreign system but does not affect message reception. All mail is sent using the address with the lowest cost. If two or more routes are available with the same cost, the load placed on the routes is roughly equal. Address space costs range from 1 to 100.

1. Select the **Address Space** tab.
2. Double-click the address for which you want to assign a cost.

3. In the **Cost** box, type a routing cost for messages transferred using this address.

Option	Description
Cost	Type a cost between 1 and 100. Lower cost address spaces take precedence over higher cost address spaces. The default is 1.

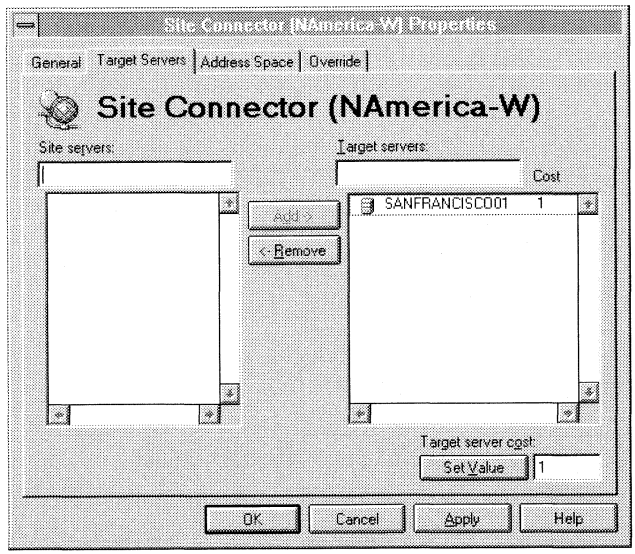
For more information about setting costs, see *Microsoft Exchange Server Concepts and Planning*.

Target Servers Properties

Use the **Target Servers** property page to add and remove target servers. Target servers are servers that receive messages.

Getting to the Target Servers property page

1. In the Administrator window, choose **Connections**.
2. Double-click the Site Connector to be modified.
3. Select the **Target Servers** tab.



Adding and Removing Target Servers

All servers in the target site are placed in the target servers list by default. You can add or remove servers using the list.

1. Select the **Target Servers** tab.
2. To add a target server, select a server in the **Site servers** box, and choose **Add**. To remove a target server, select a server in the **Target servers** box, and choose **Remove**.

Assigning a Target Server Cost

Target server costs determine routing between servers in a remote site. If two or more servers are available with the same cost, the load placed on these servers is roughly equal. The server you specified during configuration of the new Site Connector is automatically entered in the **Target servers** box with a routing cost of 1.

1. Select the **Target Servers** tab.
2. In the **Target servers** box, select the target server.
3. In the **Target server cost** box, type the cost for this server.
4. Choose Set Value.

Option	Description
0	Use this target server before any other target server.
1-99	Cost is weighted against other target server costs. The default is 1.
100	Use this target server only when all other target servers fail.

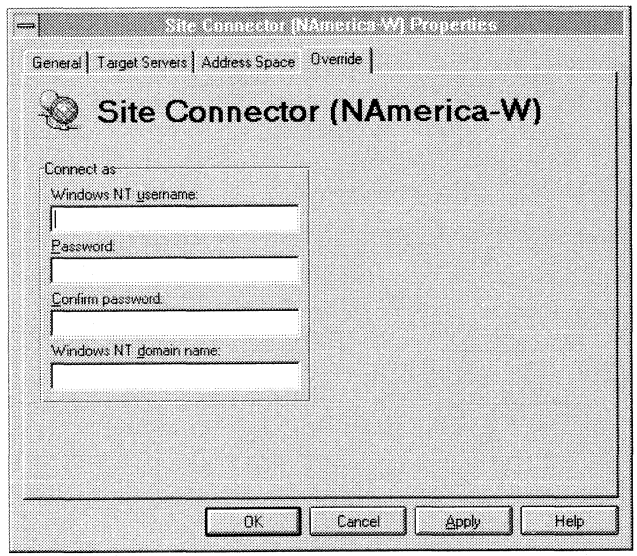
For more information about setting costs, see *Microsoft Exchange Server Concepts and Planning*.

Override Properties

Use the **Override** property page when the service account of the local site lacks service account permissions for the remote site.

Getting to the Override property page

1. In the Administrator window, choose **Connections**.
2. Double-click the Site Connector to be modified.
3. Select the **Override** tab.



Connecting Using a Different Account

If a target server does not have a Windows NT Server trust relationship with the local site, it may be necessary to provide access permissions in order for the message transfer agents (MTAs) to send mail. You can override the NT user account you used to log on to your local Microsoft Exchange Server computer.

Note To avoid any permissions-related problems, use the Microsoft Exchange Server service account for the remote site.

---

1. Select the **Override** tab.
2. Under **Connect as**, type the user information.

Dynamic RAS Connector

The Dynamic RAS Connector can be used to connect two sites. This asynchronous connection uses the RAS functionality provided with Microsoft Windows NT Server. The Site Connector communicates using RPC over IPX/SPX or TCP/IP, provided they are installed correctly and configured in Windows NT. It is important that no other LAN connection exist between the two computers.

Before using a RAS connection, you need the following:

- RAS network software installed and configured on the Microsoft Exchange Server computer.
- The service account or a Windows NT account with Send As and Mailbox Owner (User role) permissions for the Servers or Configuration containers in the remote site.
- The name to use for the MTA transport stack. The default is RAS on *servername*.
- The name of the remote server.
- The phone book entry for the remote server including the name of the server and the phone number.
- The name you want to use for the Dynamic RAS Connector.

The following procedures are used to install and configure the Dynamic RAS Connector.

- Install the RAS MTA transport stack.
- Install and configure the Dynamic RAS Connector.

For information on installing and configuring Windows NT RAS software, see your Windows NT Server documentation or Appendix A, "Setting Up Windows NT Server for RAS Connectivity."

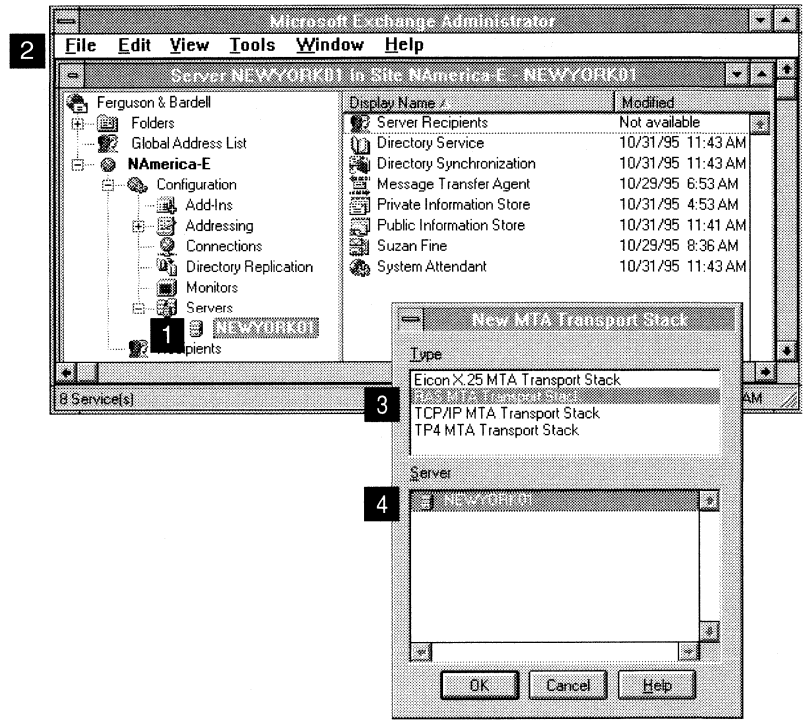
MTA Transport Stack Installation

Before you install a RAS MTA transport stack, the network software must be installed on the server.

For communications over public telephone, X.25 packet assembly/disassembly (PAD), or Integrated Services Digital Network (ISDN) networks, you can install one RAS transport stack on a Microsoft Exchange Server. This transport stack works with the RAS network software running on a Windows NT Server computer.

Use the following steps to install the MTA transport stack.

1. In the Administrator window, choose **Servers**, and then choose a server.
2. From the **File** menu, choose **New Other**, and then choose **MTA Transport Stack**.
3. In the Type box, select RAS MTA Transport Stack.

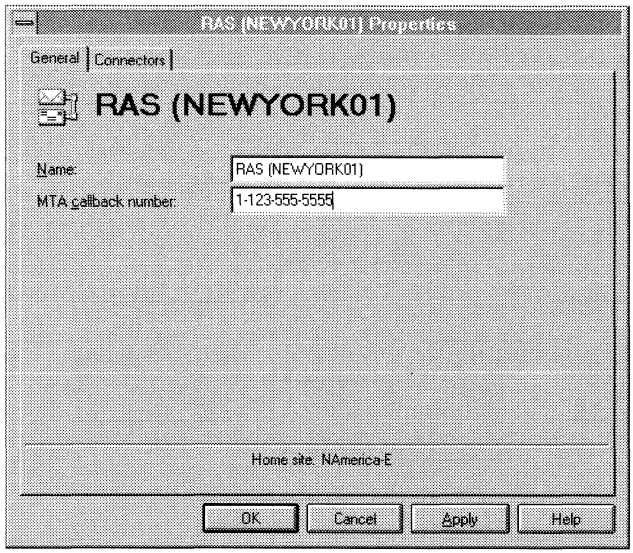


4. In the **Server** box, select the server on which to install the transport stack, and then choose **OK**.

General Properties

Use the **General** property page to set the name of the RAS MTA transport stack, and the optional MTA callback number. You can modify the transport stack name only when creating a new transport stack. The default name is RAS *(servername)*. The MTA callback telephone number is used to reach the local server over a dial-up connection when RAS callback security is enabled. Specifying this number is optional.

1. In the Administrator window, choose the server where the RAS MTA transport stack is installed.
2. Double-click the RAS MTA transport stack to be modified.
3. Type the name of the RAS MTA transport stack and the MTA callback number (optional).



Option	Description
Name	The name for this transport stack. You can modify this name only when creating a new transport stack. The default is RAS *(servername)*.
MTA callback number	The telephone number used to reach the local server over a dial-up connection when RAS callback security is enabled. Specifying this number is optional.

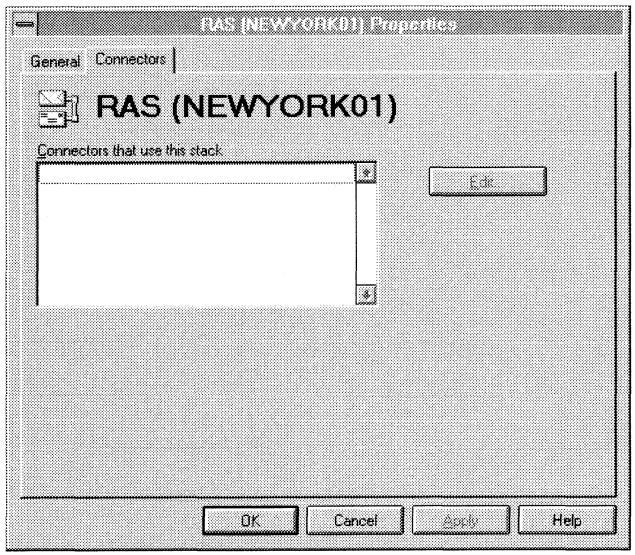
Permissions

You can assign permissions for the RAS MTA transport stack for Microsoft Windows NT accounts. For more information on permissions, see *Microsoft Exchange Server Getting Started.*

Defined RAS Connectors

Each Dynamic RAS Connector you install on this RAS MTA transport stack is displayed in the **Connectors** property page. You can view all the connectors using the MTA transport stack and make modifications if necessary.

1. Select the **Connectors** tab.



2. In the **Connectors that use this stack** box, select a connector.
3. Choose **Edit** to display the Dynamic RAS Connector property pages and make modifications if necessary.

Dynamic RAS Connector Installation

You install the Dynamic RAS Connector from the **Connections** container in the local site.

Note Before you can install the Dynamic RAS Connector, you must install at least one RAS MTA transport stack.

---

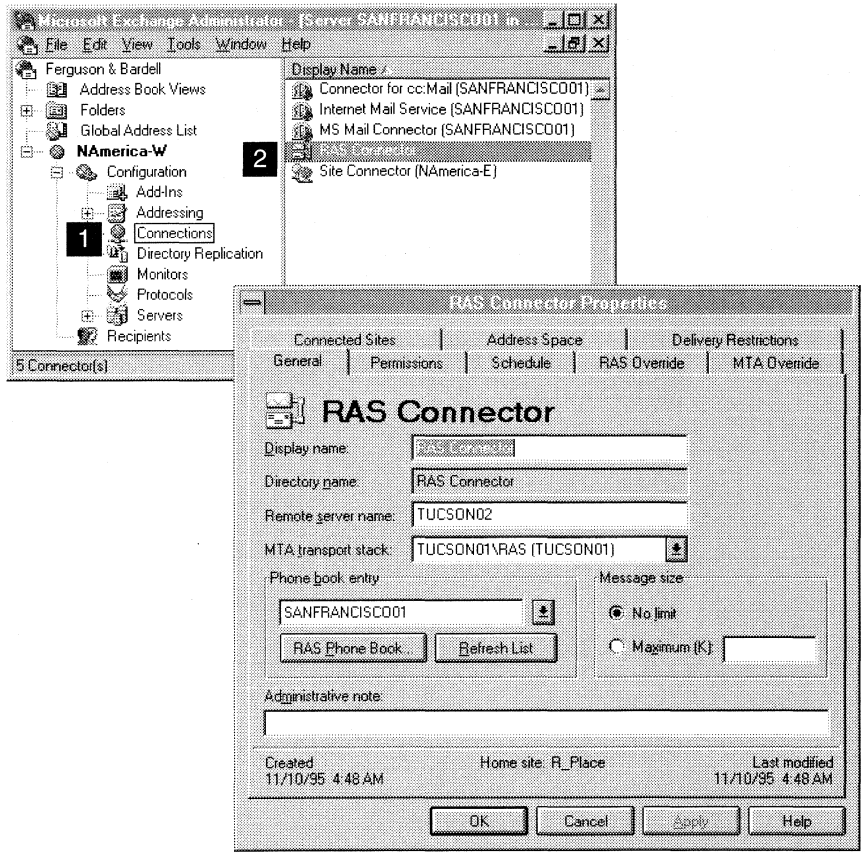
1. Select the **Connections** object for the local site.
2. From the **File** menu, choose **New Other**, and then choose **Dynamic RAS Connector**.

Dynamic RAS Connector Configuration

You configure the Dynamic RAS Connector using property pages to specify connection information, MTA and RAS override values, address spaces, connected sites information, a connection schedule, and delivery restrictions.

Getting to the Dynamic RAS Connector property pages

1. In the Administrator window, choose **Connections**.
2. Double-click the Dynamic RAS Connector to be modified.



General Properties

Use the **General** property page to specify the name for this connector, the name of the server to connect to, the transport stack for this connector, the RAS phone book entry, and a message size limit.

Getting to the General property page

1. In the Administrator window, choose **Connections**.
2. Double-click the Dynamic RAS Connector to be modified.
3. Select the **General** tab.

Specifying the Connector Name

Use the **General** property page to define a name for this Dynamic RAS Connector. The directory name cannot be changed once it is entered.

1. Select the **General** tab.
2. Type the directory name and the display name.

Option	Description
Display name	Type the name (up to 256 alphanumeric characters) that will be displayed in the Administrator window. This name is not case-sensitive.
Directory name	Type an informative and descriptive name (up to 64 alphanumeric characters). This permanent name identifies the Dynamic RAS Connector in the directory and is used in event log messages. You can modify this name only when creating a new transport stack. This name is not case-sensitive.

Specifying the Name of the Remote Server

Use the **General** property page to specify the name of the remote server. The name of the remote server is specified on the **General** property page of the Message Transfer Agent object of the remote server.

1. Select the **General** tab.
2. Specify the remote server name. This field is case-sensitive.

Specifying the MTA Transport Stack

Use the **General** property page to specify the MTA transport stack for the Dynamic RAS Connector.

1. Select the **General** tab.
2. Select a RAS MTA transport stack from the list.

Specifying the Phone Book Entry

Use the **General** property page to specify the phone book entry for the remote server. The phone book entry is part of the Windows NT Server RAS software.

Note In the configuration of the RAS phone book entry, if you choose to use the credentials of the logged on user, the RAS Connector uses the service account specified during setup. Therefore, the service account must have full Administrator permissions on the remote site. In addition, the credentials supplied by the remote system must be granted full Administrator permissions on the local system.

If you do not choose to use the credentials of the logged on user, the RAS Connector uses the values specified in the RAS **Override** property page.

---

1. Select the **General** tab.
2. Select the phone book entry or add a phone book entry for the remote server.

Option	Description
Phone book entry	The RAS phone book entry for the remote server.
RAS Phone Book	Displays the RAS phone book.
Refresh List	Refreshes the list of available phone book entries.

For more information about using the phone book entry, see your Windows NT Server documentation.

Specifying the Message Size

You can specify the size of messages transported through the Dynamic RAS Connector.

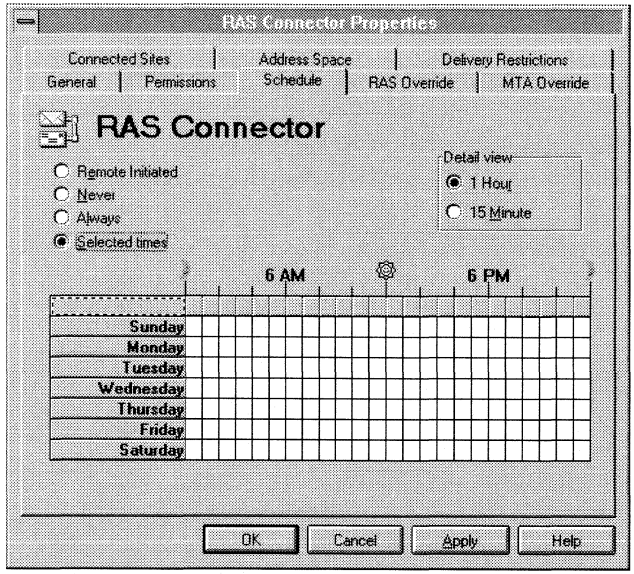
1. Select the **General** tab.
2. In the **Message size** box, select an option. Selecting **No limit** transfers messages of any size. Selecting **Maximum (K)** lets you specify a number between 1 and 9,999,999 kilobytes (KB).

Schedule Properties

Use the **Schedule** property page to specify when to connect to the remote server.

Getting to the Dynamic RAS Connector Schedule property page

1. In the Administrator window, choose **Connections**.
2. Double-click the Dynamic RAS Connector you want to modify.
3. Select the **Schedule** tab.



Setting a Schedule for the Dynamic RAS Connector

You can configure the Dynamic RAS Connector to establish a connection with the remote server at specified times. This is useful when you want to reduce costs for connections where telephone charges apply.

1. Select the **Schedule** tab.
2. Select Remote initiated, Never, Always, or Selected times.

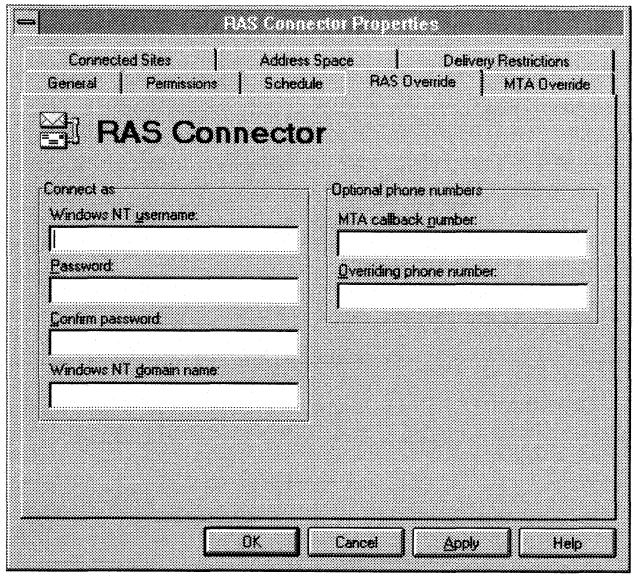
Option	Description
Remote initiated	Sends messages queued at this MTA only when the remote MTA connects to this MTA. Only one of the two MTAs can be configured for remote initiation; otherwise, messages won't be delivered.
Never	Disables the connector.
Always	Sends requests to the target server for messages when there is a message in the outgoing queue.
Selected times	Select a time or block of time in the schedule grid to assign specific connection times.
1 Hour	Displays the schedule grid in one-hour increments.
15 Minute	Displays the schedule grid in 15-minute increments.

RAS Override Properties

Use the **RAS Override** property page to provide account information used to log on to the remote system. This is recommended when the remote site is in a non-trusted Windows NT domain. Values entered on the **RAS Override** property page affect the operation of this connector only.

Getting to the RAS Override property page

1. In the Administrator window, choose **Connections**.
2. Double-click the Dynamic RAS Connector you want to modify.
3. Select the **RAS Override** tab.



Setting RAS Override Properties

The local MTA uses the account information specified on the **RAS Override** property page to provide authentication credentials to connect to the remote site. The account information specified on the **RAS Override** property page must be an authorized account in the remote system that can both log on to the remote system over RAS and access the Microsoft Exchange Server computer with full permissions. The service account of the remote system is guaranteed to have the required permissions.

Note You must specify either the service account used in the remote site or a Windows NT user account that has Send As and Mailbox Owner (User role) permissions for the Servers or Configuration containers in the remote site.

---

1. Select the **RAS Override** tab.
2. Type the **Windows NT username** and **Password** for the service account in the remote site.
3. Confirm your password and type the **Windows NT domain name** of the remote site.

Setting RAS Phone Numbers

Use the **RAS Override** property page to provide a callback phone number to override the number configured in the RAS MTA transport stack, or to override the phone number in the selected RAS phone book.

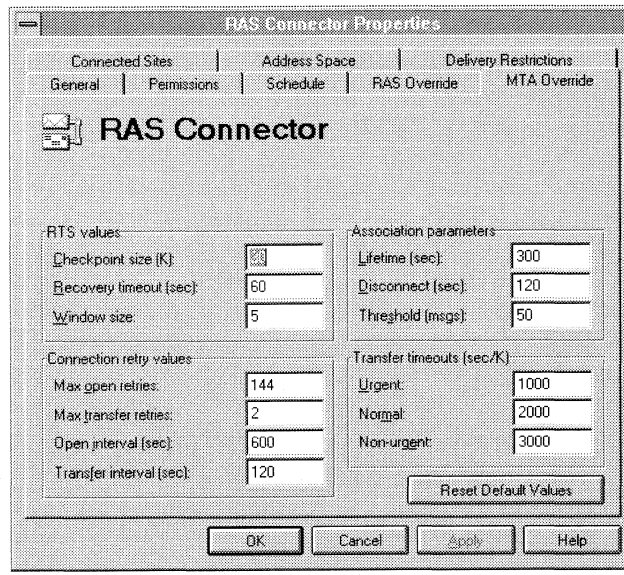
1. Select the **RAS Override** tab.
2. Type the new **MTA callback number** or the **Overriding phone number**.

MTA Override Properties

Use the **MTA Override** property page to change the default Microsoft Exchange Server MTA attributes for the Dynamic RAS Connector. Override options should be changed only when you want to match the configuration of a remote Microsoft Exchange Server computer.

Getting to the MTA Override property page

1. In the Administrator window, choose **Connections**.
2. Double-click the Dynamic RAS Connector to be modified.
3. Select the **MTA Override** tab.



Setting Override RTS Values

Use the **MTA Override** property page to match the configuration of the remote Microsoft Exchange Server. This does not affect message transfer over any other connector. If you do not specify an override value, the MTA uses the default values.

1. Select the **MTA Override** tab.
2. Modify the default **RTS values** as needed.

Option	Description
Checkpoint size (K)	Sets the amount of data to be transferred before a checkpoint is inserted. If an error occurs and the message must be transferred again, the process restarts from the most recent checkpoint. If you specify zero, no checkpoint is set. The default is 30. Using a checkpoint slightly reduces transmission speed. Decrease the checkpoint size when the connection is less reliable.
Recovery timeout (sec)	Determines the amount of time after an error occurs that the MTA waits for a reconnection before deleting checkpointed information and restarting the transfer from the beginning. The default is 60.
Window size	The number of checkpoints that can go unacknowledged before data transfer is suspended. The greater the window size, the greater the transfer rate. The window size determines the amount of resources set aside for the receiving station. Specify window size only if the checkpoint size is greater than zero. The default is 5.

Setting Override Connection Retry Values

Use the **MTA Override** property page to specify how many times the MTA should try to establish a connection.

1. Select the **MTA Override** tab.
2. Modify the default **Connection retry values** as needed.

Option	Description
Max open retries	The maximum number of times the system tries to open a connection before it sends a non-delivery report (NDR). The default is 144.
Max transfer retries	The maximum number of times the system tries to transfer a message across an open connection. The default is 2.
Open interval (sec)	The amount of time to wait before attempting to reopen a connection after an error. The default is 600.
Transfer interval (sec)	The amount of time to wait before resending a message across an open connection after a previous attempt failed. The default is 120.

Setting Override Association Parameters

Use the **MTA Override** property page to set or modify the association parameters between MTAs.

1. Select the **MTA Override** tab.
2. Modify the default **Association parameters** as needed.

Option	Description
Lifetime (sec)	The amount of time to keep an association open to a remote system after a message is sent. The default is 300. When using a RAS connection, 30 seconds is the recommended setting.
Disconnect (sec)	The amount of time to wait before terminating a connection due to a previously terminated association. The default is 120. When using a RAS connection, 15 seconds is the recommended setting.
Threshold (msgs)	The maximum number of queued messages to a remote system. When this is exceeded, the MTA opens another association. The default is 50.

Setting Override Transfer Time-outs

Use the **MTA Override** property page to set the number of times the MTA will try to transfer urgent, normal, or low priority messages.

1. Select the **MTA Override** tab.
2. Modify the default **Transfer timeouts** values as needed.

Option	Description
Urgent	The amount of time (in sec/K) to wait before sending an NDR for an urgent message. The default is 1000.
Normal	The amount of time (in sec/K) to wait before sending an NDR for a normal message. The default is 2000.
Non-urgent	The amount of time (in sec/K) to wait before sending an NDR for a non-urgent message. The default is 3000.

Resetting Override Default Values

Use the **MTA Override** property page to reset the values you previously set.

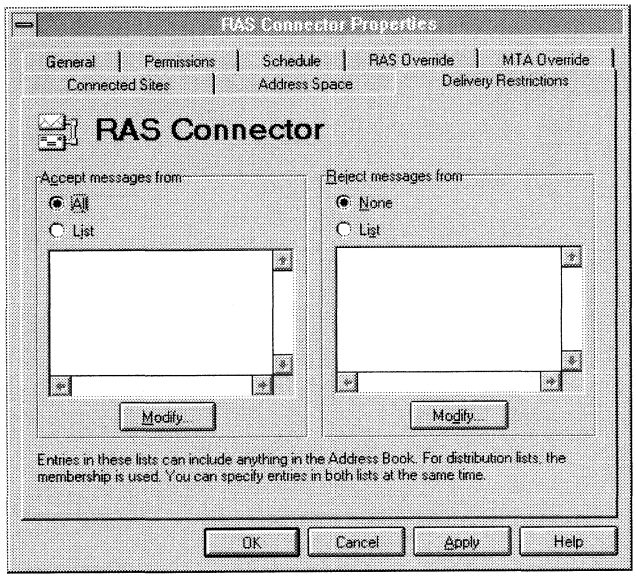
1. Select the **MTA Override** tab.
2. Choose **Reset Default Values**.

Delivery Restrictions

Use the **Delivery Restrictions** property page to accept or reject messages from any sender listed in the directory. For example, if a message is addressed to a remote Microsoft Exchange Server site, it is returned to the sender if the sender's address is in the **Reject messages from** box.

Getting to the Delivery Restrictions property page

1. In the Administrator window, choose **Connections**.
2. Choose the Dynamic RAS Connector to be modified.
3. Select the Delivery Restrictions tab.



Accepting or Rejecting Messages from Specific Senders

You can accept or reject messages from any sender listed in the directory. Delivery restrictions are optional and do not affect incoming messages. The default is to accept messages from all senders and reject messages from none. If you specify even one name in the **Accept messages from** box, messages from all other senders who are not listed in the box are rejected.

Note If a distribution list is specified, the members of the distribution list are used for the restriction, not the distribution list itself.

---

1. Select the Delivery Restrictions tab.
2. Under either Accept Messages from or Reject Messages from, select List.
3. Choose **Modify** to open the Address Book so that you can select from a list of recipients.

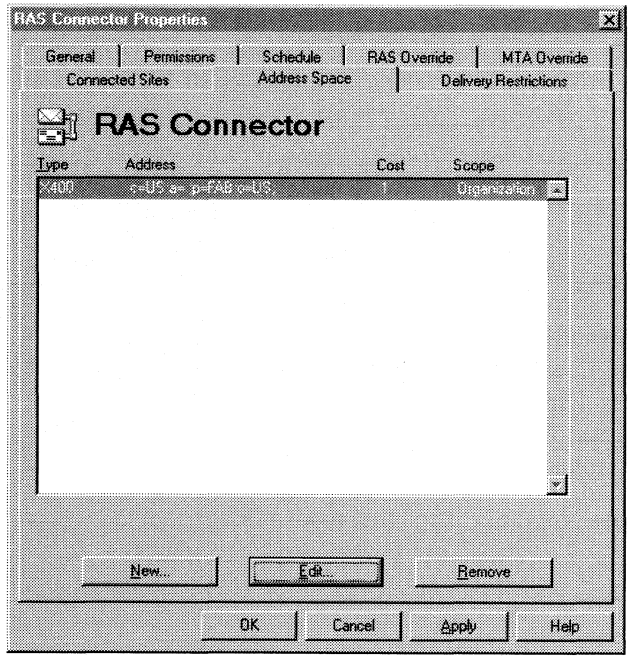
Address Space Properties

You can define the type and format of addresses used to identify messages to another site. Each entry is called an *address space* and contains only as much of the address as necessary to distinguish messages that should be sent through this connector. You need to specify only the necessary address space options that uniquely identify the route to the site. The X.400 address of the remote site is automatically entered in the **Address Space** property page when the Dynamic RAS Connector is created.

The address space cost is used to optimize message routing to the foreign system but does not affect message reception. All mail is sent using the address with the lowest cost. If two or more routes are available with the same cost, the load placed on the routes is roughly equal. Address space costs range from 1 to 100.

Getting to the Address Space property page

1. In the Administrator window, choose **Connections**.
2. Choose the Dynamic RAS Connector to be modified.
3. Select the **Address Space** tab.



Defining Address Spaces

Use the **Address Space** property page to create a new address or modify an existing one.

Note An asterisk (*) can be used for a multicharacter wildcard in an address space. A percent symbol (%) can be used for a single character wildcard.

---

1. Select the **Address Space** tab.
2. Choose **New** to create a new address space or **Edit** to modify an existing address space.

For more information about address spaces, see Chapter 4, "Address Spaces," or *Microsoft Exchange Server Concepts and Planning*.

Assigning an Address Space Cost

Address space costs determine the preference between multiple routes to a remote site. Use the **Address Space** property page to assign a cost.

1. Select the **Address Space** tab.
2. Double-click the address for which you want to assign a cost.
3. In the **Cost** box, type a routing cost for messages transferred using this address.

For more information about costs, see *Microsoft Exchange Server Concepts and Planning*.

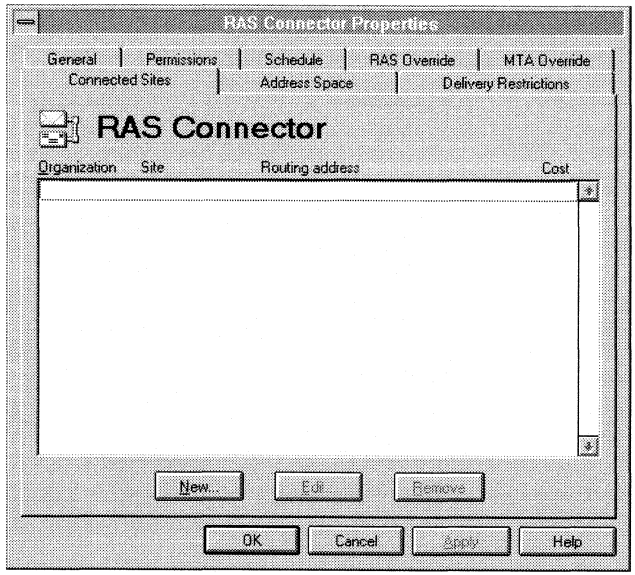
Connected Sites

When the Dynamic RAS Connector is used to connect to an existing Microsoft Exchange Server organization, use the **Connected Sites** property page to ensure directory replication can take place and that other connectors in the organization can be accessed.

Note Connected sites should list only those sites that are directly adjacent to the connector. Knowledge of all other sites will be inherited automatically through directory replication.

Getting to the Connected Sites property page

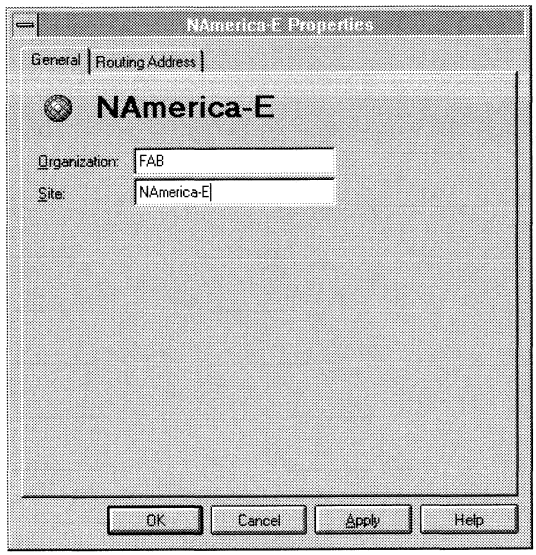
1. In the Administrator window, choose **Connections**.
2. Choose the Dynamic RAS Connector to be modified.
3. Select the **Connected Sites** tab.



Adding or Changing Connected Sites

Use the **Connected Sites** property page to set up or modify the connected site information to another site. The name of the site is the one that is connected with the Dynamic RAS Connector.

1. Select the **Connected Sites** tab.
2. Choose **New** or **Edit**.
3. In the **General** property page, type the organization and site names.



Assigning the Routing Address and Cost for an Indirectly Connected Site

Use the **Routing Address** property page to specify the address of the connected site and the connected site cost. Connected site costs are used to determine the least expensive route from the local site to the remote site. If two or more connectors have the same connected site cost, the load placed on the connectors is roughly equal.

1. Select the **Connected Sites** tab.
2. Choose **New** or **Edit**.
3. In the **General** property page, type the appropriate information.
4. In the **Routing Address** property page, enter the X.400 address found on the **Site Addressing** property page of the **Site Addressing** object on the remote server. It is important to include all spaces. This field is case-sensitive.

For more information about costs, see *Microsoft Exchange Server Concepts and Planning*. For more information about site addresses, see *Microsoft Exchange Server Getting Started.*

Removing a Connected Site

If it is no longer necessary to connect to a specific site, you can remove it from the list.

1. Select the **Connected Sites** tab.
2. Select a site and choose **Remove**.

Permissions

You can assign specific permissions on the Dynamic RAS Connector for Microsoft Windows NT accounts. For more information on permissions, see *Microsoft Exchange Server Getting Started.*

CHAPTER 7

X.400 Connector



You can use an X.400 Connector to establish an *X.400 messaging route* between two Microsoft Exchange Server sites or between a Microsoft Exchange Server site and a *foreign X.400 system.* An X.400 messaging route defines the path that an X.400 message follows to reach its final destination. It allows the message transfer agents (MTAs) in both sites or systems to communicate. A foreign X.400 system is a messaging system other than Microsoft Exchange Server that complies with the 1984 or 1988 X.400 standards.

You can configure multiple X.400 Connectors, each using different transport types. For example, one connector can use Transport Class 0 (TP0)/X.25 and operate only during the day, while another can use Transport Control Protocol/Internet Protocol (TCP/IP) and operate all the time.

When an X.400 Connector is used to connect two sites, one server in each site is configured to provide the communication link. These servers are known as *messaging bridgehead servers.*

Before you install the X.400 Connector, you need to do the following:

- Determine which type of MTA transport stack you will use to connect to the site or foreign system. The MTA transport stack can be X.25, TCP/IP, or Transport Class 4/Connectionless Network Protocol (TP4/CLNP).
- Install the network transport protocols that will be used by the MTA transport stack and test the connection. For example, if you use TCP/IP, you would install TCP/IP on each server and then use **ping** to test the connection.
- Obtain the address of the site or foreign system.

To set up an X.400 Connector, you complete these tasks:

- Install and configure an MTA transport stack on the messaging bridgehead servers in your site and the corresponding transport software on the server in the foreign system.
- Configure the X.400 Connector to communicate with the other site or foreign system.
- Configure the other site or foreign system to communicate with the local server.
- Test the X.400 connection.

Note Before you install an X.400 Connector, verify that the servers in your sites and in the foreign system are installed and running correctly, and that all required Microsoft Exchange Server services have been started.

MTA Transport Stack

An MTA transport stack contains configuration information about the network software and hardware on the local computer running the Microsoft Exchange Server. The network software and hardware are responsible for routing messages between two sites or from one site to a foreign X.400 system. Multiple transport stacks and X.400 Connectors can be installed on other servers in the same site to provide load balancing and fault-tolerant connections for the remote Microsoft Exchange Server site.

The following MTA transport stacks can be used.

TP0/X.25 using an Eicon port adapter TP0/X.25 provides both dial-up and direct communication in compliance with the OSI X.25 Recommendation. Eicon X.25 network software (and possibly hardware) must be installed and running on the server before installing the MTA transport stack. You can install multiple X.25 transport stacks on a server, and you can install multiple Eicon X.25 port adapters on one server. A separate MTA transport stack is required for each X.25 port on an adapter.

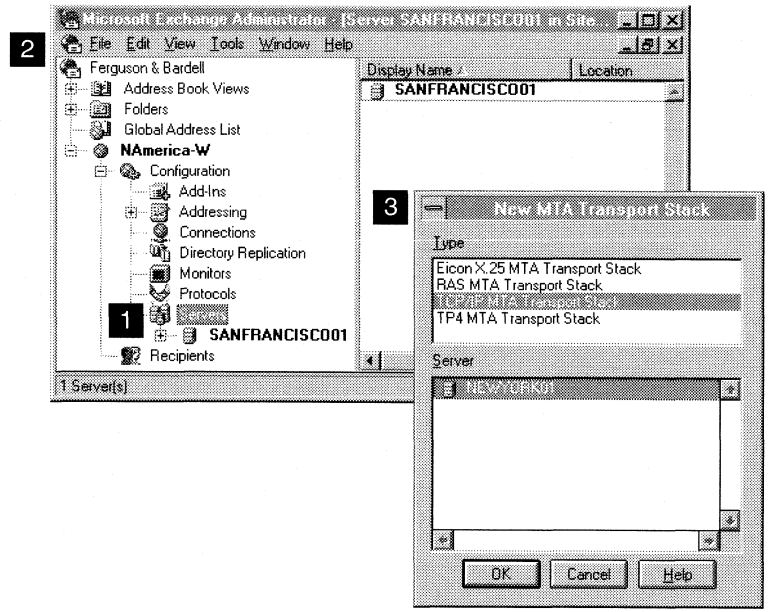
TCP/IP TCP/IP using the RFC 1006 specification is a mechanism for running OSI software, such as X.400 messaging systems, on a TCP/IP network. Microsoft Exchange Server uses Windows NT TCP/IP services. The Microsoft Exchange Server MTA uses port 102 as specified by RFC1006.

TP4/CLNP OSI transport layer protocol TP4/CLNP provides an OSI interface across a local area network (LAN). Microsoft Exchange Server has an interface that allows it to work with the Windows NT TP4 driver. It uses this interface to communicate with other systems using TP4 during message transport. In CLNP, data is transferred without using a connection request. In Windows NT, TP4 is designed for use in a connectionless mode network. TP4 network address information is determined by the server running the transport stack. The network service access point (NSAP) address used by TP4 is configured in the Windows NT Control Panel on that server.

MTA Transport Stack Installation

Before you install an MTA transport stack, verify that the appropriate network software, and possibly hardware, is installed.

1. In the Administrator window, choose a server in your organization.
2. From the **File** menu, choose **New Other**, and then choose **MTA Transport Stack**.
3. In the **Type** box, select the stack to be used.

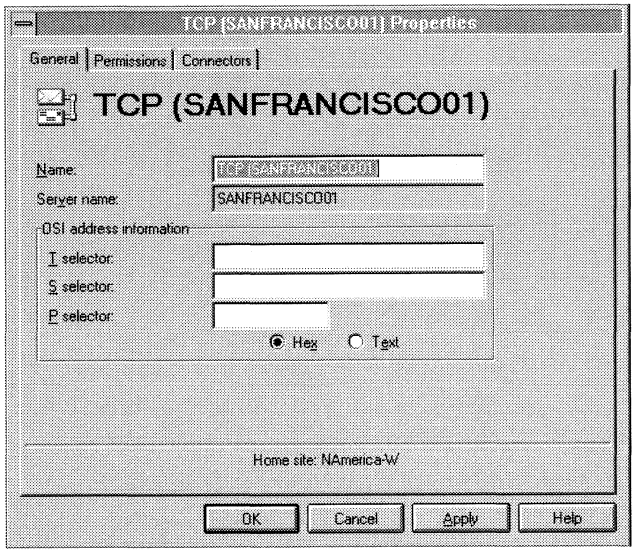


4. In the **Server** box, select the server on which to install the transport stack, and then choose **OK**.

   The property pages that follow will differ depending on the transport stack type you select.

Installing a TCP/IP MTA Transport Stack

Use the **General** property page to configure the TCP/IP MTA transport stack.

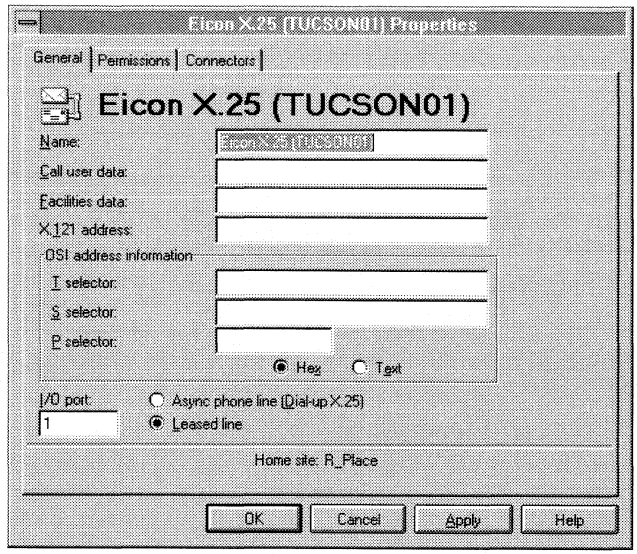


Option	Description
Name	Type a new name or accept the default. You can modify this name only when creating a new transport stack.
Server name	The name of the server where the stack will be installed. If the server name is not correct, you must cancel the task and specify the correct target server.
OSI address information	This section is used to further define the address in cases where other applications or services are using the same transport stack.
T selector	The transport service access point (TSAP). Up to 64 hexadecimal characters (32 characters).
S selector	The session service access point (SSAP). Up to 32 hexadecimal characters (16 characters).
P selector	The presentation service access point (PSAP). Up to 8 hexadecimal characters (4 characters).
Hex	Displays address information as hexadecimal values.
Text	Displays address information as text.

For information about configuring the **Connectors** property page, see "Using the MTA Transport Stack Connectors Property Page" later in this chapter.

Installing an X.25 MTA Transport Stack

Use the **General** property page to configure the X.25 MTA transport stack.



Option	Description
Name	Type a new name or accept the default. You can modify this name only when creating a new transport stack.
Call user data	Supplied by the X.25 provider. Up to 255 hexadecimal characters.
Facilities data	Used for additional information related to connection initiation, such as a reversal of line charges. Up to 218 hexadecimal characters.
X.121 address	The local X.121 address as specified in the X.25 network service setup. Up to 16 numeric characters.
OSI address information	This section is used to further define the address in cases where other applications or services are using the same transport stack.
T selector	The transport service access point (TSAP). Up to 64 hexadecimal characters (32 characters).
S selector	The session service access point (SSAP). Up to 32 hexadecimal characters (16 characters).
P selector	The presentation service access point (PSAP). Up to 8 hexadecimal characters (4 characters).

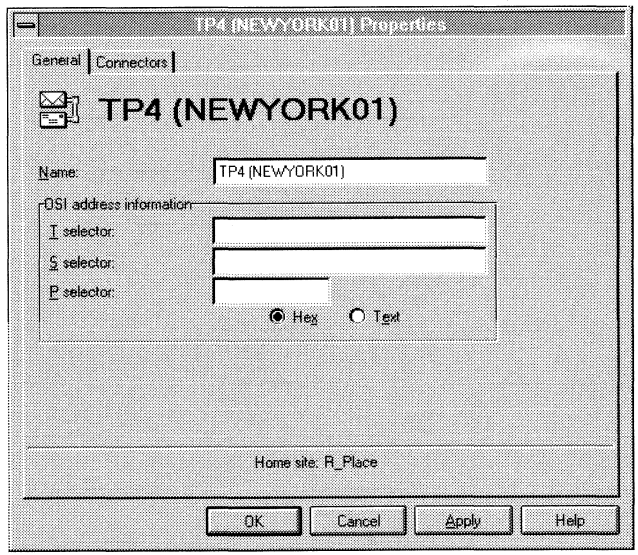
(continued)

Option	Description
Hex	Displays address information as hexadecimal values.
Text	Displays address information as text.
I/O port	The I/O port where the Eicon adapter is installed.
Line type	Determines whether the connection uses a phone line or leased line.

For information about configuring the **Connectors** property page, see "Using the MTA Transport Stack Connectors Property Page" later in this chapter.

Installing a TP4 MTA Transport Stack

Use the **General** property page to configure the TP4 MTA transport stack.



Option	Description
Name	Type a new name or accept the default. You can modify this name only when creating a new transport stack.
OSI address information	This section is used to further define the address in cases where other applications or services are using the same transport stack.
T selector	The transport service access point (TSAP). Up to 64 hexadecimal characters (32 characters).
S selector	The session service access point (SSAP). Up to 32 hexadecimal characters (16 characters).
P selector	The presentation service access point (PSAP). Up to 8 hexadecimal characters (4 characters).
Hex	Displays address information as hexadecimal values.
Text	Displays address information as text.

For information about configuring the **Connectors** property page, see "Using the MTA Transport Stack Connectors Property Page" later in this chapter.

Using the MTA Transport Stack Permissions Property Page

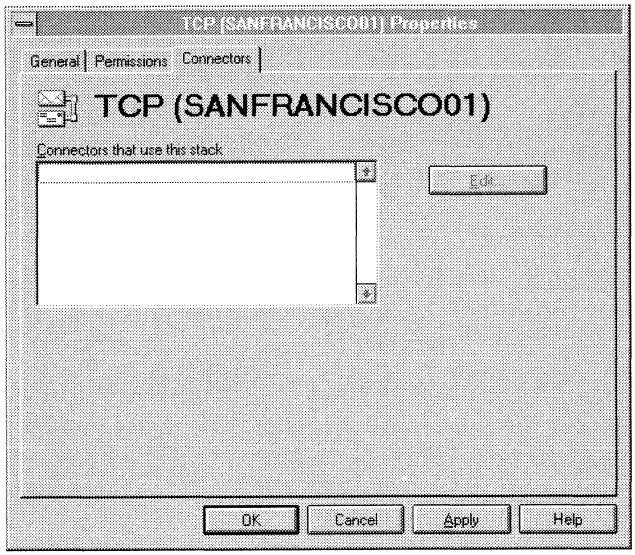
You can assign specific permissions on the MTA transport stack for Windows NT accounts. For more information on permissions, see *Microsoft Exchange Server Getting Started.*

Using the MTA Transport Stack Connectors Property Page

Use the **Connectors** property page to display a list of connectors that use this MTA transport stack. You can select a connector and edit its property pages from this property page.

Getting to the Connectors property page

1. In the Administrator window, choose the server where the MTA transport stack is installed.
2. Double-click the MTA transport stack to be modified.
3. Select the **Connectors** tab.



Option	Description
Connectors that use this stack	A list of all the connectors using this MTA transport stack.
Edit	Allows you to modify the property pages for the specified connector.

X.400 Connector

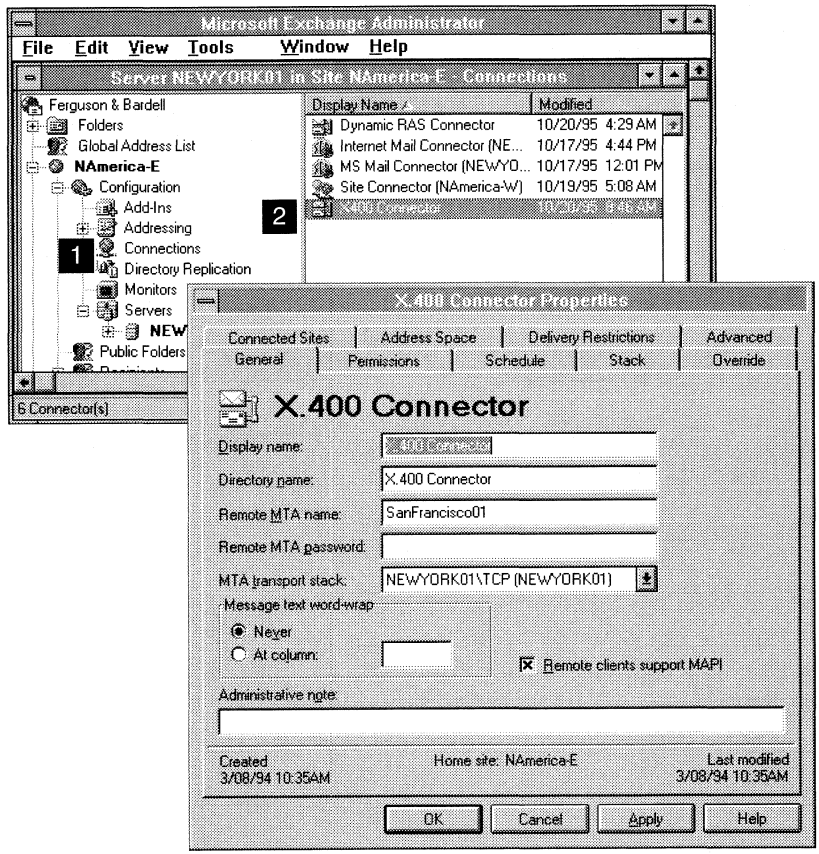
After you have installed an MTA transport stack, you can configure an X.400 Connector to communicate with another site or a foreign system.

The minimum configuration requires that you provide the appropriate information in the following property pages:

Property page	Option
General	Name (up to 64 alphanumeric characters).
	Remote MTA name.
	Remote MTA password (if the remote MTA has a password).
Stack	Specify the interface parameters used to match the configuration of the remote system.
Connected Sites	List the directly adjacent connected sites, or provide an address on the **Stack** property page.
Address Space	Any of the options that are necessary to uniquely identify the route to the foreign system or Microsoft Exchange Server site.
Advanced	Verify that the MTA conformance mode matches the remote MTA conformance mode.

Getting to the X.400 Connector property pages

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified, or follow the procedures in this chapter to install a new connector.



Adding an X.400 Connector

To add a new X.400 Connector to communicate with another site or a foreign system, use the following procedures.

Note The **Type** box shows only MTA transport stack types that have been installed on servers in this site. To install a new type, see "MTA Transport Stack Installation" earlier in this chapter.

1. In the Administrator window, choose a site in your organization.
2. Choose **Connections**.
3. From the **File** menu, choose **New Other**, and then select **X.400 Connector**.
4. In the **Type** box, select the type of MTA transport stack to use for the X.400 Connector.

General Properties

Use the **General** property page to add or modify the remote MTA name and password, define the Microsoft Exchange Server MTA transport stack, specify whether to use word wrap, and enable rich text in outgoing messages.

Getting to the X.400 Connector General property page

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified, or follow the procedures in this chapter to install a new connector.
3. Select the **General** tab.

Specifying the Connector Name

Use the **General** property page to define a name for this X.400 Connector. The directory name cannot be changed once it is entered.

1. Select the **General** tab.
2. Type the directory name and the display name.

Option	Description
Display name	Type the name (up to 255 alphanumeric characters) that will be displayed for the connector in the Administrator window. This name is not case-sensitive.
Directory name	Type an informative, descriptive name (up to 64 alphanumeric characters) for the connector. This permanent name identifies the connector in the directory and is used in event log messages. You can modify this name only when creating a new connector. This name is not case-sensitive.

Adding or Modifying the Remote MTA Name and Password

Use the **General** property page to change the name and password for the remote MTA. The name of the remote MTA of another Microsoft Exchange Server computer is found in the **General** property page of the MTA for that server.

1. Select the **General** tab.
2. Type the name and password of the remote MTA.

Option	Description
Remote MTA name	Type a name up to 32 characters. This name is not case-sensitive.
Remote MTA password	Type a name up to 64 characters. This name is case-sensitive.

Specifying the Remote MTA Transport Stack

The MTA transport stack is used to provide a network connection between two sites or between a site and a foreign X.400 system. You can use an MTA transport stack installed on any computer in your site running the Microsoft Exchange Server. Messages are automatically routed through the server where the MTA transport stack is installed.

Note If the MTA transport stack you want to use does not appear in this list, you must install it or verify that information about an installed stack has been replicated to this server before attempting this procedure.

1. Select the **General** tab.
2. In the **MTA transport stack** box, select the MTA transport stack you want to use with this connector. The default is an alphabetic list of the available transport stacks for this connector type.

Configuring Message Text Word-wrap

You can indicate whether to insert a carriage return at a specific column in outgoing message text.

1. Select the **General** tab.
2. Under **Message text word-wrap**, select an option.

Option	Description
Never	Disables word wrapping.
At column	Specifies the column where a carriage return will be inserted.

Enabling Rich Text for MAPI Client Recipients

You can configure the X.400 Connector to send outbound messages with rich text characters such as bold, color, and italic. Rich text also provides the ability to position attachments. Rich text is a feature that should be used only when the recipient client software is Messaging Application Programming Interface (MAPI) compliant.

Note If you do not select the **Remote clients support MAPI** check box, attachments will be sent to the foreign system with the message. Rich text, icons, and attachment location within the text are discarded before message transfer. If you select this option and the foreign system does not support MAPI, the foreign system displays an extra attachment called Winmail.dat.

---

1. Select the **General** tab.
2. Select or clear the **Remote clients support MAPI** check box.

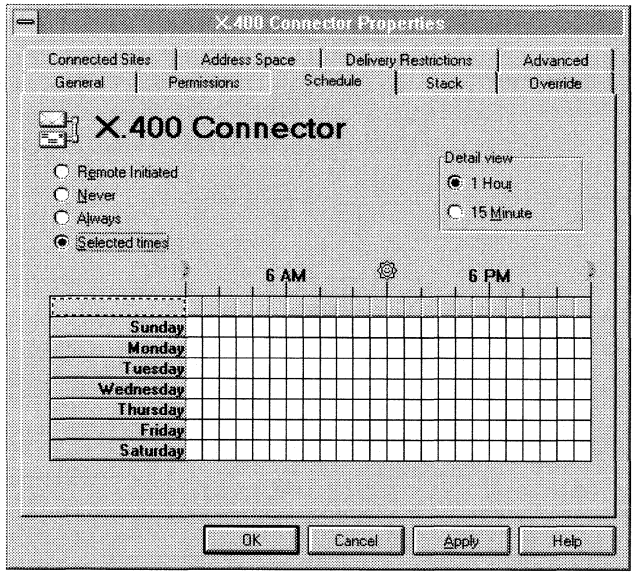
Option	Description
Remote clients support MAPI	Select to send rich text and other MAPI characteristics with messages. MAPI clients support the rich text features in Microsoft Exchange Server. This is the default. Clear when e-mail clients in the foreign system do not support rich text. Rich text and other MAPI characteristics are discarded before the message is sent.

Schedule Properties

Use the **Schedule** property page to specify the time of day when the X.400 Connector will connect to another Microsoft Exchange site or foreign system.

Getting to the X.400 Connector Schedule property page

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified.
3. Select the **Schedule** tab.



Setting the Connection Schedule

Use the **Schedule** property page to specify when and how often an X.400 connection is made. This schedule defines the frequency of connections initiated by Microsoft Exchange Server but does not affect the acceptance or frequency of connections originating from another site or foreign system.

1. Select the **Schedule** tab.
2. Select an option to specify when an X.400 connection is to be made.
3. When you choose **Selected times**, you can select how the schedule grid will be displayed using the **Detail view** options.

Option	Description
Remote Initiated	Sends messages queued at this MTA when the remote MTA connects to this MTA. Both MTAs must have the **Two way alternate** option selected in the **Advanced** property page. Only one of the two MTAs can be configured for remote initiation; otherwise, messages won't be delivered.
Never	Disables the X.400 Connector.
Always	Connects whenever messages need to be transferred. This is the default.
Selected times	Assigns specific times in the schedule grid when the X.400 Connector will initiate a connection. Select a time or block of time in the schedule grid.
Detail view	Used with the **Selected times** option. Select **1 Hour** to display the schedule grid in one-hour increments. Select **15 Minute** to display the schedule grid in 15-minute increments.

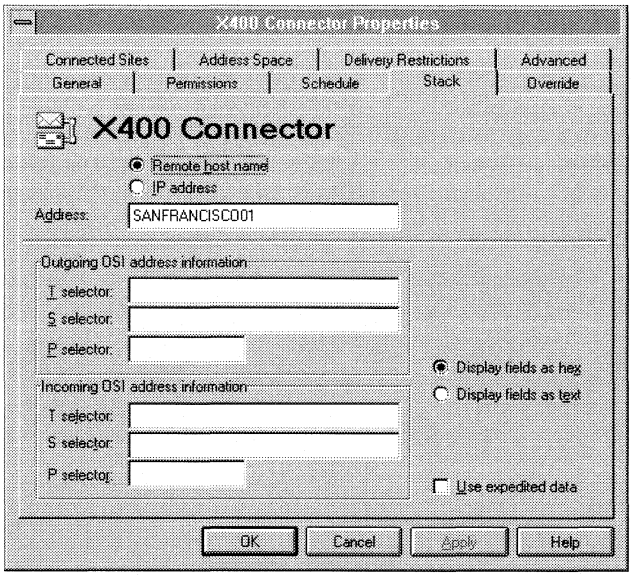
Stack Properties

Use the **Stack** property page to specify transport address information about the server or foreign system you want to connect to. Information displayed in the **Stack** property page is based on the MTA transport stack type you selected for the X.400 Connector.

Note Information in the X.400 Connector **Stack** property page must match the transport configuration on the server or foreign system for the connection to work.

Getting to the X.400 Connector Stack property page

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified.
3. Select the **Stack** tab.



Connecting to a Site or Foreign System Using TCP/IP

Use the **Stack** property page to configure a server to connect to another site or foreign system using TCP/IP.

Note You can obtain values for another site from the **General** property page of the server you plan to connect to.

You can obtain information for the selector options from the system's transport configuration utility or the administrator.

---

1. Select the **Stack** tab.
2. Enter the appropriate information about the Microsoft Exchange Server site or foreign system.

Option	Description
Remote host name	Select to use the name of the Microsoft Exchange Server computer.
IP address	Select to use the Internet protocol (IP) address for the remote site.
Address	Type the name or IP address of the remote site. The IP address is in the format *XXX.XXX.XXX.XXX*, where *XXX* is a decimal value from 0 to 255.
T selector	The transport service access point (TSAP). Up to 64 hexadecimal characters (32 characters).
S selector	The session service access point (SSAP). Up to 32 hexadecimal characters (16 characters).
P selector	The presentation service access point (PSAP). Up to 8 hexadecimal characters (4 characters).
Display fields as hex	Displays address information as hexadecimal values.
Display fields as text	Displays address information as text.
Use expedited data	Increases the speed of communications over networks that recognize data packets identified for accelerated transfer. Some networks require the use of expedited data. For more information, see your TCP/IP documentation.

Connecting to a Site or Foreign System Using X.25

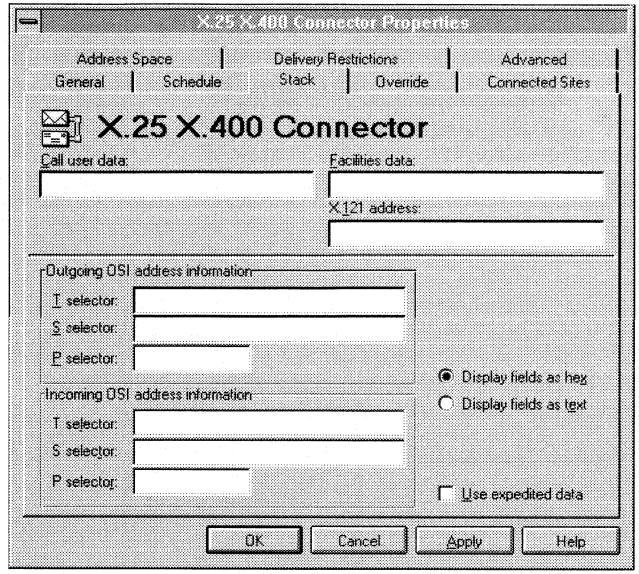
Use the **Stack** property page to configure a server to connect to another site or foreign system using X.25.

Note You can obtain values for another site from the **General** property page of the server you plan to connect to.

You can obtain information for the selector options from the system's transport configuration utility or the X.25 service provider.

---

1. Select the **Stack** tab.
2. Enter the appropriate information about the Microsoft Exchange Server site or foreign system.



Option	Description
Call user data	Supplied by the X.25 provider. Up to 255 hexadecimal characters.
Facilities data	Used for additional information related to connection initiation, such as a reversal of line charges. Up to 218 hexadecimal characters.
X.121 address	The local X.121 address as specified in the X.24 network service setup. Up to 16 numeric characters.
T selector	The transport service access point (TSAP). Up to 64 hexadecimal characters (32 characters).
S selector	The session service access point (SSAP). Up to 32 hexadecimal characters (16 characters).
P selector	The presentation service access point (PSAP). Up to 8 hexadecimal characters (4 characters).
Display fields as hex	Displays address information as hexadecimal values.
Display fields as text	Displays address information as text.
Use expedited data	Increases the speed of communications over networks that recognize data packets identified for accelerated transfer. Some networks require the use of expedited data. For more information, see your X.25 documentation.

Connecting to a Site or Foreign System Using TP4

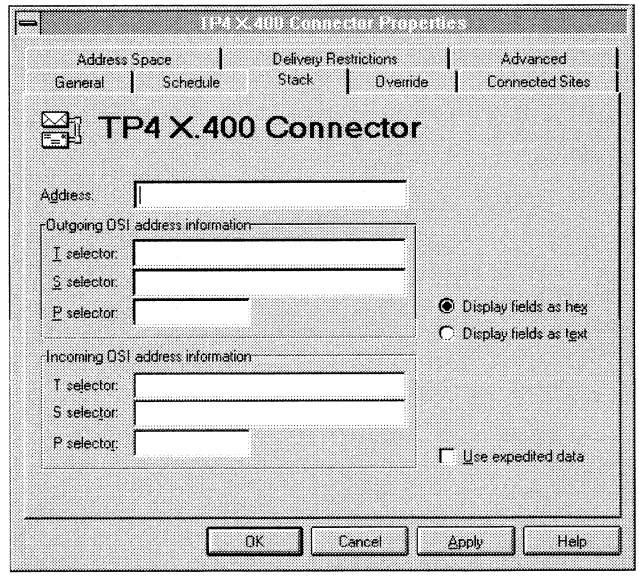
Use the **Stack** property page to configure a server to connect to another site or foreign system using TP4.

Note You can obtain values for another site from the **General** property page of the server you plan to connect to.

You can obtain address information from the TP4 transport configuration or the foreign system's administrator. Obtain selector information from the system's transport configuration utility or the TP4 provider.

---

1. Select the **Stack** tab.
2. Enter the appropriate information about the site or foreign system.



Option	Description
Address	The network service access point (NSAP) or the Windows NT Server name associated with the NSAP.
T selector	The transport service access point (TSAP). Up to 64 hexadecimal characters (32 characters).
S selector	The session service access point (SSAP). Up to 32 hexadecimal characters (16 characters).
P selector	The presentation service access point (PSAP). Up to 8 hexadecimal characters (4 characters).
Display fields as hex	Displays address information as hexadecimal values.
Display fields as text	Displays address information as text.
Use expedited data	Increases the speed of communications over networks that recognize data packets identified for accelerated transfer. Some networks require the use of expedited data. For more information, see your TP4 documentation.

Override Properties

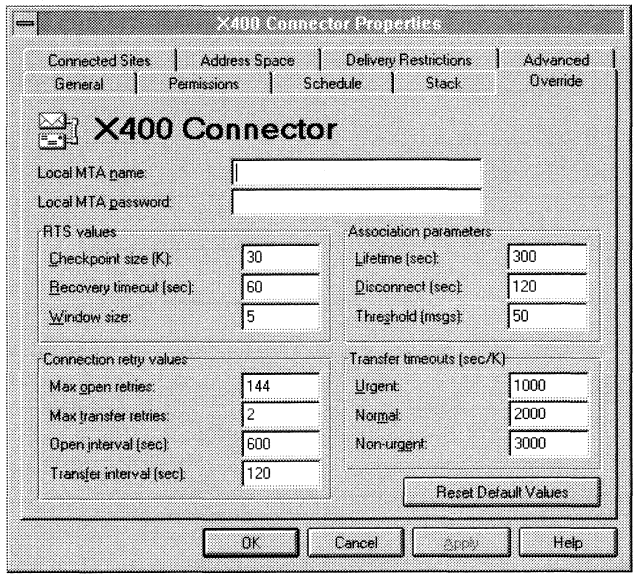
Use the **Override** property page to change the default Microsoft Exchange Server MTA attributes when using a specific X.400 Connector. Override options should be used to establish communication with a foreign system (only when necessary). For example, you can configure an override MTA name and password to be used when connecting to a foreign system if the local MTA name and password are longer than the foreign system can accept. This does not affect message transfer over any other connector.

You also use this property page to configure message transfer to a particular foreign system manually. This does not affect message transfer over any other connector. If you do not specify an override value, the MTA uses the default values when connecting to a foreign system.

For more information on X.400 MTAs and the message transfer process, see *Microsoft Exchange Server Concepts and Planning.*

Getting to the X.400 Connector Override property page

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified.
3. Select the **Override** tab.



Overriding the Local MTA Name and Password

Use the **Override** property page to override the MTA name and password of the local server. This is helpful when the Microsoft Exchange Server name is longer than the foreign system can accept.

1. Select the **Override** tab.
2. Type the local MTA name and password.

Option	Definition
Local MTA name	The name to be used when the Microsoft Exchange Server name is too long or contains characters that the foreign system MTA cannot accept.
Local MTA password	The local password that the foreign X.400 MTA uses to connect to the Microsoft Exchange Server.

Setting Override RTS Values

Use the RTS values to modify values for checkpoint size, recovery timeout, and window size. If you do not specify an override value, the MTA uses the default values or negotiates a configuration automatically when connecting to a foreign system.

1. Select the **Override** tab.
2. Modify the default **RTS Values** as needed.

Option	Definition
Checkpoint size (K)	Sets the amount of data to be transferred before a checkpoint is inserted. If an error occurs and the message must be retransferred, the process restarts from the most recent checkpoint. If you specify zero, no checkpoint is set. The default is 30. Using a checkpoint slightly reduces transmission speed. Decrease the checkpoint size when the link is less reliable.
Recovery timeout (sec)	Determines the amount of time after an error occurs that the MTA waits for a reconnection before deleting checkpointed information and restarting the transfer from the beginning. The default is 60.
Window size	The number of checkpoints that can go unacknowledged before data transfer is suspended. The greater the window size, the greater the transfer rate. The window size determines the amount of resources set aside for the receiving station. Specify window size only if the checkpoint size is greater than zero. The default is 5.

Setting Override Connection Retry Values

Use the **Override** property page to specify how many times the MTA should try to establish a connection. If you do not specify an override value, the MTA uses the default values or negotiates a configuration automatically when connecting to a foreign system.

1. Select the **Override** tab.
2. Modify the default connection retry values as needed.

Option	Description
Max open retries	The maximum number of times the system tries to open a connection before it sends a non-delivery report (NDR). The default is 144.
Max transfer retries	The maximum number of times the system tries to transfer a message across an open connection. The default is 2.
Open interval (sec)	The amount of time to wait before attempting to reopen a connection after an error. The default is 600.
Transfer interval (sec)	The amount of time to wait before resending a message across an open connection after a previous attempt failed. The default is 120.

Setting Override Association Parameters

Use the **Override** property page to set or modify the association parameters between MTAs. If you do not specify an override value, the MTA uses the default values or negotiates a configuration automatically when connecting to a foreign system.

1. Select the **Override** tab.
2. Modify the default association parameter values as needed.

Option	Description
Lifetime (sec)	The amount of time to keep an association open to a remote system after a message is sent. The default is 300.
Disconnect (sec)	The amount of time to wait before terminating a connection due to a previously terminated association. The default is 120.
Threshold (msgs)	The maximum number of queued messages to a remote system. When this is exceeded, the MTA opens another association. The default is 50.

Setting Override Transfer Timeouts

Use the **Override** property page to set the number of times the MTA will try to transfer urgent, normal, or non-urgent messages. If you do not specify an override value, the MTA uses the default values or negotiates a configuration automatically when connecting to a foreign system.

1. Select the **Override** tab.
2. Modify the default transfer timeout values as needed.

Option	Description
Urgent	The amount of time (in sec/K) to wait before sending an NDR for an urgent message. The default is 1000.
Normal	The amount of time (in sec/K) to wait before sending an NDR for a normal message. The default is 2000.
Non-urgent	The amount of time (in sec/K) to wait before sending an NDR for a non-urgent message. The default is 3000.

Resetting Override Default Values

You can reset the **Override** property page values to their default settings.

1. Select the **Override** tab.
2. Choose **Reset Default Values** to return the default values.

Address Space Properties

Use the **Address Space** property page to define the type and format of addresses used to identify messages to another site or foreign system. Each entry is called an *address space* and contains only as much of the address as is necessary to distinguish messages that should be sent through this connector. You need to configure only the necessary X.400 address space options to uniquely identify the route to the site or foreign system.

For example, if you want to use this connector to route only X.400 messages to a foreign system called Ferguson and Bardell (FAB), type the following in the **Address Space** property page:

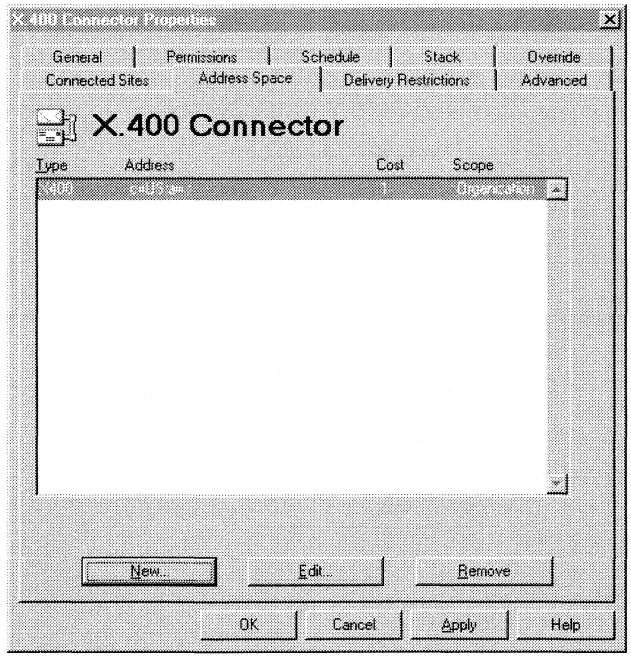
```
Private Management Domain Name (p) = FAB
Administrative Management Domain Name (a) = mci
Country (c) = us
```

The cost associated with each address space is used to optimize message routing to the foreign system but does not affect message reception. Lower cost address spaces take precedence over higher cost address spaces. If two or more routes are available with the same cost, the load placed on the routes is roughly equal. Routing costs range from 1 to 100.

Note The **Connected Sites** property page also contains address information, but is used only when connecting to other Microsoft Exchange Server sites.

Getting to the X.400 Connector Address Space property page

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified.
3. Select the **Address Space** tab.



Specifying the X.400 Connector Address Space

Use the **Address Space** property page to create a new address or modify an existing address space.

Note An asterisk (*) can be used for a multicharacter wildcard in an address space. A percent symbol (%) can be used for a single character wildcard.

1. Select the **Address Space** tab.
2. Choose **New** to create a new address space, or **Edit** to modify an existing address space.

For more information about address spaces, see Chapter 4, "Address Spaces" or *Microsoft Exchange Server Concepts and Planning*.

Connected Sites

When the X.400 Connector is used to connect to an existing Microsoft Exchange Server organization, use the **Connected Sites** property page to verify that directory replication can take place and that other connectors in the organization can be accessed.

Note Connected sites should list only those sites that are directly adjacent to the connector. Knowledge of all other sites will be inherited automatically through directory replication.

Getting to the Connected Sites property page

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified.
3. Select the **Connected Sites** tab.

Adding or Changing a Connected Site

Use the **Connected Sites** property page to set up or modify an X.400 connection to another site.

1. Select the **Connected Sites** tab.
2. Choose **New** or **Edit**.
3. In the **General** property page, enter the appropriate information.

Option	Description
Organization	The organization name of the Microsoft Exchange Server. This is the directory name of the organization container.
Site	The name of the site to connect to.

Removing Connected Sites

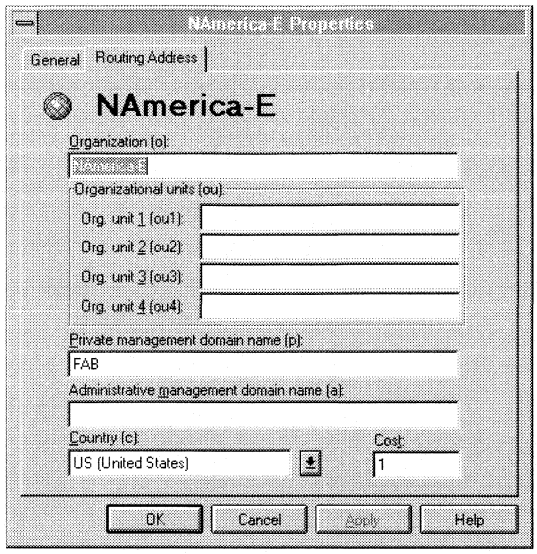
If you no longer want to connect to a specific site, you can remove it from the list of indirectly connected sites by using the **Connected Sites** property page.

1. Select the **Connected Sites** tab.
2. Select the site name and choose **Remove**.

Assigning the Routing Address and Cost for a Connected Site

Use the **Routing Address** property page to specify the address of the connected site and the connected site cost. Connected site costs determine the preference between bridgehead servers if more than one is available. If two or more servers are available with the same cost, the load placed on servers in the remote site is roughly equal. You access the **Routing Address** property page by choosing **New** or **Edit** in the X.400 Connector **Connected Sites** property page.

1. Select the **Connected Sites** tab.
2. Choose **New** or **Edit**.
3. In the **General** property page, enter the appropriate information.
4. In the **Routing Address** property page, enter the appropriate information.



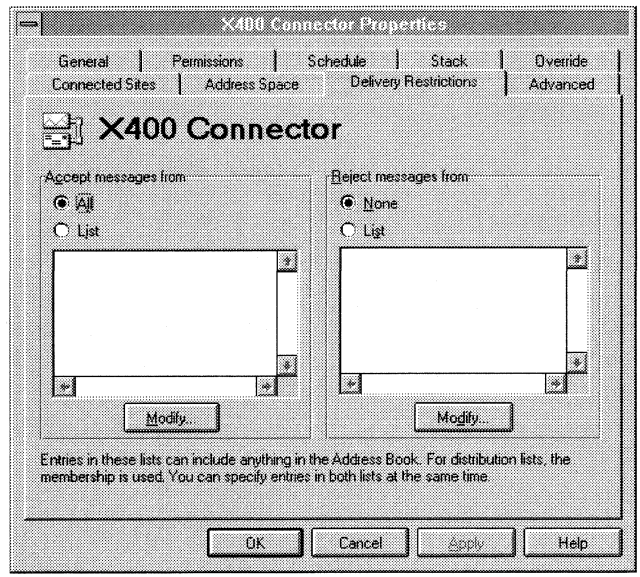
Option	Description
Organization (o)	The organization name where the site is located.
Organizational units (ou)	The X.400 address that identifies the server.
Private management domain name (p)	The X.400 address that identifies the PRMD of the server.
Administrative management domain name (a)	The X.400 address that identifies the ADMD of the server.
Country (c)	The X.400 address that identifies the country of the server.
Cost	Type 1 through 100. The default is 1. This cost is compared with the cost of other bridgehead servers when more than one messaging bridgehead server is available.

Delivery Restrictions

Use the **Delivery Restrictions** property page to accept or reject messages from any sender listed in the directory. For example, if a message is addressed to a foreign system, it is returned to the sender if the sender's address is in the **Reject messages from** box or does not appear in the **Accept messages from** box.

Getting to the X.400 Connector Delivery Restrictions property page

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified.
3. Select the Delivery Restrictions tab.

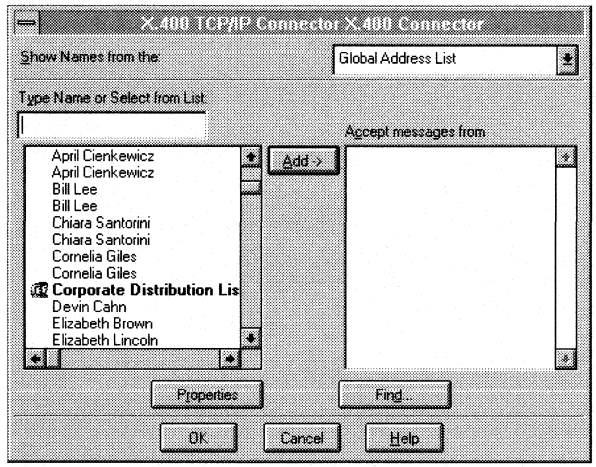


Accepting or Rejecting Messages from Specific Senders

Delivery restrictions are optional and do not affect incoming messages. The default is to accept messages from all senders and reject messages from none. These are senders that are listed in the Microsoft Exchange Server directory.

Note If a distribution list is specified, the members of the distribution list are used for the restriction, not the distribution list itself.

1. Select the **Delivery Restrictions** tab.
2. Under either **Accept messages from** or **Reject messages from**, select **List**.
3. Choose **Modify** to open the Address Book so you can select from a list of recipients.



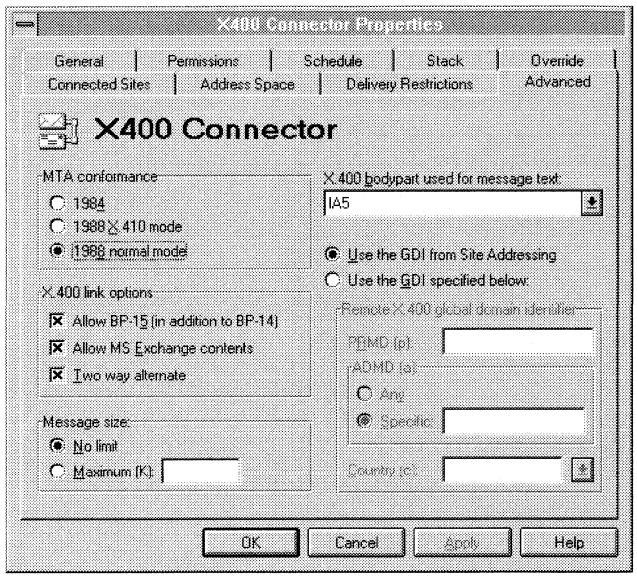
Option	Description
Show Names from the	Select the global address list or a container.
Type Name or Select from List	Type or select one or more names from the list.
Add	Adds the selected names to the **Accept messages from** box.
Properties	Displays the properties of the mailbox.
Find	Opens the **Find** dialog box where you can search for any name based on a variety of properties.

Advanced Properties

Use the **Advanced** property page to specify an MTA conformance mode, X.400 connection options, message size limits, X.400 body parts, and the remote global domain identifier (GDI).

Getting to the X.400 Connector Advanced property page

1. In the Administrator window, choose **Connections**.
2. Double-click the X.400 Connector to be modified.
3. Select the **Advanced** tab.



Configuring MTA Conformance

It is important that the configuration of MTA conformance matches the conformance of the foreign system. The MTA conformance configuration primarily affects outbound messages.

Note Hewlett Packard OpenMail requires the use of X.410 mode, not 1988 normal mode.

---

1. Select the **Advanced** tab.
2. Select a conformance mode.

Option	Description
1984	Conforms to 1984 Recommendations.
1988 X.410 mode	Conforms to 1988 X.410 Recommendations.
1988 normal mode	Conforms to 1988 Recommendations. This is the default.

Specifying X.400 Body Parts

You can specify the body part type to be used for the content of an outbound message. This body part type must be supported by the foreign system and primarily affects outbound messages. This body part specification pertains to inbound IA5 messages if you select the **Convert incoming messages to Microsoft Exchange Contents** check box in the MTA **General** property page. This allows inbound conversion from IA5 Swedish, Norwegian, or German on inbound messages.

1. Select the **Advanced** tab.
2. Under **X.400 bodypart used for message text**, select a body part type.

Specifying X.400 Link Options

Additional parameters may be needed to interoperate with the other site or foreign system. They affect outbound messages only.

1. Select the **Advanced** tab.
2. Under **X.400 link options**, select or clear the options as needed.

Option	Description
Allow BP-15 (in addition to BP-14)	Select to send BP-15 attachments formatted as file transfer body part (FTBP). Clear to send all attachments as BP-14 attachments.
Allow MS Exchange contents	Select to send message content formatted in the Microsoft Exchange Server internal format (MDBEF) when possible. Clear to convert the message format to the standard P2/P22 X.400 format.
Two way alternate	Select to specify that the two communicating MTAs take turns sending and receiving messages.

Setting the Message Size

You can specify a maximum size for messages sent to another site or foreign system. This value should match the message size specified in the other site or foreign system. Verify the message size limit with the foreign system using the system's documentation or by sending test messages after the X.400 Connector configuration is complete.

1. Select the **Advanced** tab.
2. Under **Message size**, select an option.

Option	Description
No limit	Send messages of any size. This is the default.
Maximum (K)	Set a message size from 1 to 2,097,151 kilobytes.

Configuring the Remote Global Domain Identifier

The remote GDI is used to prevent message transfer loops. The GDI is used in a relay scenario and affects outbound messages only.

1. Select the **Advanced** tab.
2. Select either **Use the GDI from Site Addressing** or **Use the GDI specified below**.
3. Under **Remote X.400 global domain identifier**, type or select the foreign system's GDI. This option is available only when you have selected the **Use the GDI specified below** option.

Option	Description
PRMD (p)	The PRMD name.
ADMD (a)	The ADMD name.
Any	Allow the local MTA to select any available ADMD.
Specific	Specify a particular ADMD to use.
Country (c)	Country name of the directly connected foreign X.400 system's GDI.

Permissions

You can assign specific permissions on the X.400 Connector for Microsoft Windows NT accounts. For more information on permissions, see *Microsoft Exchange Server Getting Started.*

Foreign X.400 System Configuration

The connection from the foreign X.400 system to the Microsoft Exchange Server must be established by configuring the foreign system with details about the X.400 Connector. It does not matter if the server or the foreign X.400 system is configured first.

To configure a foreign system, complete the following tasks:

- Determine how the X.400 Connector is to be configured to send messages to the foreign system, including the options for X.400 conformance, stack, and address information.
- Determine what information about the server is needed to configure the foreign X.400 system MTA. If the Microsoft Exchange Server is configured before the foreign system, use the Administrator program to gather the information.

- Configure the foreign MTA to receive messages from the Microsoft Exchange Server using the configuration procedure or utility for the foreign X.400 system.

Microsoft Exchange Server accepts several content and body part types. For reliable message exchange, verify that the configuration of the server and the foreign X.400 system match.

Use the following table to determine the location of options in the Administrator program.

Option	Administrator program
MTA name and password	X.400 Connector **General** property page
Message size limit	X.400 Connector **Advanced** property page
Local transport stack address	X.400 Connector **Stack** property page
Override MTA name and password	X.400 Connector **Override** property page
MTA conformance options	X.400 Connector **Advanced** property page
MTA parameters and retry intervals	X.400 Connector **Override** property page
MTA reliable transfer service settings	X.400 Connector **Override** property page
X.400 message content and body part	X.400 Connector **Advanced** property page
Connection schedule	X.400 Connector **Schedule** property page

Testing X.400 Connections to Foreign Sites

When you finish configuring a connection between Microsoft Exchange Server and a foreign system, you should test it before allowing general message transfer or starting any message-based services.

1. Send a message from the local site to the foreign X.400 system using any Microsoft Exchange Server client. To test MAPI message encapsulation, include rich text formatting and an attachment, such as a file or embedded OLE object, to verify preservation of X.400 message contents and body parts.
2. Verify that the message arrives at the foreign system recipient's mailbox.
3. Examine the message text, formatting, and attachments.
4. Messages viewed with an X.400 client should contain plain text and file attachments, plus an attachment containing all the attributes the X.400 client cannot display. Messages viewed with a Microsoft Exchange Server client or another MAPI client should contain rich text and all attachments.
5. Send a message from the foreign X.400 system to the local site using the appropriate X.400 user agent program (client).

6. Verify that the message arrives at the local recipient's mailbox.
7. If the message is delayed or does not arrive, use the Windows NT Event Viewer to examine the Windows NT application event log for a cause. Microsoft Exchange Server MTA activity is logged as ExchangeMTA for message transfer to and from foreign systems.

For more information on using the event logs and diagnostics logging to track messaging difficulties, see *Microsoft Exchange Server Maintenance and Troubleshooting.*

Testing Connections to Another Site

When you finish configuring an X.400 connection between two sites, you should test the connection before starting any message-based service, such as directory or public folder replication.

1. Send a message from one site to the other using client software.
2. Include rich text formatting and an attachment, such as a file or embedded OLE object, to verify proper transmission of X.400 message contents and body parts.
3. Verify that the message arrives at the recipient's mailbox.
4. Send a message or a reply from the remote site to the local site using client software.
5. If either message arrives but is missing rich text formatting or any attachments, verify that the X.400 Connector in each site allows the transmission of either or both TNEF-encapsulated attachments and MDBEF message contents.
6. If the message is delayed or does not arrive, use the Windows NT Event Viewer to examine the Windows NT application event log for a cause. The Microsoft Exchange Server MTA activity is logged as ExchangeMTA for all message transfer to and from remote sites.

For more information on using the event logs and diagnostics logging to track messaging difficulties, see *Microsoft Exchange Server Maintenance and Troubleshooting.*

Removing X.400 Connectors

You can temporarily stop the flow of messages by reconfiguring the X.400 Connector, or you can stop message transfer permanently by deleting the X.400 Connector or transport stack.

To remove the X.400 Connector, complete the following procedures:

1. Notify users on both systems that the connection is being removed.
2. Prevent new messages from being routed to the connector by selecting **Never** in the **Schedule** property page.

   Note If messages are addressed to a foreign system serviced by a connector with a scheduled connection time set to **Never**, the message remains in the queue until it expires or the connection is restored.

3. Allow sufficient time for queued messages to be transmitted.

   You can initiate immediate transmission of queued messages by temporarily selecting **Always** in the **Schedule** property page.
4. Stop the X.400 Connector by removing all entries in the **Address Space** property page.

   Note Messages sent to a destination address that has been deleted are returned to the sender as non-deliverable.

5. Delete the X.400 Connector from the organization hierarchy in the Administrator window.

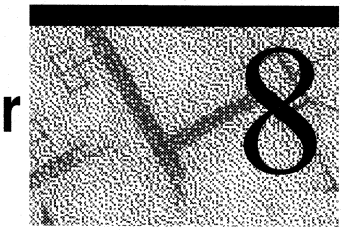
   Note All settings for this X.400 Connector are discarded.

6. Stop the Microsoft Exchange Server or foreign system MTA from connecting or transmitting messages to the local Microsoft Exchange Server by using the configuration utility in the other site or foreign system.
7. Remove the MTA transport stack software and hardware from both the Microsoft Exchange Server and foreign X.400 system.

   Caution Removing a Microsoft Exchange Server MTA transport stack immediately deletes all X.400 Connectors using that stack and also deletes all messages in that X.400 Connector's queue.

CHAPTER 8

Microsoft Exchange Connector for Lotus cc:Mail



Microsoft Exchange Server provides connectivity to Lotus cc:Mail systems using the Microsoft Exchange Connector for Lotus cc:Mail.

The connector enables message transfer and directory synchronization using one or multiple connectors depending on your messaging requirements. Each Microsoft Exchange Server in your organization can run one instance of the connector that directly services one connection to a cc:Mail post office. You cannot service one cc:Mail post office from more than one connector.

The Connector for Lotus cc:Mail is configured using the Microsoft Exchange Server Administrator program. You can administer it from any Microsoft Windows NT Workstation or Microsoft Windows NT Server that is part of your network.

Lotus cc:Mail Requirements

The following software must be installed and running on the cc:Mail post office directly connected to the Connector for Lotus cc:Mail:

- Lotus cc:Mail Post Office Database version 6 and cc:Mail Import version 5.15 and Export version 5.14. Though no known incompatibilities exist using Import/Export versions 5.12, it is recommended that you upgrade to Import 5.15 and Export 5.14.

  - or -

- Lotus cc:Mail Post Office Database version 8 and cc:Mail Import/Export version 6.0.

Connector Installation

For each Microsoft Exchange Server computer, there can be only one instance of the connector in operation. However, you can have any number Microsoft Exchange Server computers in your site operating a connector instance.

Connector Setup

Use Microsoft Exchange Server Setup to install:

- The connector extensions, including the cc:Mail e-mail address generator, for communicating with cc:Mail.
- The cc:Mail e-mail address generator for Microsoft Exchange Server computers accessing cc:Mail through a connector installed in another Microsoft Exchange Server site.

Important The Performance Optimizer is crucial to the efficient operation of Microsoft Exchange Server. Under **Type of server**, select **Connector/Directory Import** during optimization. If you skip this step during installation, make sure you complete it before putting the server into service.

Quick Start

To set up the minimum configuration requirements for a connector, use the following list of procedures in the order in which they appear.

Task	Description
Verify that the Import.exe and Export.exe programs are in the system path.	The cc:Mail Import and Export programs must be in the Microsoft Exchange Server system path where the connector is installed.
Configure the connector **Post Office** property page.	Use the Connector **Post Office** property page to assign an administrator's mailbox and establish a local area network (LAN) connection to a cc:Mail post office.
Configure the connector **Export Containers** property page.	Use the **Export Containers** property page to specify the Microsoft Exchange Server recipients that you want exported to the cc:Mail post office directory.
Configure the connector **Import Containers** property page.	Use the **Import Container** property page to specify where to store imported addresses from the cc:Mail post office on a Microsoft Exchange Server.

(continued)

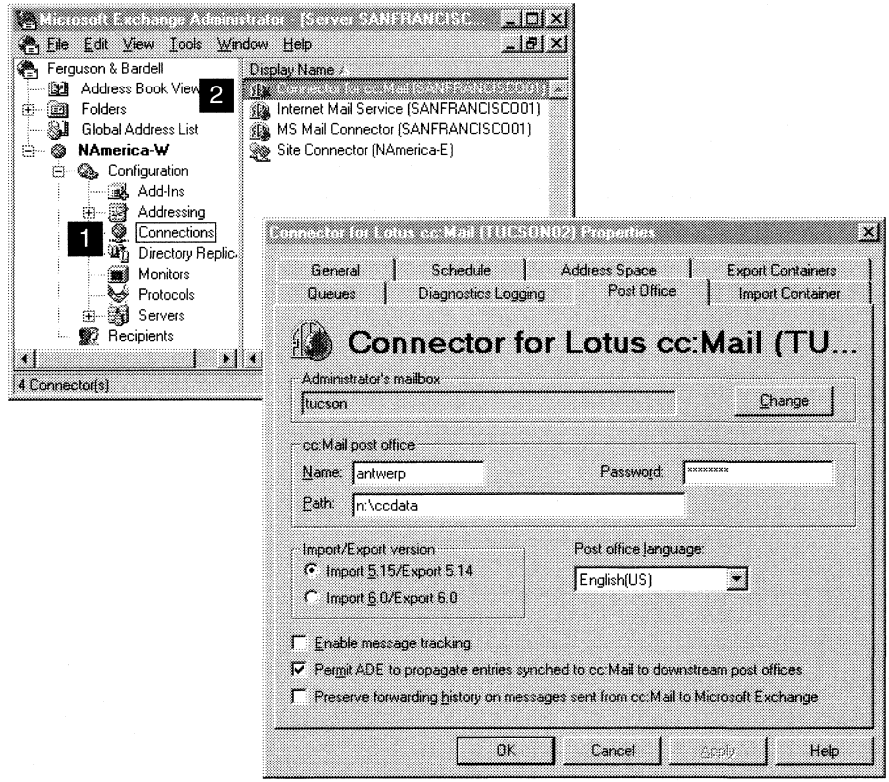
Task	Description
Configure the connector **Address Space** property page.	Use the **Address Space** property page to configure message routing for the connector. The address space can be configured to specify which messages bound for cc:Mail this connector will route.
Start the Connector for cc:Mail Service.	Use Control Panel to start the Connector for cc:Mail Service.
Run directory synchronization.	Use the **Import Container** property page to run a manual directory synchronization cycle for distributing address information between Microsoft Exchange Server and cc:Mail.
Configure the connector **Dirsync Schedule** property page.	Use the **Dirsync Schedule** property page to specify a time when Microsoft Exchange Server sends address list updates to and receives address list updates from the cc:Mail post office.
Test the connection.	Send a message from a Microsoft Exchange server recipient to a cc:Mail recipient and back.

Connector for Lotus cc:Mail Configuration

Use the Microsoft Exchange Server Administrator program to configure the Connector for cc:Mail. Each Microsoft Exchange Server in your organization can run one instance of the connector that directly services one connection to a cc:Mail post office. You cannot service one cc:Mail post office from more than one connector.

Getting to the Connector for Lotus cc:Mail property pages

1. In the Administrator window, choose **Connections**.
2. Double-click the connector to be modified.



Post Office

Use the **Post Office** property page to configure the network connection to the cc:Mail post office that the connector will communicate with directly. In the **Post Office** property page, you can:

- Select an administrator's mailbox.
- Establish a LAN connection to the cc:Mail post office from the connector.
- Select the language the connector will send and accept text messages in.
- Designate the version of cc:Mail Import and Export you are using.
- Enable message tracking for the connector.
- Permit Lotus cc:Mail Automatic Directory Exchange (ADE) to propagate directory synchronized entries to indirect cc:Mail post offices.
- Retain message forwarding history for messages sent from cc:Mail to Microsoft Exchange Server.

Getting to the Post Office property page

1. In the Administrator window, choose the site where the connector is installed, and then choose **Connections**.
2. Double-click **Connector for cc:Mail**.
3. Select the **Post Office** tab.

Assigning an Administrator's Mailbox

Use the **Post Office** property page to assign an administrator's mailbox to receive messages that cannot be converted by the connector.

Tip You can create a mailbox called cc:Mail administrator or a distribution list to receive delivery messages.

---

1. Select the **Post Office** tab.
2. Choose **Change**.
3. Select a recipient for the administrator's mailbox.

Option	Description
Show Names from the	Select the global address list or a container.
Type Name or Select from List	Type a name or select one from the list.
Properties	Display the properties for the mailbox.
Find	Search for a name based on a specific set of criteria.

Specifying the Connected cc:Mail Post Office

Use the **Post Office** property page to specify the cc:Mail post office the connector will communicate with.

Note Before you can connect to a NetWare server, your Windows NT Server must be running the Gateway Services for NetWare.

When typing a network path to a NetWare server, use the uniform naming convention (UNC) format (*\\servername\sharename\path* for a Windows NT Server or *\\servername\volumename\path* for a NetWare server). For example, a cc:Mail post office located on a NetWare server with server name SERVER1, volume name Sys, and directory name Ccdata would require the network path \\Server1\Sys\Ccdata.

---

1. Select the **Post Office** tab.
2. Under **cc:Mail post office**, type the name, path, and password for the cc:Mail post office you are connecting to.

Option	Description
Name	Type the name of the cc:Mail post office (up to 256 characters).
Password	Type the password for the cc:Mail post office (up to 10 characters).
Path	Type the network path to the cc:Mail post office data directory in UNC format. The connector's service account must have read and write permissions for this destination.

Specifying Versions of Import/Export

You must specify the versions of cc:Mail Import and Export that you will be using with the connector. The cc:Mail Import.exe and Export.exe files are necessary for message transfer between the connector and a cc:Mail post office. To determine the version of the Import and Export programs that you are using, type the program name followed by **/?** at the command prompt.

Note If you are using Import/Export 6.0, you must copy \Ccdata\Ccadmin\Ie.ri to the directory where Import.exe and Export.exe are located.

---

1. Select the **Post Office** tab.
2. Under **Import/Export version**, select the version of Import/Export that you are using.

Specifying a Post Office Language

Selecting a language determines the language *code page* used for text sent to and from the connector. A code page is an ordering or encoding of a standard set of characters within a specific locale. Encoding provides a consistent way for messaging systems to exchange and process data. The code page also determines the language the connector uses for sending text strings, such as status messages, to cc:Mail.

Note You may experience language-specific conversion problems when the **Post office language** setting is configured for a language that is different from the language specified in the Windows NT Server Regional Settings application in Control Panel.

---

1. Select the **Post Office** tab.
2. Under **Post office language**, select a language.

Configuring Other Post Office Options

Use the **Post Office** property page to enable message tracking for the connector. Inbound and outbound messages through the connector are reported as message tracking events and can be viewed from the Microsoft Exchange Server Message Tracking Center. When a message is successfully imported from Microsoft Exchange Server into a cc:Mail post office, the action is logged. Similarly, an action is logged when a message has been received by Microsoft Exchange Server from the connector.

Many cc:Mail systems use Lotus cc:Mail Automatic Directory Exchange (ADE) to propagate the contents of an established cc:Mail post office directory to any number of other cc:Mail post offices. The Connector for cc:Mail does not use ADE as the directory synchronization agent between Microsoft Exchange Server and cc:Mail. However, you can configure the connector to propagate address listings resulting from directory synchronization to indirectly connected cc:Mail post offices communicating with ADE.

1. Select the **Post Office** tab.
2. Select or clear the following options.

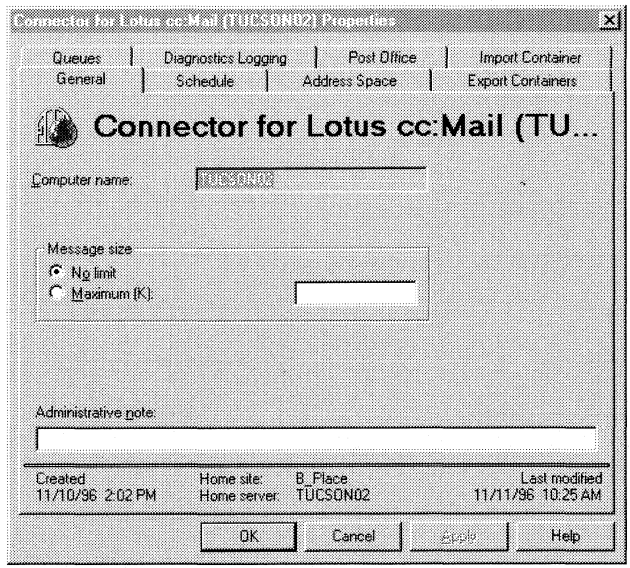
Option	Description
Enable message tracking	Tracks messages through the connector for troubleshooting. When message tracking is enabled, message activities are maintained in a log by the system attendant on Microsoft Exchange Server. The log becomes a trace of the processing of each message as each component receives, processes, and delivers it to the next component. The mail tracking log is stored in \Exchsrvr\Tracking.log.
Permit ADE to propagate entries synched to cc:Mail to downstream post offices	Allows directory synchronized entries added to the cc:Mail directory from Microsoft Exchange Server to be propagated to cc:Mail post offices indirectly connected by ADE.
Preserve forwarding history on messages sent from cc:Mail to Microsoft Exchange	Retains the message forwarding history as an attached file (Forward.txt) for messages sent from cc:Mail to Microsoft Exchange Server.

General Properties

Use the **General** property page to establish message size limits for inbound and outbound messages the connector will accept.

Getting to the General property page

1. In the Administrator window, choose **Connections**.
2. Double-click **Connector for cc:Mail**.
3. Select the **General** tab.



Specifying Message Size Limits

You can specify a size limit for inbound and outbound messages passed through the connector. Setting a maximum message size can reduce the amount of mail traffic across your network.

Note If a message body is larger than 20 kilobytes (KB), it will be converted to a text attachment in Lotus cc:Mail.

1. Select the **General** tab.
2. Under **Message size**, specify a limit.

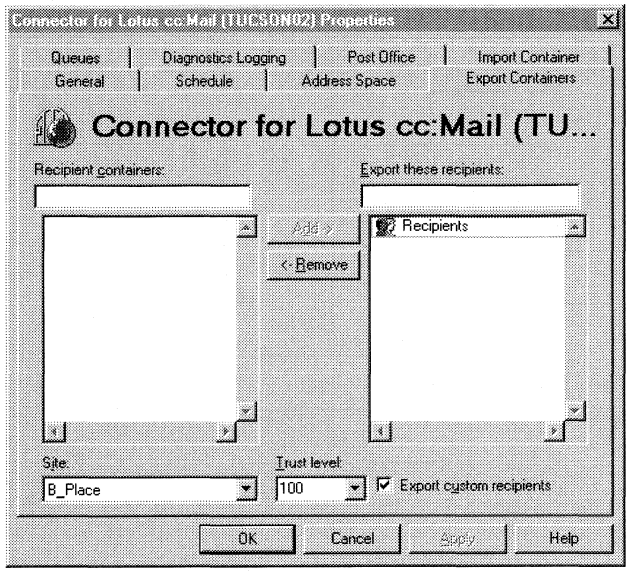
Option	Description
No limit	Messages of all sizes transferred. This is the default.
Maximum (K)	The maximum message size (1 to 2,097,151 KB) that can be transferred.

Export Containers

You use export containers to specify the Microsoft Exchange Server recipients that you want exported to the cc:Mail post office directory. Directory synchronization exports mailboxes, public folders, distribution lists, and custom recipients to the cc:Mail directory. The address names exported are the names generated by the cc:Mail e-mail address generator.

Getting to the Export Containers property page

1. In the Administrator window, choose **Connections**.
2. Double-click **Connector for cc:Mail**.
3. Select the Export Containers tab.



Selecting Export Containers

Use the **Export Containers** property page to specify containers for exporting directory information. You can also assign a trust level so that only recipients with a trust level equal to or less than the specified value are exported. By default, Microsoft Exchange Server does not export any recipient containers.

1. Select the **Export Containers** tab.
2. Under **Site**, select a site to view available containers in that site.
3. Under **Recipient Containers**, select a recipient container, and choose **Add**.
4. In the **Trust level** box, type or select a trust level.
5. Clear the **Export custom recipients** check box if you do not want to synchronize Microsoft Exchange Server custom recipients with the cc:Mail post office.

Option	Description
Trust	The trust level set for the connection. Only recipients with a trust level equal to or lower than the trust level specified for the export container are exported during directory synchronization. Set the recipient's trust level in the recipient's **Advanced** property page. The default is 100.
Export custom recipients	When selected, the custom recipients in the export container will be exported to cc:Mail. This option is selected by default.

Removing Export Containers

You can remove an export container used by the Microsoft Exchange Server to stop the export of recipients in that container.

1. Select the **Export Containers** tab.
2. Under **Export these recipients**, select the container you want to remove.
3. Choose **Remove**.

Import Container

You use an import container to store imported addresses from the cc:Mail post office on a Microsoft Exchange Server. Imported addresses from cc:Mail to Microsoft Exchange Server include:

- User names
- Bulletin board names
- Mailing lists

Imported addresses are represented as custom recipients in the Microsoft Exchange Server directory. Addresses from cc:Mail that contain text in the cc:Mail Administrator program comments field display the same text in the notes attribute for the custom recipient. When text in either the notes field or the field are edited, the updates are incorporated after the next directory synchronization cycle.

Note Lotus cc:Mail proxy names such as "user at ex1" and "user at ex2" are considered unique to Microsoft Exchange Server, but not to cc:Mail. Modify user names using the **E-mail Addresses** property page for custom recipients in the Microsoft Exchange Server Administrator program. For example, rename "user at ex1" to "user1 at ex1."

You should not manually create remote post office entries in the cc:Mail directory if you plan to run directory synchronization. The Connector for cc:Mail directory synchronization process automatically creates remote post office entries, including indirect Microsoft Exchange Server sites, in the cc:Mail directory. The connector creates a comment for each post office entry created that must remain for future directory synchronization processes to function correctly. If these comments are removed, directory synchronization fails. The format is MSExchangeCCMC *servername,* where *servername* is the name of the computer where the connector is installed. Do not delete or modify these comments.

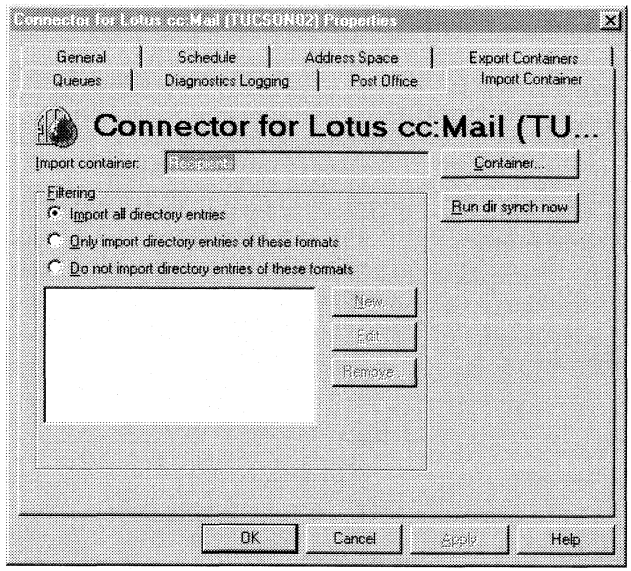
If the Microsoft Exchange Server computer hosting the Connector for cc:Mail and performing directory synchronization is removed and relocated on another server, you must delete post office and user references created automatically by the original connector in the cc:Mail directory.

When directory synchronization creates entries in the cc:Mail directory, it uses the foreign address name (FAN) field. Do not modify or delete this field. If entries to the cc:Mail directory are created manually for Microsoft Exchange Server recipients, the FAN fields for these entries must be completed manually. The field must include the CCMAIL address of the Microsoft Exchange Server recipient. For example, the Microsoft Exchange Server recipient Grover Smith will, by default, have the CCMAIL e-mail address Smith, Grover.

Distribution lists that contain a large number of cc:Mail recipients should be created on the cc:Mail post office and imported to Microsoft Exchange Server. Distribution lists created on Microsoft Exchange Server that include cc:Mail recipients are expanded in the **To** box before import to cc:Mail. The cc:Mail client does not accept a message header larger than 4000 bytes. A large number of cc:Mail recipients in the **To** box results in a non-delivery report (NDR).

Getting to the Import Container property page

1. In the Administrator window, choose **Connections**.
2. Double-click **Connector for cc:Mail**.
3. Select the **Import Container** tab.



Selecting an Import Container

Use the **Import Container** property page to specify which recipient container receives imported cc:Mail directory entries.

1. Select the **Import Container** tab.
2. Choose **Container**.
3. Select the container to place imported recipients in.

Configuring the Import Container Filter

Use the **Import Container** property page to set options for importing cc:Mail addresses. When you filter an import container, you can specify individual cc:Mail addresses you want imported to Microsoft Exchange Server.

1. Select the **Import Container** tab.
2. Under **Filtering**, select an option.

Option	Description
Import all directory entries	Imports all directory entries from the cc:Mail post office to Microsoft Exchange Server.
Only import directory entries of these formats	Imports cc:Mail addresses that correspond to the specified formats. For example, to accept addresses from the cc:Mail post office PO1 exclusively using the wildcard character asterisk, type *** at PO1**.
Do not import directory entries of these formats	Excludes cc:Mail addresses that correspond to a specified format. For example, to exclude addresses from the cc:Mail post office PO1 exclusively using the wildcard character asterisk, type *** at PO1**.
New	Specifies a new address format to include or exclude during directory synchronization.
Edit	Modifies an existing address format to include or exclude during directory synchronization.
Remove	Deletes an address format.

Running Directory Synchronization

Use the **Import Containers** property page to launch a directory synchronization cycle manually. Launching directory synchronization manually is done when an update between directories is required immediately.

To specify a regular interval for running directory synchronization, see "Directory Synchronization Schedule" later in this chapter.

1. Select the **Import Container** tab.
2. Choose **Run dir synch now** to start directory synchronization immediately.

Setting Alias and Display Name Rules for Directory Import

You can configure rules for creating the cc:Mail alias and display name during directory synchronization by editing the registry for the Windows NT Server hosting your Microsoft Exchange Server. By default, the connector creates a user alias as a combination of the first name and first letter of last name (%F%1L). For example, during directory synchronization import, the cc:Mail user Grover Smith would be given the alias *grovers*. Similarly, the connector creates a display name from the combination *first name last name* (%F %L), or in this example, *Grover Smith*.

You can edit the registry for the Windows NT Server to create a variety of combinations of alias and display names for directory synchronization import. The following is a table of rules you can specify.

Rule	Name component
%F	First name
%I	Initials
%L	Last name
%#(rule)	Specifies the number of characters for the name. For example, the format rule *%2L* for the last name Smith would generate Sm.

Configuring the Directory Import Alias Rule

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeCCMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and choose **New String Value**. If you are using Regedt32.exe, choose **Edit**, and choose **Add Value**.
4. If you are using Regedit.exe, type **Dir Synch alias name rule**; under **Value data**, type the rule combination. If you are using Regedt32.exe, type **Dir Synch alias name rule**; under **Data Type**, choose **REG_SZ**.
5. If you are using Regedt32.exe, under **Data**, type the rule combination.

Configuring the Directory Import Display Name Rule

1. Open Regedit.exe or Regedt32.exe.
2. Open the following registry keys:

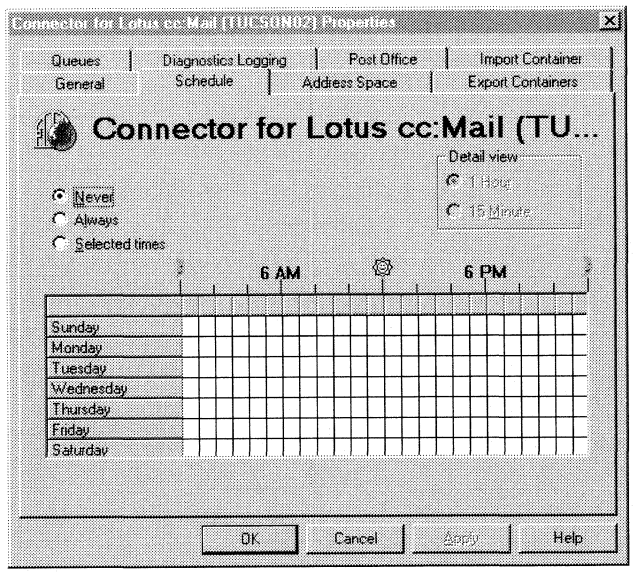
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeCCMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and choose **New String Value**. If you are using Regedt32.exe, choose **Edit**, and choose **Add Value**.
4. If you are using Regedit.exe, type **Dir Synch display name rule**; under **Value data**, type the rule combination. If you are using Regedt32.exe, type **Dir Synch display name rule**; under **Data Type**, choose **REG_SZ**.
5. If you are using Regedt32.exe, under **Data**, type the rule combination.

Directory Synchronization Schedule

You can schedule the time when Microsoft Exchange Server sends address list updates to and receives address list updates from the cc:Mail post office.

Getting to the Dirsync Schedule property page

1. In the Administrator window, choose **Connections**.
2. Double-click **Connector for cc:Mail**.
3. Select the **Dirsync Schedule** tab.



Setting the Directory Exchange Server Schedule

Use the **Dirsync Schedule** property page to specify when directory synchronization is performed. You can also specify to never run directory synchronization.

1. Select the **Dirsync Schedule** tab.
2. Select Never, Always, or Selected times.
3. Under **Detail view**, select a view for the schedule grid.

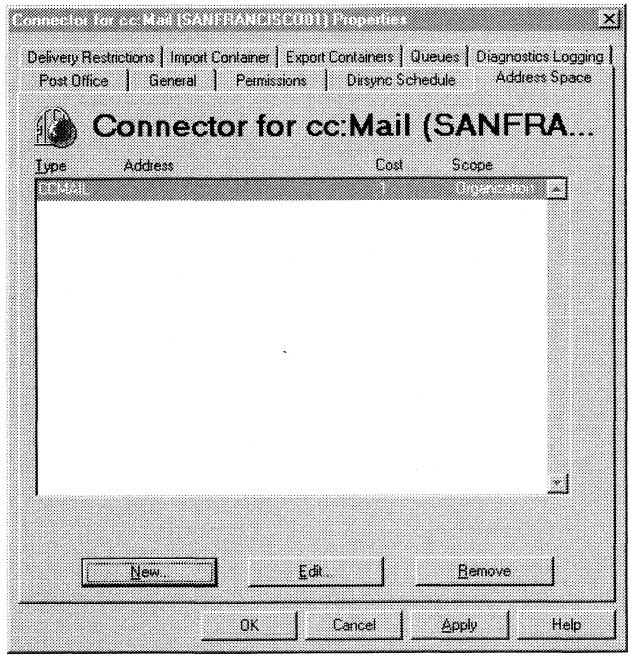
Option	Description
Never	Disables directory synchronization.
Always	Runs directory synchronization every 15 minutes.
Selected times	Runs directory synchronization at specific times during the week.
1 Hour	Shows the schedule in 1-hour increments.
15 Minute	Shows the schedule in 15-minute increments.

Address Space

Use the **Address Space** property page to configure message routing for the connector. You can configure the address space to specify which messages bound for cc:Mail this connector will route.

Getting to the Address Space property page

1. In the Administrator window, choose **Connections**.
2. Double-click **Connector for cc:Mail**.
3. Select the **Address Space** tab.



Configuring the Address Space

Use the **Address Space** property page to enter information about the addresses you want the connector to process. If you enter the CCMAIL address space entry *** at SERVER1**, it matches all recipient addresses for the post office SERVER1. You can type a wildcard (* or %) when necessary to specify a group of addresses. For example, entering **SITE??** specifies all entries that contain SITE followed by two alphanumeric characters, such as SITE01 and SITE11.

1. Select the **Address Space** tab.
2. Choose **New**.
3. Choose **Other**.
4. In the **Type** box, type **CCMAIL**.
5. In the **Address** box, type the address.

Option	Description
Type	The address type used to identify the cc:Mail post office. You must type the address type CCMAIL.
Address	Type enough address information for routing. To route all traffic for a message type through the connector, leave the **Address** box blank.
Cost	The routing cost (0 to 100) for messages sent through this connector. The routing cost determines the preference between multiple routes. Lower cost routes take precedence over higher cost routes. The default routing cost is 1. Load balancing across multiple connectors is achieved by assigning equal cost values for all connectors.

Removing an Address Space

You can remove an address space that is no longer necessary.

1. In the Administrator window, choose the Configuration container.
2. Double-click the connector to be modified.
3. Select the **Address Space** tab.
4. Select the address space to be removed.
5. Choose **Remove**.

Modifying the Address Generator Format

When the connector is initially installed in a site, cc:Mail e-mail address generator creates an address of type CCMAIL (*username* at *siteproxy*) for every recipient, public folder, distribution list, and custom recipient in the site. During Setup, the site proxy name is derived from the Microsoft Exchange Server site name. The user name format can be configured.

Note A site address name cannot be the same as an existing cc:Mail post office name.

Format specifier	Name component
%g	First name
%i	Initials
%s	Last name
%d	Display name
%m	Alias
%#(specifier)	Specifies the number of characters for the user name. For example, the format specifier *%3s* for the last name Johnson generates Joh.

For example, the recipient Grover Smith in the site Ferguson will by default have the address format *%s, %g at siteproxy*, generating Smith, Grover at Ferguson. However, site names can be modified for multiple formats. The following table shows possible addressing for the display name Grover L. Smith in the site Ferguson.

Example	Format
%d at Ferguson	Grover L. Smith at Ferguson
%s.%g at Ferguson	Smith.Grover at Ferguson
%s, %g %i at Ferguson	Smith, Grover L. at Ferguson
%s, %2g at Ferguson	Smith, Gr at Ferguson

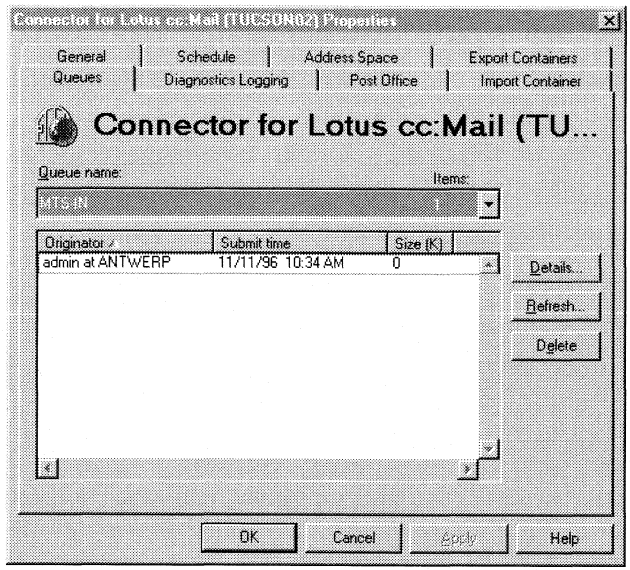
1. In the Administrator window, choose the Configuration container.
2. Select an entry.
3. Choose **Edit**.
4. Make the necessary changes.

Connector for cc:Mail Queues

The information store has queues for monitoring outbound and inbound messages through the connector. The MTS-OUT queue displays outbound messages destined for the connector. The MTS-IN queue displays converted messages traveling inbound from the connector. You can view the queues for all messages pending transfer. You can also return messages to the originator by deleting them from the queue. Use the **Queues** property page to determine the number of messages in a queue, to view a message in a queue in detail, and to delete a pending message.

Getting to the Queues property page

1. In the Administrator window, choose **Connections**.
2. Double-click **Connector for cc:Mail**.
3. Select the **Queues** tab.



Viewing Message Queue Details

Use the **Queues** property page to view the details of a queued message. The originator information is taken from the message heading showing the sending or receiving server.

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

Refreshing the Queues Property Page

The **Queues** property page is a snapshot of the queues taken when you select this page. 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

Messages can be deleted from the connector queue. Deleted messages are returned to the originator as non-deliverable.

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

Diagnostics Logging

You can control how logging information for the connector is written to the Windows NT Event Log. You can specify the types of events that are logged for the connector and the level of logging information for each event. Viewing the event log for the Connector for cc:Mail is useful when troubleshooting message transfer through the connector. For additional information about diagnostics logging, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

Setting up Diagnostics Logging

You can enable logging for the Connector for cc:Mail Service to be written to the application event log. You can assign a level of logging for the categories related to the MSExchangeCCMC service. The level determines which events generated by the service are logged. Normally, you log only critical events. However, when a problem occurs, detailed events can disclose a path to the source of the problem. Outbound and inbound events pertain to messages destined to cc:Mail and messages destined to Microsoft Exchange Server respectively.

1. Select the **Diagnostics Logging** tab.
2. Under **Category**, select a service category.
3. Under **Logging level**, select a level.

Option	Description
None	Only critical events and error events are logged. This is the default.
Minimum or Medium	This setting is appropriate when the problem has been narrowed to a service or group of categories.
Maximum	A complete trail of the operation of the service. This level is appropriate when the problem has been traced to a particular category.

Delivery Restrictions Properties

Use the **Delivery Restrictions** property page to accept or reject messages from any sender listed in the Microsoft Exchange Server directory. For example, if a message is addressed to cc:Mail users, it is returned to the sender if the sender's address is in the **Reject messages from** box or does not appear in the **Accept messages from** box. Delivery restrictions do not affect incoming messages. The default is to accept messages from all senders and reject messages from none.

Getting to the Delivery Restrictions property page

1. In the Administrator window, choose **Connections**.
2. Double-click **Connector for cc:Mail**.
3. Select the **Delivery Restrictions** tab.

For more information about using delivery restrictions, see *Microsoft Exchange Server Getting Started.*

Connecting to a Post Office on a Novell NetWare Server

You can configure the Connector for cc:Mail to connect to a post office residing on a NetWare server (version 3.1*x* or 4.*x*). The service account accessing the directory where the cc:Mail post office data (\CCDATA) resides must have full access, and the account must be configured so that it never expires. Sufficient access can be accomplished by either:

- Installing and configuring Gateway Services for NetWare on the Windows NT Server where the Connector for cc:Mail resides. The directory that contains the cc:Mail post office data files can be shared using the gateway service. Share permissions are determined by the Microsoft Exchange Server service account.

  - or -

- Creating an account on the NetWare server where the cc:Mail post office resides that is identical to the Microsoft Exchange Server service account. The NetWare account must have the same user account name and password information as the Windows NT Server account used as the Microsoft Exchange Server service account. NetWare rights for the account must be set for Read, File Scan, Modify, and Create to the directory.

Use the following procedure to test the Microsoft Exchange Server service account for verification of sufficient rights when installing the connector.

1. On Microsoft Windows NT Server, create the account that will be used as the Microsoft Exchange Server service account. This account should have the **Password Never Expires** box selected.
2. Verify that Gateway Services for NetWare is properly installed and configured.
3. Using the appropriate NetWare administration tool, create an account on the Novell server to access the cc:Mail post office.
4. On Microsoft Windows NT Server, temporarily give the Microsoft Exchange Server service account local logon rights using the Windows NT User Manager for Domains program. Log on as the Microsoft Exchange Server service account. The first time you log on after Gateway Services for NetWare is installed, Windows NT Server prompts you for your default server (for NetWare 3.1*x* or 4.*x* using bindery emulation), or the correct NDS Tree and Context for NetWare 4.*x*. Select the default server or NDS Tree/Context for the Microsoft Exchange Server service account.

5. While logged on using the Microsoft Exchange Server service account, run the cc:Mail Administrator program to verify the service account has sufficient rights. You should have access to the cc:Mail post office for creating local users and post office entries. If you can access the post office but cannot create new directory entries, the Microsoft Exchange Server service account on the NetWare server does not have Create rights to the cc:Mail post office directory.
6. Log off the Microsoft Exchange Server service account. You can remove local logon rights from the Microsoft Exchange Server service account using the User Manager for Domains program.

For information on configuring Gateway Services for NetWare, see your Windows NT Server documentation.

Test the Connection

After you configure the connector, you should test the connection before allowing general message transfer. To test the connection, send a message from a Microsoft Exchange Server recipient to a cc:Mail recipient using an e-mail client. To ensure a complete connection from both sides of the connector, send a message from a cc:Mail client to a Microsoft Exchange Server recipient.

If address lists have not been exchanged between systems, enter the post office and mailbox names for any recipients you wish to send a test message to. For information on synchronizing directory information, see "Running Directory Synchronization" earlier in this chapter.

Testing from the Microsoft Exchange Server

You can test the connector by sending test messages from a Microsoft Exchange Server recipient to a cc:Mail recipient using an e-mail client. This helps to determine if the outbound side of the connector is functioning correctly. After you have tested the connector from a Microsoft Exchange server, you should also send a test message from a cc:Mail client to a Microsoft Exchange Server recipient. For information on testing the connector from a cc:Mail client, see "Testing from a cc:Mail Client" later in this chapter.

Before you send a test message from a Microsoft Exchange server to a cc:Mail recipient, create a custom recipient address for the mailbox you are sending the test message to. Once the address is created, the recipient appears in your personal address list. You must know the post office name and mailbox name for the recipient. Use the cc:Mail Administrator program to find this information.

Before testing the connection, check to see that the cc:Mail service has been started. Use the Services icon in Control Panel to start the Connector cc:Mail Service.

Note Messages sent from a Microsoft Exchange Server computer to a cc:Mail recipient will not be delivered if the word "at" appears in the cc:Mail user name. For example, a message addressed to the cc:Mail user name *Grover Smith at Legal* located on post office *Postoffice1* (*Grover Smith at Legal at Postoffice1*) results in a non-delivery report.

Testing from a cc:Mail Client

You can test the connector by sending test messages from a cc:Mail client to a Microsoft Exchange Server recipient. This helps to determine if the inbound side of the connection is functioning correctly. Once you have tested the connector from a cc:Mail client, you should also send a test message from a Microsoft Exchange Server recipient to a cc:Mail recipient using an e-mail client. For information on testing the connector from Microsoft Exchange Server, see "Testing from the Microsoft Exchange Server" earlier in this chapter.

Before you send a test message from a cc:Mail client to a Microsoft Exchange Server recipient, you create a recipient address for the mailbox you are sending the test message to. Once the address is created, the recipient appears in your address list. You must know the cc:Mail address for the Microsoft Exchange Server recipient. This information can be found in the Microsoft Exchange Server Administrator program.

Note Before testing the connection, if directory synchronization has not yet occurred or if directory synchronization will never occur, you must add the Microsoft Exchange Server site as a cc:Mail post office using the cc:Mail Administrator program. If you plan to use directory synchronization after a post office has been created manually, you must delete the post office entry before running directory synchronization. You must also add a test user mailbox that corresponds to a Microsoft Exchange Server mailbox. For information on configuring cc:Mail, see your cc:Mail documentation.

---

1. In the cc:Mail client for Windows, compose a new message.
2. Choose **Address**.
3. Under **Name**, select the mailbox for the Microsoft Exchange Server recipient.
4. Choose **Done**.
5. Send the message.

How the Connector Manages Attached Objects

The connector does not support all the linking features in some e-mail client software. A Microsoft Exchange Server system allows:

- Embedding objects into the message body
- Linking objects to the message body
- Inserting links to files
- Inserting shortcuts to Microsoft Exchange folders
- Inserting shortcuts to Internet sites

These features cannot be fully implemented when sending a message from some e-mail clients to a cc:Mail recipient.

Sending Attachments

The Connector for cc:Mail does not fully support object linking between dissimilar applications. When an object, such as an image created in a graphics application, is *linked* to another document, such as a word processor document, the document contains only a reference to the object. When an object is *embedded* in a document, the document contains a copy of the object.

The following table describes how objects are sent.

Object	Connector management	Object viewed by client
Embedded object in a Microsoft Exchange message body.	Embedded object is forwarded to the cc:Mail post office.	The embedded object appears in the cc:Mail attachment entitled "OLE Object." The object can be viewed using the viewers available from the cc:Mail 6.0 client or saved and opened in the application that created it.
Linked object in a Microsoft Exchange message body.	Linked object is not forwarded to the cc:Mail post office.	The object appears in a cc:Mail client message as an attachment entitled "OLE Object." The object cannot be viewed.

Sending Shortcuts and Links

The Connector for cc:Mail does not fully support links to files, shortcuts to Uniform Resource Locators (URLs), and shortcuts to Microsoft Exchange public folders.

Shortcuts to URLs are created in a Web browser and copied to the Microsoft Exchange message body.

The following table describes how shortcuts and links are sent.

Object	Connector management	Object viewed by client
Links to files	Forwarded to the cc:Mail post office.	The network path to the linked file is inserted into the message body. The file cannot be viewed from the cc:Mail client.
Shortcuts to URLs	Forwarded to the cc:Mail post office as a URL in the message body.	The URL site address is inserted into the message. The URL can be copied from the message and viewed from a Web browser.
Shortcuts to Microsoft Exchange public folders	Forwarded to the cc:Mail post office as an attachment.	The folder shortcut is inserted into an attached file. The attachment name is derived from the folder name. The shortcut cannot be launched from a cc:Mail client.

Moving the Connector for cc:Mail

You can relocate the connector responsible for directory synchronization from one Microsoft Exchange Server site to another. For example, you can centralize cc:Mail message traffic in a single Microsoft Exchange Server site for handling cc:Mail message throughput. This can require relocating the existing connector to a new Microsoft Exchange Server.

Relocating an existing connector from one Microsoft Exchange Server computer to another does not require restarting the Microsoft Exchange Server computer running the connector. However, the Microsoft Exchange Connector Service must be stopped during the time it takes to move the connector.

Relocating the Connector for cc:Mail

You should schedule relocating a connector at a time that coincides with a time the connector is used least.

Relocating a connector from one Microsoft Exchange Server computer to another requires waiting for messages in the MTS-OUT queue to be delivered. For information on monitoring the MTS-OUT queue, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

Relocating a Connector to Another Site

When you relocate a connector to another site, you must designate an import container for the new site and remove the custom recipient objects (cc:Mail users) from the recipients container used for import in the former site. Otherwise, directory synchronization does not function properly.

1. Install the Connector for cc:Mail on the Microsoft Exchange Server where the connector is being relocated.
2. Start the Connector for cc:Mail Service for the new connector.
3. In the **Dirsync Schedule** property page for the connector being removed, select **Never**.
4. In the **Import Container** property page for the new connector, select a container for directory import.
5. Stop the Microsoft Exchange Connector Service on the Microsoft Exchange Server computer where the connector is being removed.
6. Remove the Connector for cc:Mail object from the **Connections** container for the site where the connector is being removed.
7. Delete the previously used import container, or remove all custom recipients in the container.
8. Schedule a directory synchronization cycle for the new connector, or initiate a cycle manually by choosing **Run dir sync now** in the **Import Container** property page.

Relocating a Connector Within a Site

When you relocate a connector within a site, you must designate a new import container for the site and remove the custom recipient objects (cc:Mail users) from the recipients container formerly used for import. Otherwise, directory synchronization does not function properly.

1. Install the Connector for cc:Mail on the Microsoft Exchange Server computer where the connector is being relocated.
2. Start the Connector for cc:Mail Service for the new connector.
3. In the **Dirsync Schedule** property page for the connector being removed, select **Never**.
4. In the **Import Container** property page for the new connector, select the same recipients container used by the previous connector for directory import.
5. Stop the Microsoft Exchange Connector Service on the Microsoft Exchange Server computer where the connector is being removed.
6. Remove the Connector for cc:Mail object from the **Connections** container for the site where the connector is being removed.

7. Delete the previously used import container, or remove all custom recipients in the container.
8. Schedule a directory synchronization cycle for the new connector, or initiate a cycle manually by choosing **Run dir sync now** in the **Import Container** property page.

Relocating the Import Container Within a Site

When you relocate a directory synchronization import container within a site, you must remove the custom recipient objects (cc:Mail users) from the recipients container formerly used for import. Otherwise, directory synchronization does not function properly.

1. In the **Import Container** property page, choose **Container**.
2. Select a new recipients container to import address information.
3. Delete the previously used import container, or remove all custom recipients in the container.
4. Schedule a directory synchronization cycle for the new connector, or initiate a cycle manually by choosing **Run dir sync now** in the **Import Container** property page.

Public Folders and cc:Mail Bulletin Boards

Microsoft Exchange Server and cc:Mail can be configured to forward mail sent to either a public folder or a bulletin board. Because of limitations in the propagation of bulletin board messages, forwarding can be configured for one direction only (cc:Mail to Microsoft Exchange Server or Microsoft Exchange Server to cc:Mail). Configuration of cross-posting between a cc:Mail bulletin board and a Microsoft Exchange Server public folder may result in message looping.

Modifying E-mail Addresses

Directory synchronization creates custom recipient entries for cc:Mail bulletin boards in the Microsoft Exchange Server directory. Messages sent to these custom recipients will be delivered only to the bulletin boards on the connected post office. You must modify the CCMAIL target address on the bulletin board custom recipients to propagate bulletin board messages to downstream post offices. For example, a bulletin board named "Social" located on the cc:Mail post office "PO5" would have the address "#Social." Modify this to "#Social at PO5." You can determine the home post office for a bulletin board from the cc:Mail Administrator program.

1. Double-click the bulletin board custom recipient.
2. Select the **General** tab, and then choose **E-mail**.
3. Select Modify existing e-mail address.
4. Type e-mail address information.
5. Run directory synchronization.

Propagating Messages Between cc:Mail Bulletin Boards and Public Folders

The Lotus cc:Mail Router program (an agent that propagates bulletin board messages on a cc:Mail system) must be active between the bulletin board home post office and the recipient post office to enable the propagation of cc:Mail bulletin board messages. Messages sent through the Connector for cc:Mail to Microsoft Exchange Server are extracted from the connected cc:Mail post office using the cc:Mail Import/Export programs. These messages are not delivered by the cc:Mail Router. As a result, bulletin boards propagated into Microsoft Exchange Server public folders cannot be hosted on the connected cc:Mail post office. Furthermore, bulletin boards hosted on the connected cc:Mail post office must be moved and homed to another post office. Create a Microsoft Exchange Server public folder that bulletin board messages will be propagated to. The public folder must have the same name as the cc:Mail bulletin board.

1. In the Microsoft Exchange Server Administrator program, choose **Folders**, choose **Public Folders**, and then double-click the public folder used for propagating bulletin board messages.
2. Select the **Advanced** tab, and clear the **Hide from address book** check box.
3. Configure the connector and run directory synchronization. Verify that the cc:Mail SiteProxy post office has propagated through ADE to the cc:Mail post office hosting the bulletin board.
4. Modify the Microsoft Exchange Server custom recipient for the cc:Mail bulletin board.
5. From the cc:Mail Administrator program Main menu, choose **Manage Bulletin Boards**. Choose the name of the bulletin board to be propagated, and press ENTER.
6. From the **Bulletin Board menu**, choose **Add names to propagation list**. If the target public folder is the same as the bulletin board, select the Microsoft Exchange SiteProxy post office name; otherwise, select the name of the Microsoft Exchange Server public folder.

Other methods for synchronizing messages posted to bulletin boards into public folders include:

- Use cc:Mail's client-based rules to automatically add the address of a public folder to messages the user sends to a bulletin board. These rules must be created on a per-bulletin board basis and must be created directly by the end user or by an administrator who then distributes the .Rul files to end users.
- Create mailing lists in the cc:Mail directory that include a bulletin board/public folder pair. Instruct users to send to these mailing lists instead of posting directly to the bulletin board.

Propagating Public Folder Messages into cc:Mail Bulletin Boards

Messages are propagated from Microsoft Exchange Server public folders using a Folder Assistant rule. You create a rule to forward all messages posted or sent to the public folder to the cc:Mail bulletin board.

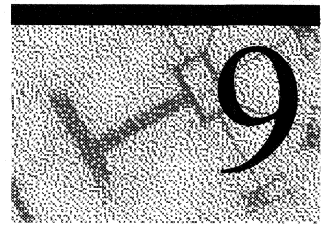
1. Configure the connector and run directory synchronization. Verify that the cc:Mail SiteProxy post office has propagated through ADE to the cc:Mail post office hosting the bulletin board.
2. Modify the Microsoft Exchange Server custom recipient for the cc:Mail bulletin board.
3. In the e-mail client program, right-click the public folder to be propagated, and choose **Properties**.
4. Select the **Administration** tab.

5. Enable Folder Assistant, Add Rule, and Forward. Double-click **To**, and select the cc:Mail bulletin board for receiving the propagated messages. In the **Method** box, select **Leave message intact**.
6. When you receive a message asking if you want this rule to fire for all incoming messages, choose **Yes.**

Another method of synchronizing messages posted or sent to public folders is to create a distribution list for each public folder and include the public folder and the corresponding bulletin board as members. Instruct users to send to the distribution list instead of sending or posting directly to the public folder.

CHAPTER 9

Microsoft Mail for AppleTalk Networks



You can use the Microsoft Mail Connector to connect an MS Mail (AppleTalk) server or a Quarterdeck Mail server to Microsoft Exchange Server. Microsoft Exchange Server uses the Microsoft Mail Connector to replace the function of the former Mail Connection Gateway. You use the Microsoft Exchange Server Administrator program to configure and administer the Microsoft Mail Connector.

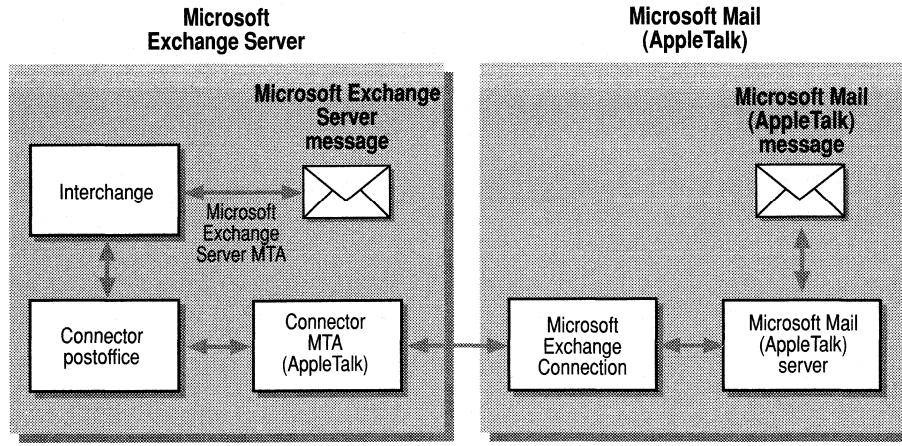
Microsoft Exchange Server uses components of the Microsoft Mail Connector and a gateway component for the MS Mail (AppleTalk) server to communicate with MS Mail (AppleTalk).

Microsoft Mail Connector interchange A Windows NT Server service that routes and transfers messages between Microsoft Exchange Server and the Microsoft Mail Connector postoffice.

Microsoft Mail Connector postoffice A temporary information store for messages in transit and a connection point for the Microsoft Exchange Connection.

Microsoft Mail Connector (AppleTalk) message transfer agent (MTA)
A Windows NT Server service that works with the Microsoft Exchange Connection to transfer messages using the MS Mail (AppleTalk) server.

Microsoft Exchange Connection A gateway for the MS Mail (AppleTalk) server provided with Microsoft Exchange Server. This gateway works with the Microsoft Mail Connector (AppleTalk) MTA to transfer messages between the Microsoft Mail Connector postoffice and MS Mail (AppleTalk).



For more information on the Microsoft Mail Connector and its components, see Chapter 10, "Microsoft Mail for PC Networks."

Microsoft Mail Connector Requirements

For each Microsoft Exchange Server computer, there can be only one instance of the Microsoft Mail Connector in operation. However, you can have every Microsoft Exchange Server computer in your site operating a connector. To use the Microsoft Mail Connector with MS Mail (AppleTalk), your Windows NT Server configuration must include:

- Windows NT Services for Macintosh installed on your Microsoft Exchange Server computer.
- A Windows NT file system (NTFS) partition, which is required to support Services for Macintosh. The Microsoft Exchange Server must be installed on the NTFS partition.

For information on NTFS, partitions, installing or converting file systems, and installing Services for Macintosh and related network software, see your Windows NT Server documentation.

Microsoft Exchange Connection Requirements

The Microsoft Exchange Connection software is installed on the MS Mail (AppleTalk) server. The MS Mail (AppleTalk) server requirements include the following:

- A Macintosh computer with an extra 2 megabytes (MB) of RAM in addition to the basic RAM requirements for an MS Mail (AppleTalk) server.
- Enough hard disk space available to store incoming and outgoing messages until transfer is made to the Microsoft Mail Connector postoffice.
- Microsoft Mail for AppleTalk Networks version 3.1*c* or later.
- System 7.1 or later.

For more information on MS Mail (AppleTalk) requirements and setup, see your Microsoft Mail for AppleTalk Networks documentation.

Microsoft Mail Connector Setup

Setting up the Microsoft Mail Connector to communicate with MS Mail (AppleTalk) includes the following:

- Making the Microsoft Mail Connector postoffice Macintosh accessible.
- Configuring the Microsoft Mail Connector components.

When this process is complete, you can install, configure, and start the Microsoft Exchange Connection gateway software on an MS Mail (AppleTalk) server.

For Microsoft Mail Connector installation information, see *Microsoft Exchange Server Getting Started.*

Quick Start

To set up the minimum configuration requirements for a Microsoft Mail Connector, use the following list of procedures in the order in which they appear.

Task	Description
Create a Macintosh-accessible volume.	A Macintosh-accessible volume must be created on the Microsoft Exchange Server computer for the MS Mail (AppleTalk) server to connect to the volume.
Configure the connector **Interchange** property page.	From the connector **Interchange** property page, you must assign an administrator's mailbox and configure the Microsoft Mail Connector (AppleTalk) MTA.
Connect to the Microsoft Mail Connector postoffice.	You must connect to the Connector postoffice from the Macintosh server to configure the Microsoft Exchange Connection software. The MS Mail (AppleTalk) administrator should configure the Chooser to connect to the volume that contains the Connector postoffice at startup.
Install and configure the Microsoft Exchange Connection.	▪ Specify the postoffice location. ▪ Set the gateway options. ▪ Set the gateway connection times. ▪ Install access connection software on additional mail servers for indirect access.
Start the Microsoft Mail Connector (AppleTalk) MTA service.	Start the Microsoft Mail Connector (AppleTalk) MTA service from the Control Panel.
Test the connection.	Send a mail message from a Microsoft Exchange Server recipient to an MS Mail (AppleTalk) recipient and back.

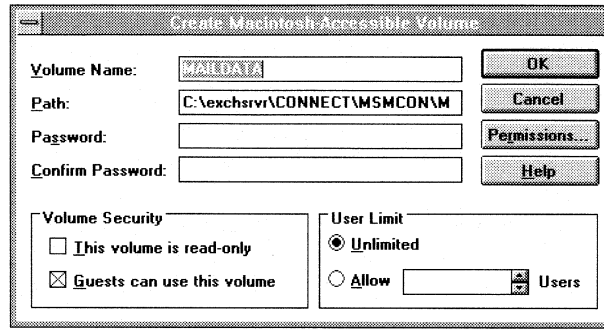
Macintosh-Accessible Volume

A Macintosh-accessible volume is a directory on the computer running Windows NT Server that is made available to Macintosh clients. The directory that contains the Microsoft Mail Connector postoffice must be created as a Macintosh-accessible volume. Once the volume has been created, MS Mail (AppleTalk) servers can view and exchange files with the connector. You can create a Macintosh-accessible volume from the **MacFile** menu in File Manager.

Creating a Macintosh-Accessible Volume

A Macintosh-accessible volume must be created on the Microsoft Exchange Server computer for the MS Mail (AppleTalk) server to connect to the volume. Before creating a Macintosh-accessible volume, verify that Windows NT Services for Macintosh is installed on the Microsoft Exchange Server computer.

1. From File Manager, select the Exchsrvr\Connect\Msmcon\Maildata directory.
2. From the **MacFile** menu, choose **Create Volume**.



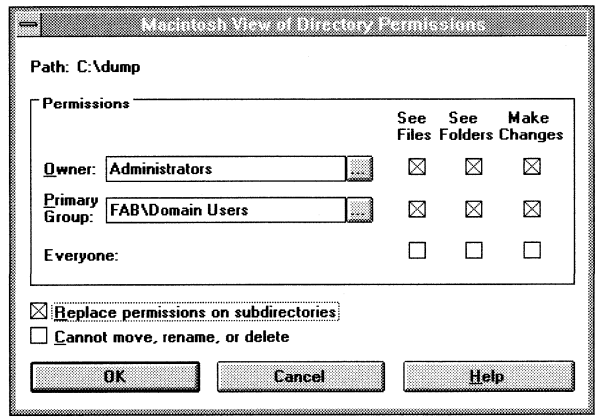
3. Type a volume name.
4. Type and confirm a password.
5. Verify that the **This volume is read-only** check box is cleared.
6. Clear the **Guests can use this volume** check box.
7. Select a user limit.

Option	Description
Volume Name	The name used when connecting to Microsoft Exchange Server from the MS Mail (AppleTalk) server. MAILDATA is the default.
Password	Used by the MS Mail (AppleTalk) server when connecting to this volume. If you want message transfer to start automatically when the Macintosh computer starts or restarts, do not enter a volume password.
Guests can use this volume	Clear the guest access to the Connector postoffice volume to preserve message security. This option is selected by default.
User Limit	Select **Allow**, and type or select a number to limit simultaneous connections to this volume. The default is **Unlimited**.

Setting Permissions for a Volume

Permissions for a volume are equivalent to Macintosh file sharing, which specifies which users can use a volume or folder. You can grant permissions for a Windows NT Server user account, group, or both to connect to the volume from the Chooser. Sufficient permissions must be set for the MS Mail (AppleTalk) administrator to access the Microsoft Mail Connector volume. After the administrator has sufficient permissions, the volume can be viewed from the MS Mail (AppleTalk) server and configured for mail transfer.

1. From File Manager, select the directory you have designated as a Macintosh-accessible volume.
2. From the **MacFile** menu, choose **Permissions**.



3. Select an owner and a primary group.
4. Select all permissions for the owner and primary group.
5. Clear all permissions for **Everyone**.
6. Select the **Replace permissions on subdirectories** check box.
7. Clear the **Cannot move, rename, or delete** check box.

Option	Description
See Files	Allows the owner, primary group, or all users to view and open files in this volume. This permission is selected by default.
See Folders	Allows the owner, primary group, or all users to view and open directories in this volume. This permission is selected by default.
Make Changes	Allows the owner, primary group, or all users to add or delete files and directories as well as save changes to files in this volume. This permission is selected by default.
Replace permissions on subdirectories	Select to copy the permissions you just set to all directories within this volume. This option is cleared by default.
Cannot move, rename, or delete	Select to prevent users from moving, renaming, or deleting the volume or subdirectories. This option is cleared by default.

Microsoft Mail Connector Interchange

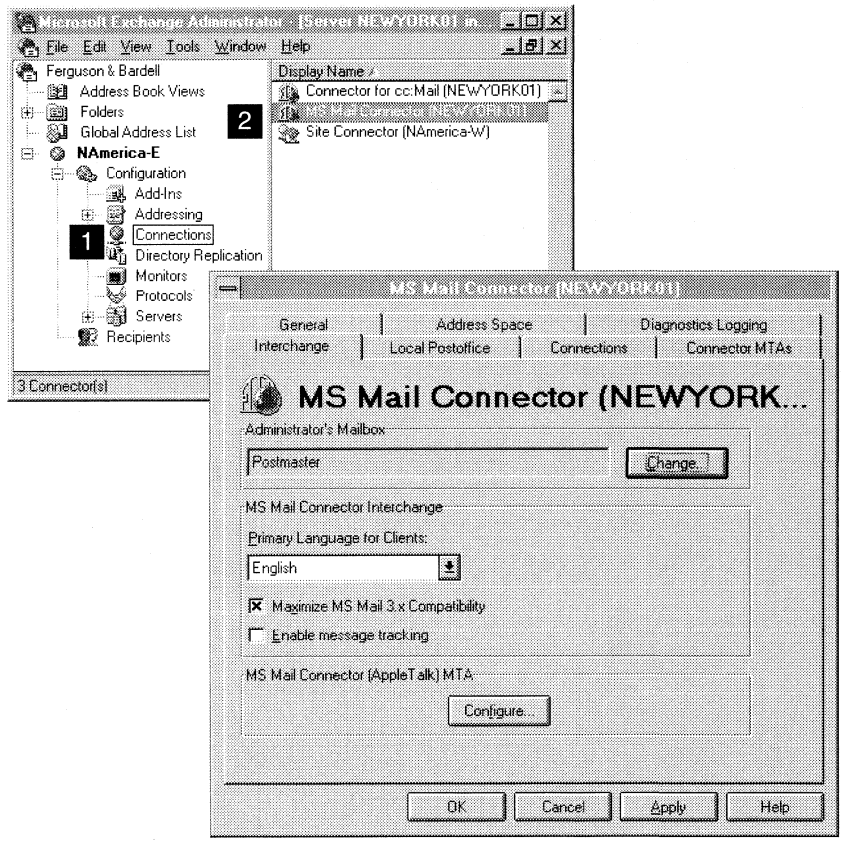
Use the **Interchange** property page to configure how the connector interchange translates information between Microsoft Exchange Server and the Connector postoffice. To configure the Microsoft Mail Connector interchange you must:

- Assign an administrator's mailbox for receiving delivery status messages.
- Set up the Microsoft Mail Connector (AppleTalk) MTA.

Note OLE compatibility settings in the **Maximize MS Mail 3.x Compatibility** check box affect only connections to MS Mail (PC).

Getting to the Interchange property page

1. In the Administrator window, choose the site container where the Microsoft Mail Connector is installed, and choose **Connections**.
2. Double-click the Microsoft Mail Connector.
3. Select the **Interchange** tab.



Assigning an Administrator's Mailbox

Use the **Interchange** property page to assign an administrator's mailbox to receive delivery status messages.

Tip You can create a mailbox called Postmaster to receive delivery messages.

---

1. Select the **Interchange** tab.
2. Choose **Change**.
3. Select a recipient for the administrator's mailbox.

Option	Description
Show Names from the	Select the global address list or a container.
Type Name Or Select from List	Type a name or select one from the list.
Properties	Displays the properties for the mailbox.
Find	Searches for a name based on a specific set of criteria.

Enabling Message Tracking

The Microsoft Exchange Server Administrator program has a tool used to track message movement that can be applied when troubleshooting message flow. You can follow the progress of a message as it passes from the Microsoft Exchange Server information store to the Connector postoffice. To use this tool, you must first enable message tracking in the **Interchange** property page.

1. Select the **Interchange** tab.
2. Select **Enable message tracking**.

For more information on message tracking, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

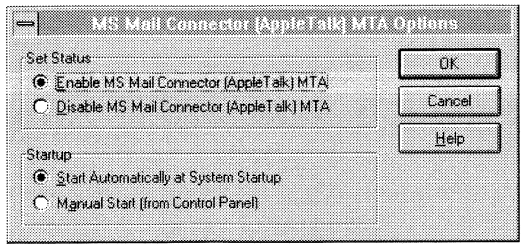
Setting Up the Microsoft Mail Connector (AppleTalk) MTA

The Microsoft Mail Connector (AppleTalk) MTA is responsible for moving messages between the MS Mail (PC) and Macintosh areas of the Microsoft Mail Connector postoffice. When you enable the Microsoft Mail Connector (AppleTalk) MTA, it is added to the list of available Windows NT Server services. Once the Microsoft Mail Connector (AppleTalk) MTA has been configured, you can start the service from either the Control Panel or Server Manager.

Note The **Connector MTAs** property page is used only when configuring MS Mail for PC Networks.

---

1. Select the **Interchange** tab.
2. In the **MS Mail Connector (AppleTalk) MTA** box, choose **Configure**.
3. Under **Set Status**, select **Enable MS Mail Connector (AppleTalk) MTA**.
4. Under **Startup**, select a method for starting the Microsoft Mail Connector (AppleTalk) MTA service.



Option	Description
Start Automatically at System Startup	Runs the Microsoft Mail Connector (AppleTalk) MTA with the Windows NT Server services at system startup. For message transfer, you need to restart the Microsoft Exchange Server computer.
Manual Start (from Control Panel)	Manually starts the Microsoft Mail Connector (AppleTalk) MTA from either the Windows NT Control Panel or Server Manager. For message transfer, you need to start the Microsoft Mail Connector (AppleTalk) MTA service.

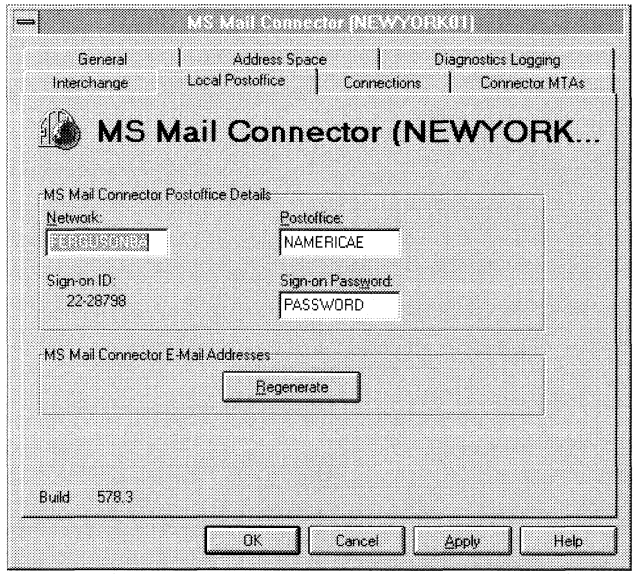
For more information on starting or stopping Microsoft Exchange Server services, see *Microsoft Exchange Server Getting Started.*

Local Postoffice Properties

Use the **Local Postoffice** property page to view or modify the network and postoffice name of the Microsoft Mail Connector. These names are used to identify the Microsoft Exchange Server externally for routing services between Microsoft Mail postoffices and Microsoft Exchange Server. The default names are determined during installation from the Microsoft Exchange Server organization and site names. In a typical configuration, you would not change these names.

Getting to the Local Postoffice property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Local Postoffice** tab.



Modifying Local Postoffice Name and Password

Use the **Local Postoffice** property page to change the network name and postoffice name for the Connector postoffice. You can also assign or reassign an existing password for the Connector postoffice. For example, you may want to group a set of postoffices by a single network name. You can change a Connector postoffice name in the **Local Postoffice** property page and then regenerate the change to represent the new Microsoft Mail address for the postoffice.

The Connector interchange and all instances of the Microsoft Mail Connector (AppleTalk) MTA read the network and postoffice name at startup. If you want the changes you have made to take effect immediately, stop and then restart the Connector interchange and Microsoft Mail Connector (AppleTalk) MTAs.

Warning Any change to network or postoffice names will cause regeneration of the Microsoft Mail address for the Connector postoffice. Changing the network or postoffice name after message transfer has started will cause messages that were in transit during the change to be returned. You must modify the external listing for the Connector postoffice for all Microsoft Mail postoffices connected directly or indirectly to the connector. You must also stop, reconfigure, and restart all Microsoft Mail gateways and occurrences of the External program.

---

1. Select the **Local Postoffice** tab.
2. In the **Network** box, type a network name.
3. In the **Postoffice** box, type a postoffice name.
4. In the **Sign-on Password** box, type a password.
5. Choose **Regenerate**.

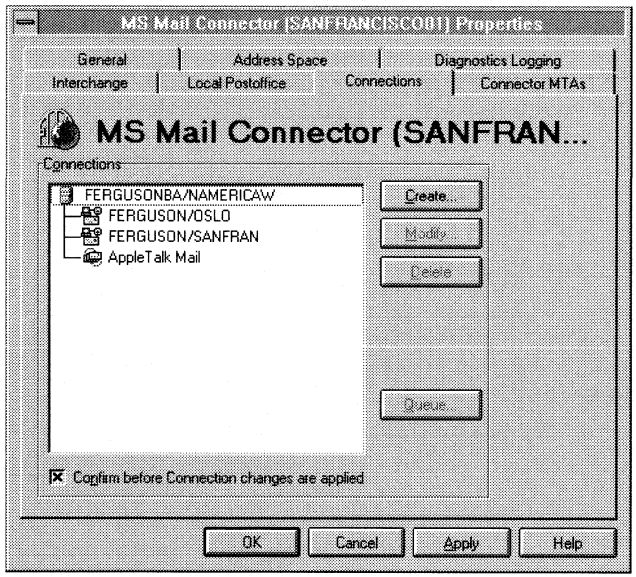
Option	Description
Network	The Microsoft Mail network name (up to 10 characters) of the Microsoft Mail Connector postoffice. The default name is based on the Microsoft Exchange Server organization name.
Postoffice	The Microsoft Mail postoffice name (up to 8 characters) of the Microsoft Mail Connector postoffice. The default name is based on the Microsoft Exchange Server site name.
Sign-on ID	The serial number identifier assigned during installation. It cannot be changed.
Sign-on Password	The password (up to 8 characters) required to connect to the Microsoft Mail Connector postoffice. The default is PASSWORD.
Regenerate	Regenerates the Connector postoffice address.

Connections Properties

Most of the options in the **Connections** property page are specific to MS Mail (PC). You can view the Connector MTA message queue for messages intended for an MS Mail (AppleTalk) recipient, but you cannot create, modify, or delete an MS Mail (AppleTalk) connection. A connection is configured when you enable the Microsoft Mail Connector (AppleTalk) MTA in the **Interchange** property page.

Getting to the Connections property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Connections** tab.



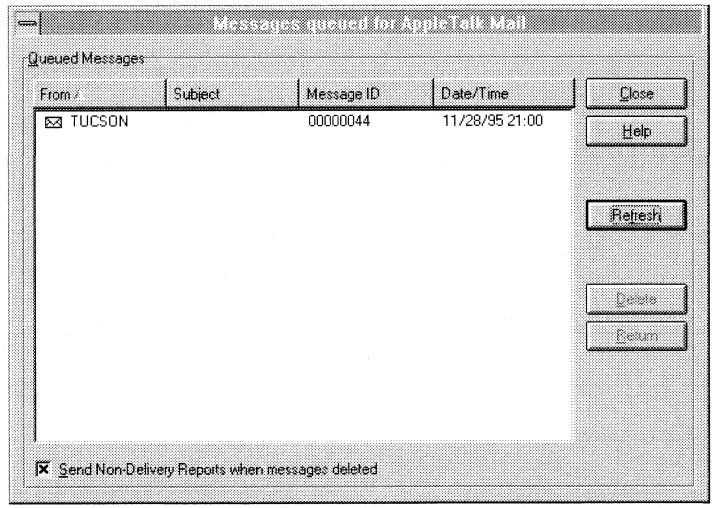
For information on configuring the Connector MTA, see "Setting Up the Microsoft Mail Connector (AppleTalk) MTA" earlier in this chapter.

Viewing the MS Mail (AppleTalk) Message Queue

Use the **Connections** property page to view the Connector MTA message queue for mail pending transfer from the Connector postoffice to the MS Mail (AppleTalk) server. When you view the message queue, you see a snapshot of the queue status. The ability to view message queue activity is useful for troubleshooting message progress through the connector.

Note View the Connector MTA message queue for messages pending transfer before stopping the Microsoft Mail Connector (AppleTalk) MTA service.

1. Select the **Connections** tab.
2. In the **Connections** box, select **AppleTalk Mail**.
3. Choose **Queue**.
4. Select **Refresh** to update queue status information.



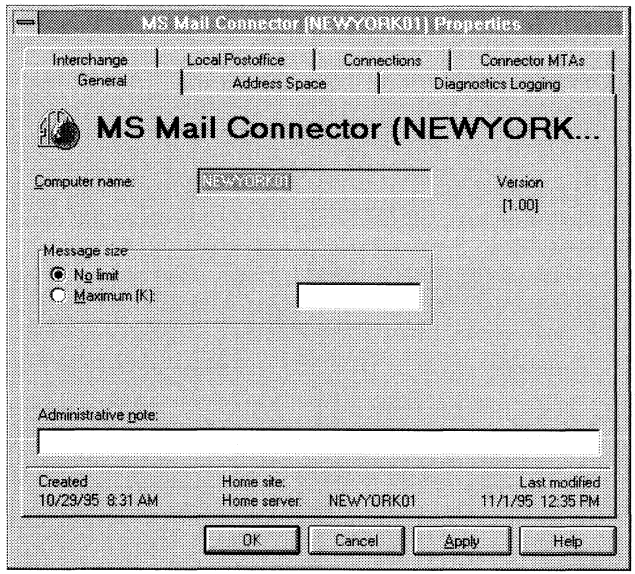
Option	Description
Refresh	Updates the display to reflect the current queue status.
Delete	Deletes a message from the queue.
Return	Returns a message and removes it from the queue.
Send Non-Delivery Reports when messages deleted	Sends a notice to the sender when a message is deleted from the queue. This option is selected by default.

General Properties

Use the **General** property page to set the basic properties for the Microsoft Mail Connector. You can establish the limits for message size transfer between Microsoft Exchange Server and Microsoft Mail. You can also determine installation and the date of last modification for the Microsoft Mail Connector.

Getting to the General property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **General** tab.



Defining Message Size Limits

You can define a size limit for messages passed through the connector. When you define a size limit, it is applied to both MS Mail (PC) and MS Mail (AppleTalk) systems. Setting a maximum message size can reduce the amount of traffic across your network.

1. Select the **General** tab.
2. Under **Message size**, determine a limit value.

Option	Description
No limit	Messages of all sizes transferred. This is the default.
Maximum (K)	Maximum message size (1 to 9999999 kilobytes) to be transferred.

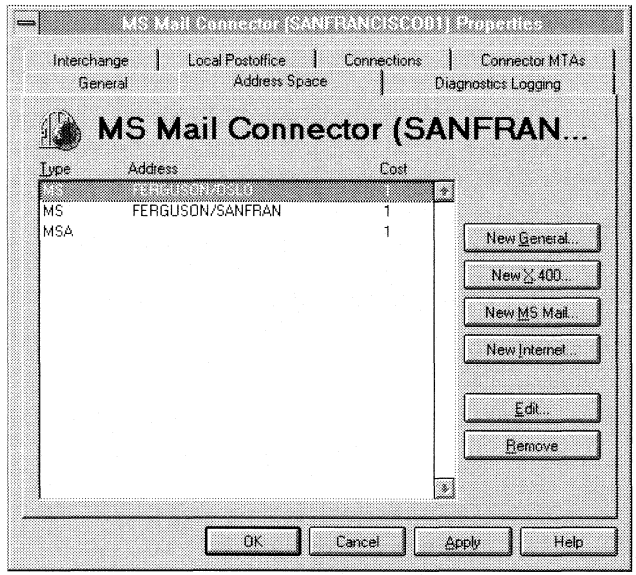
Address Space Properties

Use the **Address Space** property page to define the type and format of addresses used to identify messages to the Microsoft Mail system. Each entry is called an *address space* and contains only as much of the address as is necessary to distinguish messages that should be sent through the connector.

After the procedures for configuring the Microsoft Mail Connector interchange are complete, a default address space for MS Mail (AppleTalk) is automatically created. This new address space is designated as type MSA. No additional address information is specified. Messages destined for any MS Mail (AppleTalk) server will be processed by the Microsoft Mail Connector.

Getting to the Address Space property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Address Space** tab.



For more information on address spaces and routing for MS Mail (AppleTalk) systems, see *Microsoft Exchange Server Concepts and Planning*.

Defining Additional Addressing and Routing Information

Use the **Address Space** property page to define additional addressing and routing information for this Microsoft Mail Connector. You can then specify which MS Mail (AppleTalk) servers are to be serviced by the Microsoft Mail Connector. For example, your site may have more than one instance of the Microsoft Mail Connector servicing multiple MS Mail (AppleTalk) servers. For each Microsoft Mail Connector, you can specify the address information of individual MS Mail (AppleTalk) servers to which you would like to route messages.

Note When configuring the interchange, the Microsoft Mail Connector address space routes messages to all MS Mail (AppleTalk) servers by default. When connecting a single MS Mail (AppleTalk) server, no additional address space configuration is necessary.

---

1. Select the **Address Space** tab.
2. Choose **New**.
3. Choose **Other**.
4. In the **Type** box, type **MSA** for an MS Mail (AppleTalk) address space.
5. In the **Address** box, type the address information.
6. In the **Cost** box, type a routing cost.
7. Choose **OK** to return to the **Address Space** property page.

Option	Description
Address	Enter address information using the Microsoft Mail (AppleTalk) server addressing format (*accountname@servername*). Wildcard characters can be used within the address space. For example, typing ***@SALES** matches MARK@SALES and MARIE@SALES. If you want all messages of the type MSA to be sent through this connector, leave this box empty.
Cost	Enter a routing cost for messages sent through the connector at this address space. The default is 1.

Editing an Address Space

In some cases, an existing address space may require modification. You can edit the address space type, address format, and routing cost for the connector in the **Address Space** property page.

For example, you may want to restrict message delivery to a group of MS Mail (AppleTalk) servers. By editing the address format for specific servers, you can list only the servers maintained by the connector.

1. Select the **Address Space** tab.
2. Select an entry.
3. Choose **Edit**.
4. Make the appropriate changes.

For information on the **MSA Properties** dialog box options, see "Defining Additional Addressing and Routing Information" earlier in this chapter.

Removing an Address Space

You may need to remove an address space. For example, to modify routing of an MS Mail (AppleTalk) server through another instance of a Microsoft Mail Connector, you can remove the server listing from one connector and add it to another.

1. Select the **Address Space** tab.
2. Select an entry.
3. Choose **Remove**.

Diagnostics Logging

You can control how logging information for the Microsoft Mail Connector is written to the Windows NT Event Log. You can specify the types of events that are logged for the Microsoft Mail Connector and the level of logging information for each event. Viewing the event log for connector services is useful when troubleshooting message transfer through the connector.

For additional information about diagnostics logging, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

Setting Up Connector Diagnostic Logging

You can enable logging for three connector services to be written to the application event log. For each category, you can assign a level of logging. The level determines which events generated by that service are logged. Normally, you would want to log only critical events. However, when a problem occurs, detailed events may disclose a path to the source of the problem. The three service categories available for logging are:

MSExchangeMSMI Connector interchange activity for message transfer between Microsoft Exchange Server and the Connector postoffice.

MSExchangePCMTA Connector (PC) MTA activity for MTA transport between the Connector postoffice and a directly connected MS Mail (PC) postoffice.

MSExchangeATMTA Microsoft Mail Connector (AppleTalk) MTA activity for MTA transport between the MS Mail (PC) and the MS Mail (AppleTalk) areas of the Connector postoffice.

1. Select the **Diagnostics Logging** tab.
2. In the **Category** box, select a service category.
3. In the **Logging Level** box, select a level.

Option	Description
None	Only critical events and error events are logged. This is the default.
Minimum	Very high-level events are logged. This setting is appropriate for the beginning of an investigation when the location of the problem is in doubt.
Medium	This setting is appropriate when the problem has been narrowed to a service or group of categories.
Maximum	A complete trail of the operation of the service. This level is appropriate when the problem has been traced to a particular category.

Microsoft Exchange Connection Setup

From a Macintosh computer on your local area network (LAN), you can connect to the Connector postoffice after you configure it as a Macintosh-accessible volume on the Windows NT Server computer. The MS Mail (AppleTalk) server computer uses AppleShare, a Macintosh file sharing protocol, to connect to the Connector postoffice just as if it were an AppleShare server.

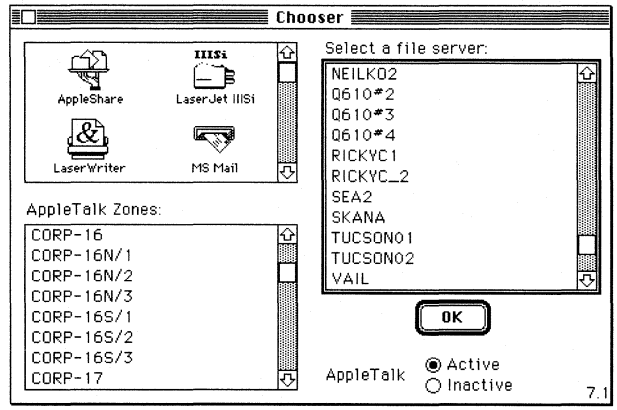
Setting up Microsoft Exchange Connection includes the following tasks:

- Connect to the Microsoft Mail Connector postoffice.
- Install the Microsoft Exchange Connection software.
- Configure the Microsoft Exchange Connection.
- Set the connection times.

Connecting to the Microsoft Mail Connector Postoffice

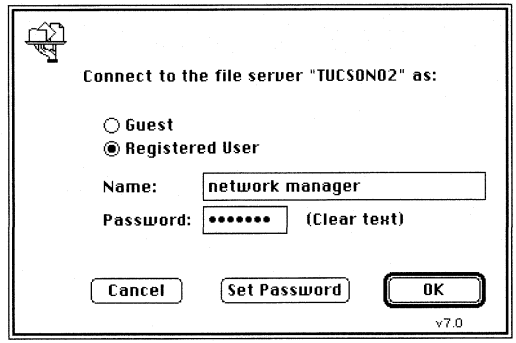
You must connect to the Connector postoffice from the Macintosh server to install Microsoft Exchange Connection software. The MS Mail (AppleTalk) administrator should configure the Chooser to connect to the volume that contains the Connector postoffice at startup. If the volume is not available to the Macintosh server, mail will not be transferred.

1. From the **Apple** menu, choose the **Chooser**.

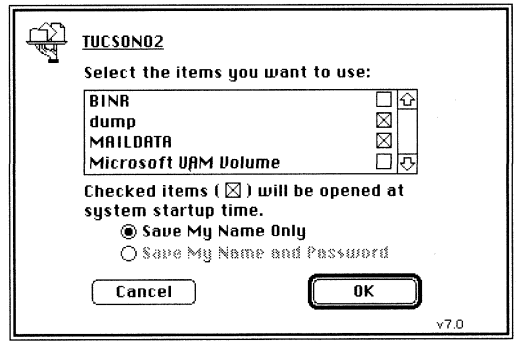


2. Choose the **AppleShare** icon.

3. In the **Select a file server** box, select the name of the Microsoft Exchange Server computer, and then choose **OK**.



4. Type the name and password to access the volume.
5. Choose **OK** to display the available volumes.



6. In the **Select the items you want to use** box, select the volume that contains the Microsoft Mail Connector postoffice, and then choose **OK**.
7. Select the check box to the right of the volume to open the connection at startup.
8. Choose **OK**, and quit the **Chooser**.

Option	Description
Guest	Select if you have chosen to allow guests to use this volume.
Registered User	Select if you have set permissions on this volume to exclude guest users and allow registered users.
Name	The name you specified when creating the volume (typically the Microsoft Exchange Server service account).
Password	The password you specified when creating the volume (typically the Microsoft Exchange Server service account).

Installing Microsoft Exchange Connection Files

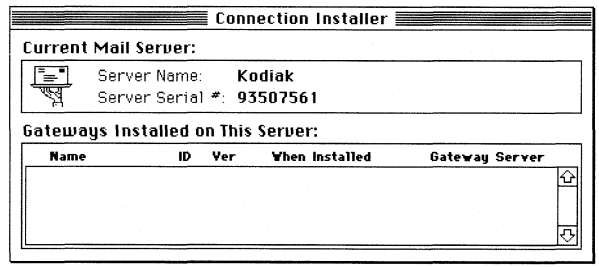
Microsoft Exchange Server provides a floppy disk of all the files required to install the Microsoft Exchange Connection gateway. Before you install the Microsoft Exchange Connection gateway, you must first install the necessary files on your mail server.

1. Insert the Microsoft Exchange Connection floppy disk into a floppy drive on your MS Mail (AppleTalk) server.
2. Double-click Installer.
3. Choose **Install**.
4. Choose **Restart**.

Installing the Microsoft Exchange Connection Gateway

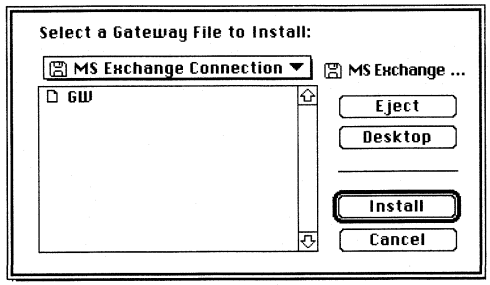
You can install Microsoft Exchange Connection software on the MS Mail (AppleTalk) server you want to act as the gateway to Microsoft Exchange Server. The installation places a Macintosh Chooser extension, the Microsoft Exchange Connection gateway, into the Extensions folder of the server System folder. For more information, see your Microsoft Mail for AppleTalk documentation.

1. Log on to mail as network manager.
2. Open the **MS Exchange Connection** folder.
3. Open the **Connection Installer** folder.
4. Choose **Exchange Connection Installer**.

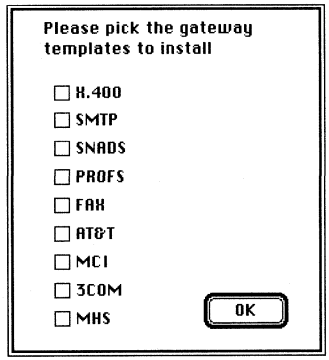


5. Select a gateway.

6. From the **Gateway** menu, choose **Install Gateway**.



7. Select **GW** and choose **Install**.
8. In the **Gateway ID** box, type a gateway identifier.
9. In the **Gateway Name** box, type a new name for this gateway.
10. Choose **OK**.



11. Select the templates you want to install.
12. Choose **OK** to complete the Microsoft Exchange Connection installation.
13. From the **File** menu, choose **Quit**.

Option	Description
Gateway ID	Enter a unique gateway identifier for each MS Mail (AppleTalk) site. The default is NC (2 characters).
Gateway Name	The name for the gateway you are installing. The default is Exchange Connection.
Gateway templates	Install only the templates for gateways you will access.

Microsoft Exchange Connection Configuration

After the Microsoft Exchange Connection has been installed, you can configure the basic connection options. While configuring the gateway connection, the MS Mail (AppleTalk) administrator selects the Connector postoffice volume from which messages are to be exchanged, and sets options for the amount, size, and age of messages handled by the gateway. In addition, the administrator specifies the logging level for gateway activity and the connection times.

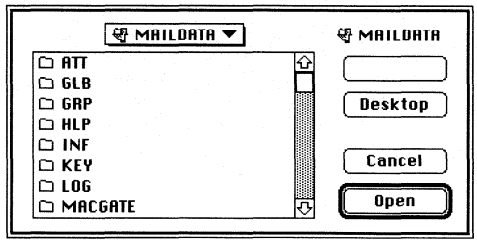
Specifying the Postoffice Location

If you are configuring the Microsoft Exchange Connection for the first time, you must specify the location of the Connector postoffice. To move messages, the MS Mail GW extension must know the location of the Connector postoffice. Once the location has been established, you can determine parameters for messages being passed through the gateway.

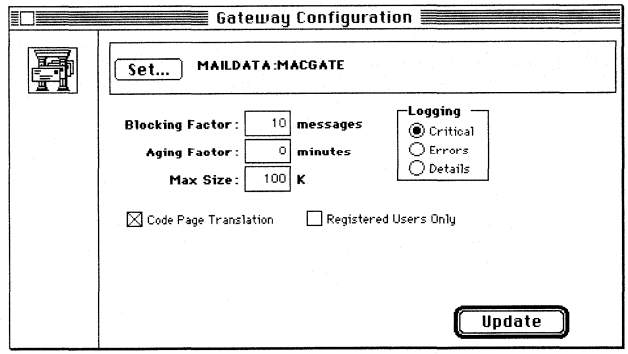
Note The gateway configuration is stored in the Macgate.ini file on the Microsoft Exchange Server computer.

---

1. Log on to mail as network manager.
2. From the **Mail** menu, choose **Gateway**, and then choose **Configuration**.
3. Choose **OK** to locate the connection store directory.
4. Select **Desktop**, and choose **Open**.
5. Select **MAILDATA**, and choose **Open**.



6. Select **MACGATE,** and choose **Open.**



7. Type values for **Blocking Factor**, **Aging Factor**, and **Max Size**.
8. Select a logging level.
9. Specify whether you want code page translation and whether the gateway is to service only registered users.
10. Choose **Update**.

Option	Description
Blocking Factor	The maximum number of messages that can be transferred per gateway cycle. The default is 10.
Aging Factor	The maximum amount of time a message can stay in the Connector postoffice before a message is sent to the network manager. A value of zero prevents warning messages from being sent. The default is 0.
Max Size	The maximum message size including attachments. The default is 100 KB.
Critical	Logs only major message transfer failures. This is the default.
Errors	Logs only message transfer failures.
Details	Logs all message transfer activity.
Code Page Translation	Clear to prevent mapping of characters from one code page to another. This option is selected by default.
Registered Users Only	Select to allow only users with gateway accounts to send messages through this gateway. This option is cleared by default.

If you have already specified the location of the Connector postoffice in a previous installation and would like to reconfigure an existing gateway configuration, see "Setting Gateway Options" later in this chapter.

Setting Gateway Options

Use the **Gateway Configuration** command to set the basic gateway options. You can specify a new Connector postoffice, set gateway message parameters, and determine logging levels for the gateway connection.

Note The Microsoft Mail Connector limits the length of an MS Mail (AppleTalk) user's address to 252 characters. If a message is sent to the Microsoft Exchange Server from a user with a longer address, it is returned as non-deliverable.

---

1. Log on to mail as network manager.
2. From the **Mail** menu, choose **Gateway Configuration**.
3. Choose **Set** to connect to a different Connector postoffice.
4. Type values for **Blocking Factor**, **Aging Factor**, and **Max Size**.
5. Under **Logging**, select a logging level.
6. Specify whether you want code page translation and whether the gateway is to service only registered users.
7. Choose **Update**, and restart the server.

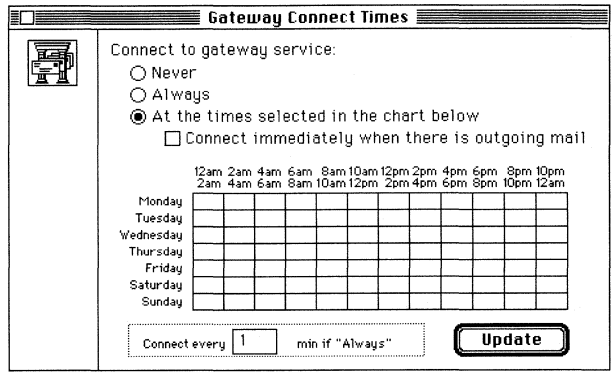
Option	Description
Blocking Factor	The maximum number of messages that can be transferred per gateway cycle. The default is 10.
Aging Factor	The maximum amount of time a message can stay in the Connector postoffice before a message is sent to the network manager. A value of zero prevents warning messages from being sent. The default is 0.
Max Size	The maximum message size including attachments. The default is 100 KB.
Critical	Logs only major message transfer failures. This is the default.
Errors	Logs only message transfer failures.
Details	Logs all message transfer activity.
Code Page Translation	Clear to prevent mapping of characters from one code page to another. This option is selected by default.
Registered Users Only	Select to allow only users with gateway accounts to send messages through this gateway. This option is cleared by default.

If you are configuring the Microsoft Exchange Connection for the first time, see "Specifying the Postoffice Location" earlier in this chapter.

Setting the Gateway Connection Times

After you configure the basic Microsoft Exchange Connection gateway settings, you can configure the gateway connection times. You can limit the amount of time the gateway connection is in service. For example, you may want to restrict message exchange to a specific time of day due to network bandwidth or leased line cost considerations.

1. From the **Mail** menu, choose **Gateway Connect Times**.
2. Choose the **Microsoft Exchange Connection** icon.



3. Under Connect to gateway service, select an option.
4. If you choose **At the times selected in the chart below**, select times to connect and transfer messages in the schedule grid.
5. Choose **Update**.

Option	Description
Never	Select to stop message transfer.
Always	Select to connect on a continuous basis. The default is 1 minute.
At the times selected in the chart below	Select to set up specific connection times in the schedule grid.
Connect immediately when there is outgoing mail	Overrides the specified schedule for outgoing messages only.

Access Connection Gateway Installation

After you install the Microsoft Exchange Connection on a MS Mail (AppleTalk) server, you can use an access connection gateway for additional servers you want to connect to Microsoft Exchange Server through the gateway. An access connection gateway allows mail servers not directly connected to the Microsoft Mail Connector to exchange messages with recipients on a Microsoft Exchange Server.

For example, you may have an MS Mail (AppleTalk) system with multiple servers. You can configure the Microsoft Exchange Connection on one server that will serve as a gateway postoffice. You can then install the access gateway connection on the remaining MS Mail (AppleTalk) servers. These servers will have an indirect connection through the Microsoft Exchange Connection for sending messages to Microsoft Exchange Server recipients. Setting up an access gateway is a two-part process that requires:

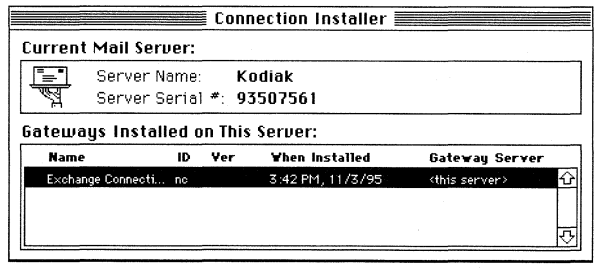
- Extracting the access connection gateway from the server on which the Microsoft Exchange Connection gateway is installed.
- Installing the access connection gateway on another MS Mail (AppleTalk) server.

For more information on how access connection gateways work, see your Microsoft Mail for AppleTalk Networks documentation.

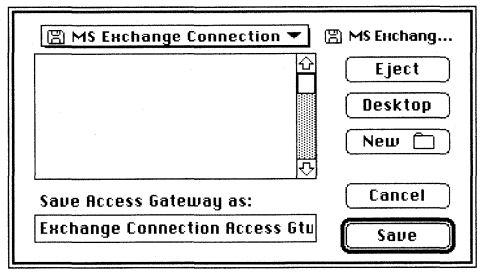
Extracting the Access Connection Gateway

You can extract the access connection gateway from the Microsoft Exchange Connection using the Microsoft Exchange Connection floppy disk. When the access connection gateway is extracted from the server on which the Microsoft Exchange Connection is installed, an icon is placed on the Microsoft Exchange Connection floppy disk. This is used to install the access connection gateway on MS Mail (AppleTalk) servers.

1. Log on to mail as network manager.
2. Insert the Microsoft Exchange Connection floppy disk.
3. Choose **Exchange Connection Installer**.



4. In the **Gateways Installed on This Server** box, select the **Exchange Connection Gateway**.
5. From the **Gateway** menu, choose **Extract Access Gateway**.
6. Type a name for the access gateway, and choose **Save**.



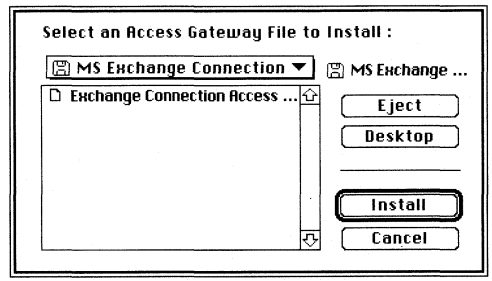
Installing the Access Connection Gateway

Before you install an access connection gateway on an MS Mail (AppleTalk) server, make sure you have completed the procedure for extracting the access connection gateway. You can use an access connection gateway component for mail servers you want to indirectly connect to the Microsoft Exchange Server through the Microsoft Exchange Connection gateway.

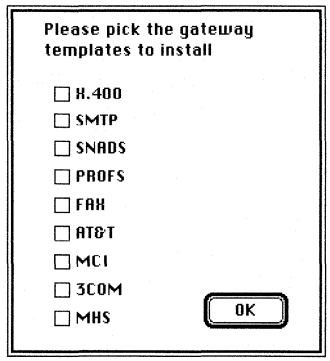
Note Gateway addresses that are not supported by the Microsoft Exchange Connection are not available for installation.

---

1. Log on to mail as network manager.
2. Insert the Microsoft Exchange Connection gateway floppy disk.
3. Choose **Exchange Connection Installer**.
4. From the **Access** menu, choose **Install Access Gateway**.



5. Select the access connection gateway file you extracted from the server with the Microsoft Exchange Connection gateway, and then choose **Install**.



6. Select the templates you want to install.
7. Choose **OK**.

Microsoft Mail for AppleTalk Networks Connection Gateway

Although Microsoft Exchange Server provides the Microsoft Mail Connector for connectivity with MS Mail (AppleTalk), administrators may choose to use the Microsoft Mail for AppleTalk Networks Connection Gateway version 1.0b provided with Microsoft Exchange Server. To do this, you change the Microsoft Exchange Connector postoffice to route mail through the actual postoffice that hosts the version 1.0b gateway.

Installing Microsoft Mail for AppleTalk Networks Connection Gateway

To install the Microsoft Mail for AppleTalk Networks Connection Gateway version 1.0b:

1. Run Macsetup.exe from the <Exchsrvr>\Connect\Msmcon\Bin directory.
2. Press ENTER after the first screen.
3. Choose **Remove**.
4. Type the path to the Microsoft Exchange Maildata directory:

   ```
   <exchsrvr>\connect\msmcon\maildata
   ```

5. Choose **Y**.
6. Type the Network and Postoffice name through which Macintosh-bound mail should be routed. This is the postoffice where the version 1.0b gateway is installed.
7. Type the path to the Microsoft Exchange Connection executables:

   ```
   <exchsrvr>\connect\msmcon\bin
   ```

8. Enter the path to the Microsoft Exchange Connection postoffice:

   ```
   <exchsrvr>\connect\msmcon\maildata
   ```

9. Press ENTER.

Microsoft Exchange Server and Quarterdeck Mail Server Connections

To connect Microsoft Exchange Server to Quarterdeck Mail servers, you must add an addressing .Dll file to Microsoft Exchange Server. The Macproxy.dll file automatically creates a Quarterdeck Mail address type (MSA) for Microsoft Exchange Server recipients. The Quarterdeck Mail proxy enables Microsoft Exchange Server to convert addresses into the correct Microsoft Exchange Server address so replies will work. To automatically create the MSA address type, install the Macproxy.dll before adding recipients to Microsoft Exchange Server.

Installing the Macproxy.dll

1. Create the following subdirectories in the Exchange\Address directory, depending on the platform you have:

   msa\<*server type*> (e.g., i386, alpha, ppc)

2. Copy the Macproxy.dll from the Connect\Msmcon\Bin subdirectory to the platform-specific directory.

3. Run the address installation program (Addrinst.exe) located in the Support\Macproxy\platform\Msmcon directory with the following parameters:

   /sitedn=site name

   /name="Quarterdeck Mail proxy generator"

   /machine=server type

   /type=MSA

   /proxydll=path to macproxy.dll

   /server=server name

   /gwproxy=gateway name on Mail server

Note By default, the gateway name on the Quarterdeck Mail server is Exchange Connection, but it can be changed at installation. Once the Quarterdeck Mail Proxy.dll is installed, it functions like other proxy generators and can be configured in the **Site Addressing** property page.

---

4. For optimal performance transferring messages, set the polling interval (available on the **Gateway Connect** menu) to **Always** with an interval of three minutes and a **blocking factor** (set from the **Gateway Configuration** menu) of 30. This allows the Quarterdeck Mail server to empty the gateway queue without spending too much time checking the connection status. Microsoft Exchange Server is faster than Quarterdeck Mail and can process the messages without becoming backlogged.

Test the Connections

After you configure the Microsoft Mail Connector and the Microsoft Exchange Connection, you should test the connection before allowing general message transfer or starting any messaging-based services. To test the connection, send a message from a Microsoft Exchange Server recipient to an MS Mail (AppleTalk) recipient. To ensure a complete connection from both sides of the connector, you can send a message from an MS Mail (AppleTalk) client to a Microsoft Exchange Server recipient. Because address lists have not been exchanged between systems, you must enter the network, postoffice, and mailbox names for any recipients you wish to send a test message to.

For information on synchronizing directory information, see Chapter 11, "Directory Synchronization for Microsoft Mail."

Sending Messages from the Microsoft Exchange Server Computer

You can test the Microsoft Mail (AppleTalk) Connector by sending test messages from a Microsoft Exchange Server recipient to an MS Mail (AppleTalk) recipient. This will determine if the Microsoft Exchange Server side of the connector is functioning correctly.

Before you send a test message from a Microsoft Exchange Server recipient to an MS Mail (AppleTalk) recipient, create a custom recipient address for the mailbox you are sending the test message to. After the address is created, the recipient will appear in your personal address book (PAB). You must know the user name and server name for the recipient.

Using the MS Mail (AppleTalk) Client

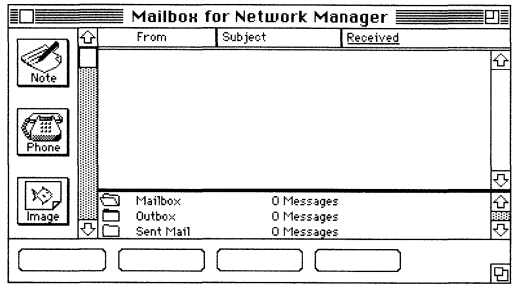
You can test the Microsoft Mail Connector by sending test messages from an MS Mail (AppleTalk) client to a Microsoft Exchange Server recipient. This will determine if the MS Mail (AppleTalk) side of the connection is functioning correctly.

Before you send a test message from an MS Mail (AppleTalk) client to a Microsoft Exchange Server recipient, create an address for the mailbox you are sending the test message to. After the address is created, the recipient will appear in your address list. You must know the network, postoffice, and mailbox names for the recipient. This information can be found in the Microsoft Exchange Server Administrator program.

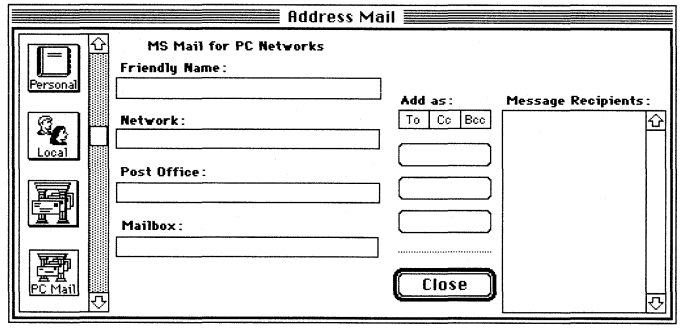
Note If you send messages using the Bcc feature in MS Mail (AppleTalk) to Microsoft Exchange or MS Mail (PC) users, the information in the **Bcc** line appears in the **To** box when the message is received.

---

1. In the MS Mail (AppleTalk) client, choose the Note icon.



2. Choose the PC Mail Gateway icon.

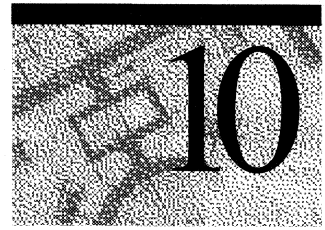


3. Type the **Friendly Name**, **Network**, **Post Office**, and **Mailbox** information.
4. Choose **Add**.
5. Choose **Close**.
6. Send the test message.

Option	Description
Friendly Name	The name that will appear in your PAB.
Network	The Microsoft Mail Connector network name, which can be found in the **Local Postoffice** property page.
Post Office	The Microsoft Mail Connector postoffice name, which can be found in the **Local Postoffice** property page.
Mailbox	The name for the recipient, which can be found in the recipient's **E-mail Addresses** property page. For example, Jonathan Fredricks will have an MS listing of jonathanf.

CHAPTER 10

Microsoft Mail for PC Networks



The Microsoft Mail Connector is used for information transfer between Microsoft Exchange Server sites and Microsoft Mail for PC Networks. Each server in your organization can run one instance of the Microsoft Mail Connector, servicing one or more connections to MS Mail postoffices and gateways using a local area network (LAN), X.25, or asynchronous connections.

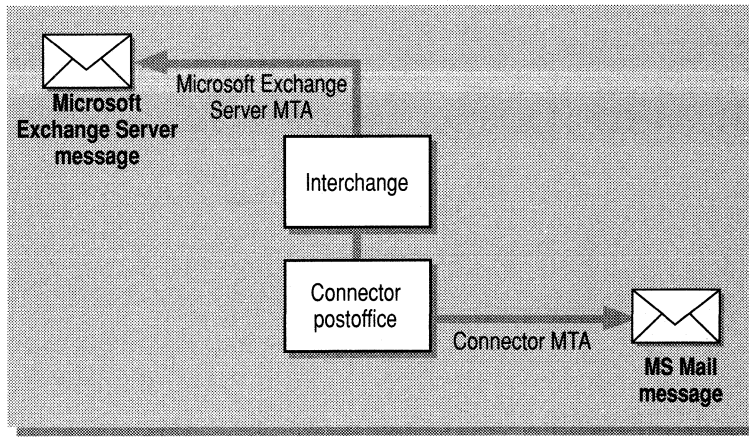
Microsoft Exchange Server uses three components of the Microsoft Mail Connector to communicate with MS Mail (PC) systems.

Microsoft Mail Connector interchange A Windows NT Server service that routes and transfers messages between Microsoft Exchange Server and the Microsoft Mail Connector postoffice.

Microsoft Mail Connector postoffice A temporary information store for messages in transit.

Microsoft Mail Connector (PC) message transfer agent (MTA) A Windows NT Server service that transfers messages between the Connector postoffice and the MS Mail postoffice.

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



The Microsoft Mail Connector (PC) MTA can perform most functions of the MS Mail External (and Multitasking MTA) programs, including message delivery and distribution to recipients on MS Mail (PC) postoffices on the same LAN. Therefore, it isn't necessary to set up the MS Mail External program on LAN-based MS Mail postoffices.

When connecting to an MS Mail postoffice over asynchronous or X.25, you must set up an instance of the MS Mail External program (or Multitasking MTA) at the remote postoffice. Message delivery and distribution to an MS Mail (PC) postoffice using a Microsoft Mail Connector (PC) MTA can only be performed over a LAN connection.

For more information about the MS Mail External and Multitasking MTA programs, see the *Microsoft Mail for PC Networks Administrator's Guide* and the *Microsoft Mail Multitasking MTA Administrator's Guide*.

Microsoft Mail Connector Setup

Setting up the Microsoft Mail Connector to communicate with MS Mail (PC) postoffices includes the following:

- Configure the Microsoft Mail Connector interchange.
- Configure the Microsoft Mail Connector general properties.
- Set up an MS Mail postoffice connection.
- Configure an MTA.
- Configure the Microsoft Mail Connector in the MS Mail Administrator program.
- Start the Microsoft Mail Connector services.

Configuring the Microsoft Mail Connector interchange and the general connector properties is the same for LAN, asynchronous, and X.25 connections. However, setting up a connection and configuring an MTA instance is unique for each connection type.

You must have the Microsoft Mail Connector installed on your Microsoft Exchange Server before proceeding with the connector set up.

For Microsoft Mail Connector installation information, see *Microsoft Exchange Server Getting Started.*

Quick Start

To set up the minimum configuration requirements for a LAN-connected Microsoft Mail Connector (PC), use the following list of procedures in the order in which they appear.

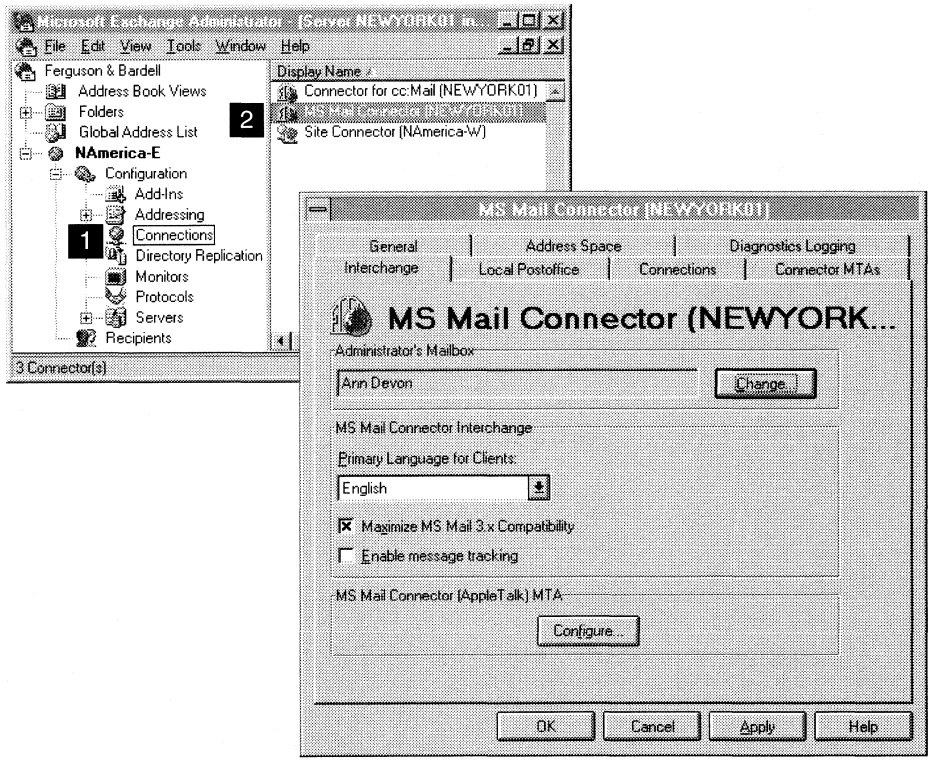
Task	Description
Configure the Connector **Interchange** property page.	In the Connector **Interchange** property page, assign an administrator's mailbox.
Configure the **Connections** property page.	In the **Connections** property page, create a LAN connection to the MS Mail (PC) postoffice.
Configure the **Connector MTAs** property page.	In the **Connector MTAs** property page, configure a Connector MTA for servicing LAN-connected MS Mail (PC) postoffices.
Define the MS Mail (PC) postoffices the Connector MTA will service.	In the **Connector MTAs** property page, specify the MS Mail (PC) postoffices the Connector MTA will service.
Start the MS Mail (PC) MTA service.	Start the MS Mail (PC) MTA service from Control Panel.
Test the connection.	Send a mail message from a Microsoft Exchange Client to an MS Mail (PC) recipient. Send a message from an MS Mail (PC) client to a Microsoft Exchange Server recipient.

Microsoft Mail Connector Configuration

The Microsoft Mail Connector is configured using the Microsoft Exchange Server Administrator program. You can administer the Microsoft Mail Connector from any Windows NT Workstation or Windows NT Server that is part of your network.

Getting to the Microsoft Mail Connector property pages

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and then choose **Connections**.
2. Double-click MS Mail Connector.



Interchange Properties

Use the **Interchange** property page to configure how the Connector interchange moves and translates information between Microsoft Exchange Server and the Microsoft Mail Connector. Configuring the Connector interchange must be done for LAN, asynchronous, and X.25 connections. To configure the Microsoft Mail Connector interchange, you must do the following:

- Assign an administrator's mailbox for receiving delivery status messages.
- Establish a primary language used by the majority of postoffices using the connector.
- Enable MS Mail clients to receive OLE 2.0 embedded objects from Microsoft Exchange clients.

Whether you are connecting to an MS Mail postoffice across a LAN or using an asynchronous or X.25 connection, you must configure the **Interchange** property page before you configure other property pages.

Getting to the Interchange property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and then choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Interchange** tab.

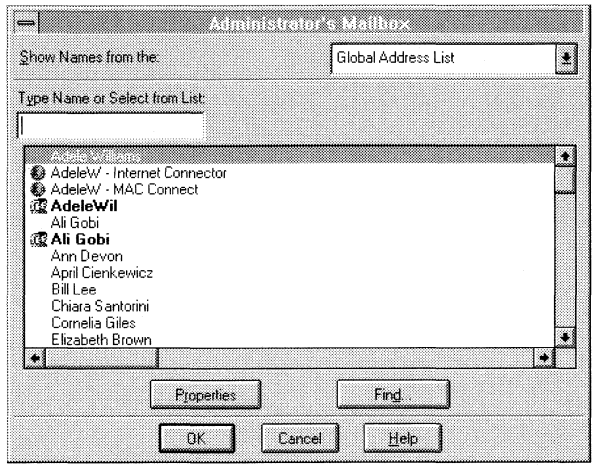
Assigning an Administrator's Mailbox

Use the **Interchange** property page to assign an administrator's mailbox to receive delivery status messages.

Tip You can create a mailbox called postmaster to receive delivery messages.

---

1. Select the **Interchange** tab.
2. Choose **Change**.
3. Select a recipient for the administrator's mailbox.



Option	Description
Show Names from the	Select the global address list or a container.
Type Name or Select from List	Type a name or select one from the list.
Properties	Display the properties for the mailbox.
Find	Search for a name based on a specific set of criteria.

Specifying the Primary Language for Clients

Use the **Interchange** property page to specify the primary language for the Microsoft Mail Connector. This is necessary for interoperability with MS Mail 3.*x* clients that use a different language. Select the language that the majority of your clients use. The default is the language being used by Microsoft Exchange Server.

1. Select the **Interchange** tab.
2. Under **Primary Language for Clients**, select a language.

Configuring MS Mail 3.*x* Client Compatibility

MS Mail 3.*x* supports early versions of OLE only. To enable MS Mail 3.*x* users to view saved or embedded objects sent from Microsoft Exchange clients, the Microsoft Mail Connector can be configured to create two versions of each OLE object. This option will double the size of any OLE message. If this option is not selected, MS Mail 3.*x* clients cannot view or save embedded objects sent from Microsoft Exchange clients.

1. Select the **Interchange** tab.
2. Select **Maximize MS Mail 3.x Compatibility**.

Enabling Message Tracking

The Administrator program has a tool used for tracking message movement that can be applied when troubleshooting message flow through a connector. You can follow the progress of a message as it passes from the Microsoft Exchange Server information store to a directly connected MS Mail (PC) postoffice. To use this tool, you must first enable message tracking in the **Interchange** property page.

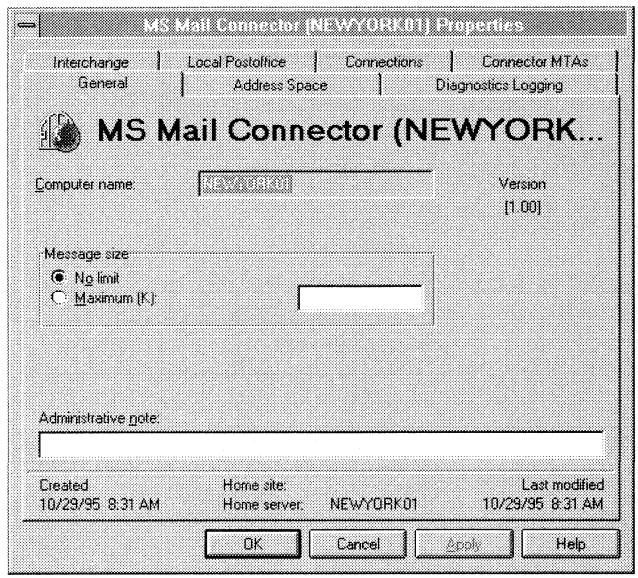
1. Select the **Interchange** tab.
2. Select **Enable message tracking**.

General Properties

Use the **General** property page to set the basic properties for the Microsoft Mail Connector. You can set limits for message size transfer between Microsoft Exchange Server and MS Mail. You can also enter an administrative note as well as determine the installation and last modification date for the Microsoft Mail Connector.

Getting to the General property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **General** tab.



Defining the Computer Name

You can view the Microsoft Exchange Server computer name in the **General** property page. However, you cannot modify the computer name from this page. To change the computer name, you must open Control Panel and double-click the Network icon.

For information on changing your computer name, see your Windows NT Server documentation.

Specifying Message Size Limits

You can specify a size limit for messages passed through the connector. When you define a message limit, it is applied to both MS Mail (PC) and MS Mail (AppleTalk) systems. Setting a maximum message size can reduce the amount of mail traffic across your network.

1. Select the **General** tab.
2. Under **Message size**, specify a limit.

Option	Description
No limit	Messages of all sizes transferred. This is the default.
Maximum (K)	Maximum message size (1 to 9999999 kilobytes) to be transferred.

LAN Connection to MS Mail

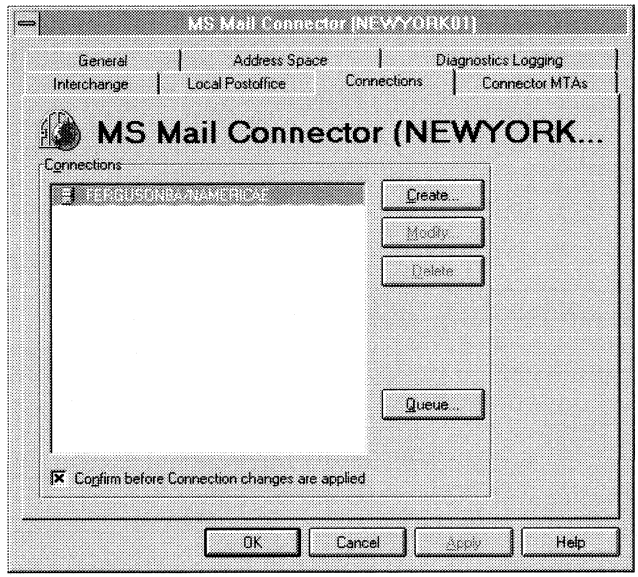
You can connect a Microsoft Exchange Server computer to an MS Mail (PC) postoffice across a LAN. This section describes how to configure the Microsoft Mail Connector for a LAN connection, and then test the connection. You should first complete the previous sections describing how to configure the Connector **Interchange** and **General** property pages before configuring a LAN connection to an MS Mail (PC) postoffice.

LAN Connection Setup

When you establish a LAN connection to an MS Mail postoffice, the Microsoft Mail Connector extracts the network and postoffice names from the external postoffice. No manual entry of external postoffice information is necessary. You need to know only the network path to the directory where the external postoffice is stored.

Getting to the Connections property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and then choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Connections** tab.



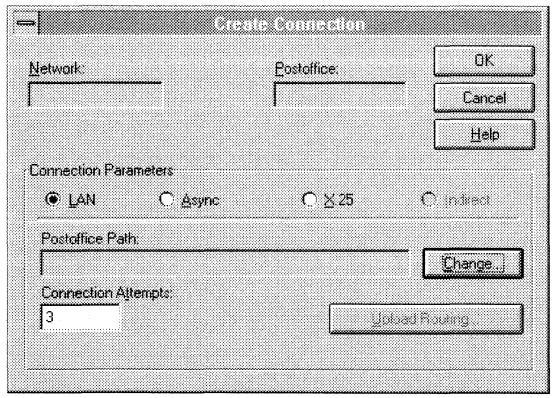
Creating a LAN Connection

You can create and view LAN connections to MS Mail (PC) postoffices in the **Connections** property page. You can also specify whether the Microsoft Mail Connector will indirectly access any postoffices that a LAN-connected postoffice exchanges mail with.

Note Before attempting to connect to a NetWare server, your Windows NT Server must be running the Gateway Service for NetWare. When typing a network path to a NetWare server, use the uniform naming convention (UNC) format (*\\servername\sharename\path* for a Windows NT Server or *\\servername\volumename\path* for a NetWare server). For example, an MS Mail (PC) postoffice located on a NetWare server with server name Server1, volume name Sys, and directory name Maildata would require the network path \\Server1\Sys\Maildata.

---

1. Select the **Connections** tab.
2. Choose **Create**.



3. Under **Connection Parameters**, select **LAN**.
4. To enter the **Postoffice Path**, choose **Change**.
5. In the **Path** box, type the full path to the server using UNC format.
6. In the **Connect As** box, type the logon identifier. Type a logon ID only if the MS Mail postoffice is in a non-trusted domain or the Windows NT service account is not a valid user on the server where the postoffice exists
7. In the **Password** box, type the account password if necessary, and then choose **OK** to return to the **Create Connection** dialog box.
8. In the **Connection Attempts** box, type a value (1 to 99) to set the number of attempts to send mail before it is returned to the sender with a non-delivery report (NDR). The default is 3.
9. Choose **Upload Routing** to display a list of any indirect postoffices connected to the MS Mail postoffice. You can include any of the postoffices on the routing list.

   For more information on indirect routing, see "Indirect Connections to MS Mail Postoffices" later in this chapter.

Confirming Connection Changes

You have the option to view a confirmation message when changes have been made to the **Connections** property page. This option is selected by default.

1. Select the **Connections** tab.
2. Select or clear the **Confirm before Connection changes are applied** check box.

Removing Connections

If service to a specific MS Mail postoffice is no longer necessary, you can delete the connection to that postoffice without disturbing other message transfer processes.

Note You must delete any indirect postoffice connections routed through a direct postoffice before deleting that direct postoffice.

---

1. Select the **Connections** tab.
2. In the **Connections** box, select a postoffice.
3. Choose **Delete**.

MTA Configuration for a LAN-Connected Postoffice

You use the **Connector MTAs** property page to define and configure Microsoft Mail Connector (PC) MTAs for transferring messages between the connector and one or more MS Mail postoffices. Each Connector (PC) MTA you define in the **Connector MTAs** property page becomes a separate Windows NT service. The Connector MTA can be started or stopped using the Windows NT Server Manager or Control Panel. You can run as many instances of the Connector (PC) MTA as necessary on a single Microsoft Exchange Server computer.

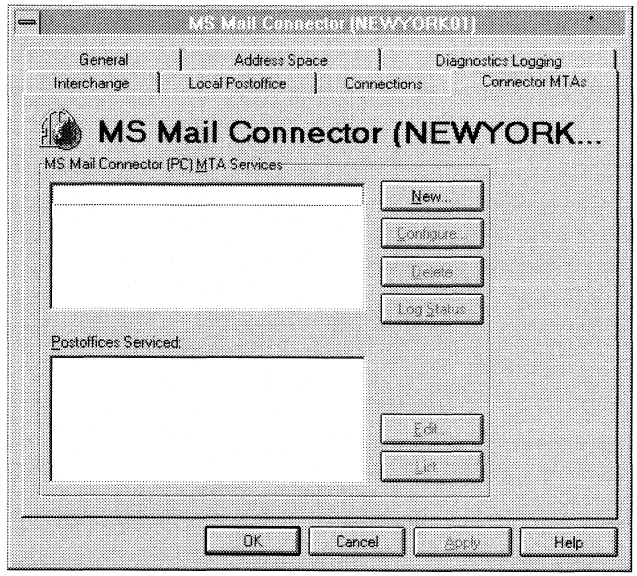
Connector (PC) MTAs can service MS Mail postoffices for three connection configurations:

- LAN only
- Asynchronous and LAN
- X.25 and LAN

Each instance of the Connector (PC) MTA should generally service one primary type of connection, such as LAN, asynchronous, or X.25. To optimize performance, you should create a separate instance of the Connector (PC) MTA to service a group of postoffices based on the connection used.

Getting to the Connector MTAs property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and then choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Connector MTAs** tab.



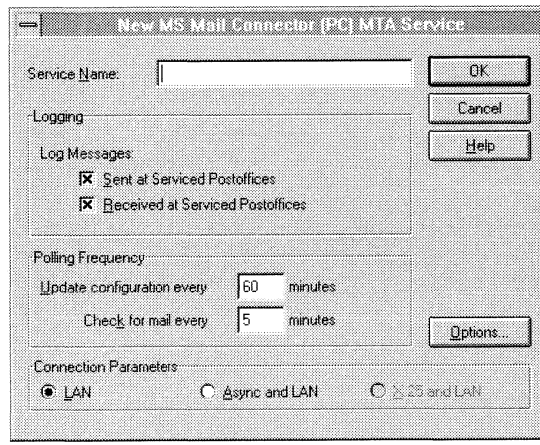
Setting Up a Microsoft Mail Connector (PC) MTA for LAN Connections

To transfer messages between the Microsoft Mail Connector and one or more MS Mail postoffices, you must configure a Microsoft Mail Connector (PC) MTA. When you create a Connector MTA service, you give it a name that can be viewed in the **Services** portion of the Control Panel. You also have the option to create a log to record all messages sent to and received from an external postoffice.

Note By default, the Microsoft Mail Connector (PC) MTA uses the Microsoft Exchange Server service account specified during installation.

---

1. Select the **Connector MTAs** tab.
2. Choose **New** to create a new Connector (PC) MTA.



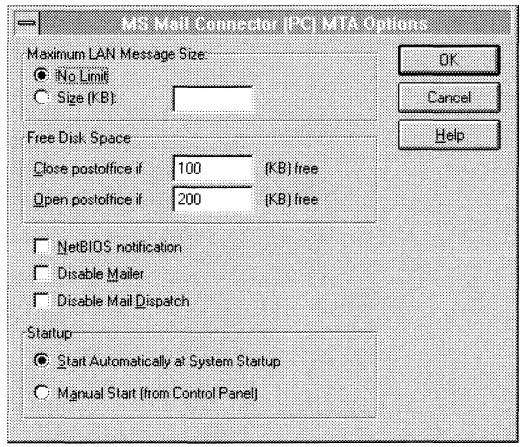
3. Type the service name.
4. Specify logging options.
5. Specify the polling frequency.
6. Choose **OK** to return to the **Connector MTAs** property page.

Option	Description
Service Name	This name is used to register a new Connector (PC) MTA instance as a Windows NT service. You can use up to 30 characters, including a-z (lowercase), A-Z (uppercase), and the space. If you are editing an existing Connector (PC) MTA, you cannot modify the service name.
Sent at Serviced Postoffices	Logs messages delivered to MS Mail postoffices. The log is stored in the LOG directory of the Connector postoffice.
Received at Serviced Postoffices	Logs messages received from MS Mail postoffices. The log is stored in the LOG directory of the Connector postoffice.
Update configuration every	Determines how often (0 to 999 minutes) the Connector MTA is to check both the Connector postoffice and the MS Mail postoffice for updated user and network information. The default is 60 minutes. Specifying 0 stops new configuration checking.
Check for mail every	Determines how often (0 to 999 minutes) the Connector MTA is to check both the Connector postoffice and the MS Mail postoffice for mail. The default is 5 minutes. Specifying 0 minutes causes continuous polling.

Configuring Connector (PC) MTA Options

After performing the previous task described in "Setting Up a Microsoft Mail Connector (PC) MTA for LAN Connections," you can then configure the Connector (PC) MTA options. You can enable options for controlling how the Connector MTA will handle special MS Mail (PC) postoffice features, such as Mail Dispatch and NetBIOS notification. You can also determine whether you would like the Connector MTA service to start manually or with system startup.

1. Select the **Connector MTAs** tab.
2. Select an MTA service, and choose **Configure**.
3. Choose **Options**.



4. Type a LAN message size.
5. Specify free disk space information.
6. Select an MTA startup method.

Option	Description
Maximum LAN Message Size	Choose the size limit (0 to 999999 KB) for messages. The default is **No Limit**.
Close postoffice if	The minimum amount of disk space (0 to 999999999 KB) required on a destination postoffice for message transfer to be performed. If the available space is less than this amount, the Connector (PC) MTA marks the postoffice as unavailable and does not deliver messages until the open variable is reached.
Open postoffice if	The minimum amount of disk space (0 to 999999999 KB) required to restore the destination postoffice to an available state after being marked unavailable. If the available space on an unavailable postoffice rises above this amount, the postoffice is marked available, and the Connector (PC) MTA resumes mail delivery.
NetBIOS notification	Select to notify MS Mail users about new mail immediately using NetBIOS. Both the client computer and the server running the Connector (PC) MTA must be running NetBIOS for notification to occur. If this option is selected, any message submitted with a high priority overrides the Connector (PC) MTA polling frequency setting and causes the message to be transmitted immediately.
Disable Mailer	Prevents this instance of the Connector (PC) MTA from distributing messages to users on LAN-connected MS Mail postoffices.
Disable Mail Dispatch	Prevents this instance of the Connector (PC) MTA from delivering messages to LAN-connected postoffices.
Start Automatically at System Startup	This instance of the Connector MTA service starts with system services startup. This is the default.
Manual Start (from Control Panel)	This instance of the Connector MTA service must be started manually from Control Panel or Server Manager.

For more information on the External program mailer function, see the *MS Mail for PC Networks Administrator's Guide*.

Removing a Connector MTA Service

If connectivity provided by a Connector (PC) MTA is no longer necessary, you can delete that Connector (PC) MTA. This immediately stops all message transfer provided by that Connector (PC) MTA and removes it from the Windows NT services registry.

Note Before removing a Connector MTA service, you must first stop the service from the Control Panel.

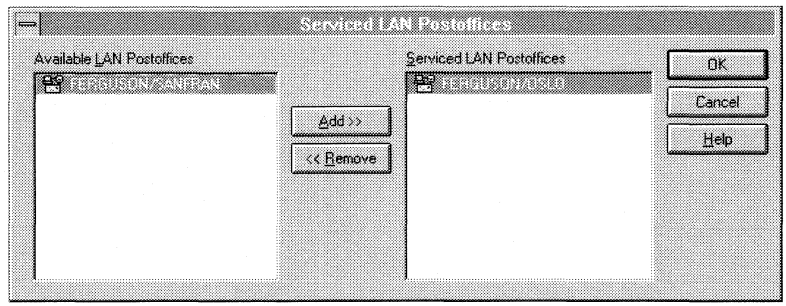
---

1. Select the **Connector MTAs** tab.
2. In the **MS Mail Connector (PC) MTA Services** box, select a service.
3. Choose **Delete**.

Setting Up Service to LAN-Connected Postoffices

A single Connector MTA instance can service more than one LAN-connected MS Mail postoffice. You use the **Connector MTAs** property page to specify which MS Mail postoffices each Connector (PC) MTA services.

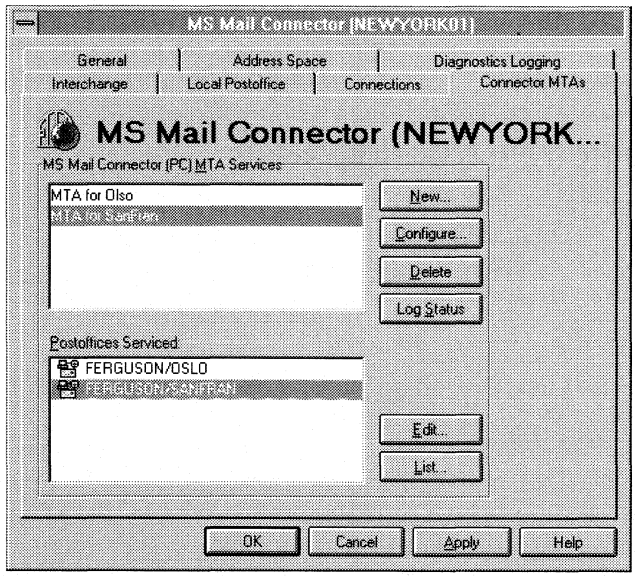
1. Select the **Connector MTAs** tab.
2. In the **Microsoft Mail Connector (PC) MTA Services** box, select a Connector (PC) MTA.
3. Choose **List**.
4. Under **Available LAN Postoffices**, select a postoffice.
5. Choose **Add** to add the service to the postoffice.
6. Choose **OK** to return to the **Connector MTAs** property page.



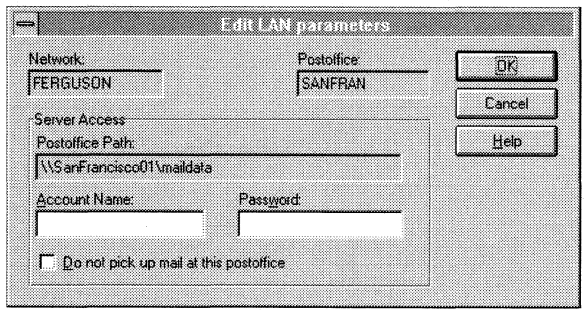
Setting LAN Postoffice MTA Options

Use the **Connector MTAs** property page to modify LAN parameters for a specific MS Mail postoffice on the same LAN. You may want to assign a specific network user account for each occurrence of an MTA service. For example, a Connector (PC) MTA service that logs on to a NetWare server can be assigned an account name, password, and user rights for the MS Mail postoffice Maildata directory. This is helpful in determining connection information from a NetWare server.

1. Select the **Connector MTAs** tab.
2. Select an MS Mail (PC) postoffice being serviced by a Connector (PC) MTA.



3. Choose **Edit**.



4. In the **Account Name** box, type the logon name.

5. In the **Password** box, type the logon account password.
6. Select **Do not pick up mail at this postoffice** to send but not receive messages from the MS Mail (PC) postoffice.
7. Choose **OK** to return to the **Connector MTAs** property page.

Option	Description
Account Name	The network logon name required to log on to a LAN Manager or NetWare server accessing the MS Mail postoffice.
Do not pick up mail at this postoffice	Select to send but not receive messages from the MS Mail postoffice. Another external program must be running at the destination postoffice to assume the responsibility of distributing the mail on the destination postoffice.

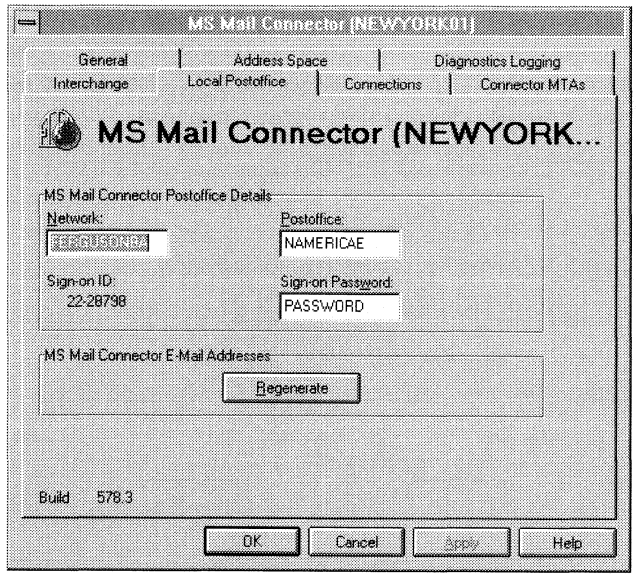
MS Mail (PC) Postoffice Configuration

When you finish setting up the Microsoft Mail Connector, you must configure each MS Mail (PC) postoffice that you identified in the Microsoft Mail Connector. You can use the MS Mail 3.*x* Administrator program to create an external postoffice list for the Microsoft Exchange Server you are communicating with.

Use the **Local Postoffice** property page in the Microsoft Mail Connector to obtain the postoffice and network name of the Microsoft Mail Connector. This information will be used in the MS Mail (PC) Administrator program to configure the Microsoft Mail Connector postoffice as an external postoffice. You must do this for every MS Mail (PC) postoffice that uses the Microsoft Mail Connector, whether the connection is direct or indirect. The type of connection specified in the MS Mail (PC) Administrator program depends on how that postoffice is configured on the Microsoft Mail Connector.

Getting to the Local Postoffice property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and then choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Local Postoffice** tab.



For more information about creating external postoffices, see the *MS Mail for PC Networks Administrator's Guide*.

Modifying Local Postoffice Properties

Use the **Local Postoffice** property page to change the network name and postoffice name for the Connector postoffice. These names are used to identify the Microsoft Exchange Server externally for routing services between MS Mail postoffices and the Microsoft Exchange Server. The default names are determined during installation from the Microsoft Exchange Server organization and site names. In a typical configuration, you would not change these names. You can also assign or reassign an existing password for the Connector postoffice.

For example, you may want to group a set of postoffices by a single network name. You can change a Connector postoffice name in the **Local Postoffice** property page and then regenerate the change to represent the new MS Mail address for the postoffice.

The Connector interchange and all instances of the Connector (PC) MTA read the network and postoffice name at startup. If you want the changes you have made to take effect immediately, stop and then restart the Connector interchange and Connector (PC) MTAs.

Warning Any change to network or postoffice names requires regeneration of the MS address type for the Connector postoffice. Changing the network or postoffice name after message transfer has started causes messages that were in transit during the change to be returned. You must modify the external list for the Connector postoffice for all Microsoft Mail postoffices connected directly or indirectly to the connector. You must also stop, reconfigure, and restart all Microsoft Mail gateways and occurrences of the External program.

1. Select the **Local Postoffice** tab.
2. In the **Network** box, type a network name.
3. In the **Postoffice** box, type a postoffice name.
4. In the **Sign-on Password** box, type a password.
5. Choose **Regenerate**.

Option	Description
Network	The MS Mail network name (up to 10 characters) of the Microsoft Mail Connector postoffice. The default name is based on the Microsoft Exchange Server organization name.
Postoffice	The MS Mail postoffice name (up to 8 characters) of the Microsoft Mail Connector postoffice. The default name is based on the Microsoft Exchange Server site name.
Sign-on ID	The serial number identifier that is assigned during installation. This identifier cannot be changed. A sign-on ID is required for an external MS Mail postoffice that has been specified as direct route type and connected through an asynchronous or X.25 connection.
Sign-on Password	The password (up to 8 characters) required to connect to the Microsoft Mail Connector postoffice. A sign-on password is required for an external MS Mail postoffice that has been specified as direct route type and connected through an asynchronous or X.25 connection. The default is PASSWORD.
Regenerate	Regenerates the Connector postoffice address.

Test the Connection

After you configure the Microsoft Mail Connector, you should test the connection before allowing general message transfer or starting any message-based services. To test the connection, you need to send a message from a Microsoft Exchange Server mailbox to an MS Mail (PC) recipient. Furthermore, to ensure a complete connection from both sides of the connector, you can send a mail message from an MS Mail (PC) client to a Microsoft Exchange Server recipient.

Because address lists have not been exchanged between systems, you need to enter the network, postoffice, and mailbox names for recipients you wish to send a test message to.

For information on synchronizing directory information, see Chapter 11, "Directory Synchronization for Microsoft Mail."

Using the MS Mail (PC) Client

You can test the Microsoft Mail Connector by sending test mail messages from an MS Mail (PC) client to a Microsoft Exchange Server recipient. This will help determine if the MS Mail (PC) side of the connection is functioning correctly. Once you have tested the connector from an MS Mail (PC) client, you should also send a test message from a Microsoft Exchange Server mailbox to an MS Mail (PC) recipient.

Before you send a test message from an MS Mail (PC) client to a Microsoft Exchange Server recipient, you will need to create a recipient address for the mailbox you are sending the test message to. Once the address is created, the recipient will appear in your personal address list. You must know the network, postoffice, and mailbox names for the recipient. This information can be found in the Microsoft Exchange Server Administrator program.

Note Before testing the connection, verify that the Connector MTA services configured earlier in this chapter have been started. You can start Connector MTA services from the Control Panel.

---

1. In the Microsoft Mail client, compose a new message.
2. Choose **Address**.
3. Choose the **New Address** icon.
4. Select **Custom Address**.
5. Type the e-mail name and address information.
6. Send the test message.

Option	Description
Name	The name that will appear in your personal address book (PAB).
E-mail Address	The MS Mail (PC) style name for the recipient. This can be found by viewing the **E-mail Addresses** property page for the mailbox in the Microsoft Exchange Server Administrator program.
E-mail Type	The mail system type.
Comment	A comment that can be viewed from the **Details** dialog box in the PAB.

Diagnostics Logging

You can control how logging information for the Microsoft Mail Connector is written to the Windows NT Event Log. You can specify the types of events that are logged for the Microsoft Mail Connector and the level of logging information for each event. Viewing the event log for the connector service is useful when troubleshooting message transfer through the connector.

For additional information about diagnostics logging, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

Setting Up Diagnostics Logging

You can enable logging for three connector services to be written to the application event log. You can assign a level of logging for each category. The level determines which events generated by that service are logged. Normally, you would want to log only critical events. However, when a problem occurs, detailed events may disclose a path to the source of the problem. The three service categories available for logging are:

MSExchangeMSMI The Connector interchange activity for message transfer to and from Microsoft Exchange Server and the Connector postoffice.

MSExchangePCMTA The Connector (PC) MTA activity for MTA transport between the Connector postoffice and a directly connected MS Mail (PC) postoffice.

MSExchangeATMTA The Connector (AppleTalk) MTA activity for MTA transport between the MS Mail (PC) and the MS Mail (AppleTalk) areas of the Connector postoffice. This is applicable when the Microsoft Mail Connector is configured for MS Mail (AppleTalk).

1. Select the Diagnostics Logging tab.
2. Under **Category**, select a service category.
3. Under **Logging Level**, select a level.

Option	Description
None	Only critical events and error events are logged. This is the default.
Minimum	Very high-level events are logged. This setting is appropriate for the beginning of an investigation.
Medium	This setting is appropriate when the problem has been narrowed to a service or group of categories.
Maximum	A complete trail of the operation of the service. This level is appropriate when the problem has been traced to a particular category.

Asynchronous and X.25 MS Mail Postoffice Connections

You can connect a Microsoft Exchange Server computer to an MS Mail (PC) postoffice using either an asynchronous or X.25 connection. This section describes how to configure the Microsoft Mail Connector when using either an asynchronous or X.25 connection to an MS Mail (PC) postoffice. You should first complete the earlier sections on configuring the Microsoft Mail Connector **Interchange** and Connector **General** property pages before proceeding with this section.

Asynchronous and X.25 Setup

The procedures for setting up an asynchronous connection and setting up an X.25 connection are similar. To configure either connection, you must manually enter the network name, postoffice name, sign-on ID number, and password (if required). Differences between the two connection types occur when configuring the communication settings. For an asynchronous connection, you must know the phone number to dial when connecting to the external postoffice. For an X.25 connection, you must know the X.121 address for the Microsoft Exchange Server computer and the X.121 address for the external postoffice. Otherwise, the configuration process is the same.

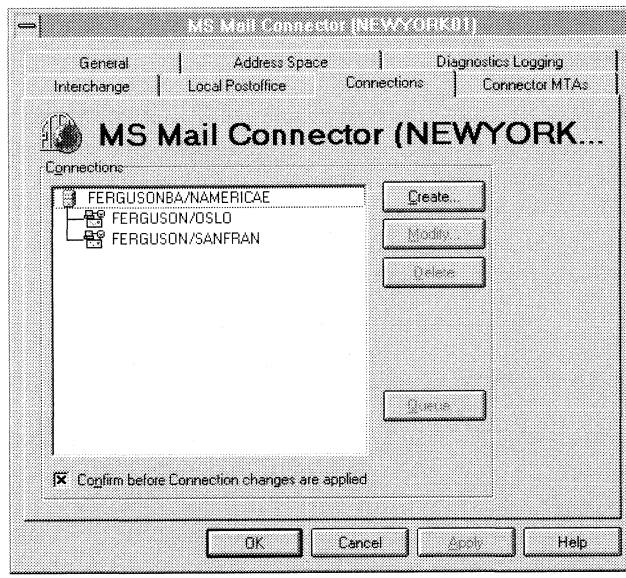
Setting Up an Asynchronous or X.25 Connection

Use the **Connections** property page to set up an asynchronous or X.25 connection to an MS Mail postoffice. Verify that you have an asynchronous communication device, such as a modem, or an X.25 device, such as an Eicon port adapter, correctly installed on the MS Mail postoffice and the Microsoft Exchange Server computer before starting this procedure.

Note Use the MS Mail (PC) Administrator program on each MS Mail postoffice to be connected asynchronously. Use the Config Password command to determine the network name, postoffice name, sign-on ID, and password of the postoffice. You must also verify that each MS Mail postoffice you want to connect to is not a workgroup postoffice. Workgroup postoffices can be identified by a sign-on ID (serial number) that begins with 799 and must be upgraded to the full version of MS Mail before proceeding.

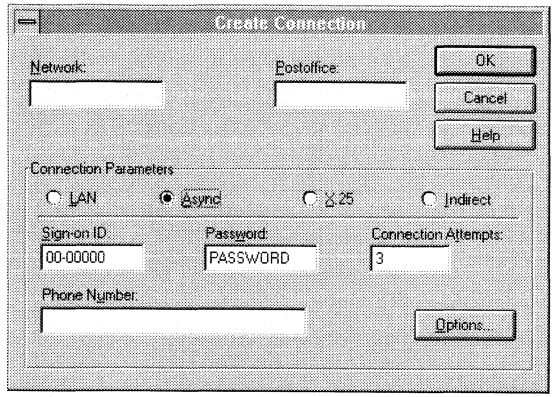
For information on getting to the **Connections** property page, see "LAN Connection Setup" earlier in this chapter.

1. Select the **Connections** tab.



2. Choose **Create**.

3. Under **Connection Parameters**, select **Async** or **X.25**.



4. Type the **Network**, **Postoffice**, and **Connection Parameters** information.

Option	Description
Network	The network name (up to 10 characters) for the postoffice.
Postoffice	The postoffice name (up to 10 characters).
Sign-on ID	The serial number identifier (must be *XX-XXXX* format) for the postoffice.
Password	The password (up to 8 characters) used to log on to the postoffice.
Connection Attempts	The number of times (1 to 99) to attempt to send mail before it is returned to the sender with an NDR. The default is 3.
Phone Number	Appears only if you are configuring an asynchronous connection. Include the entire dialing sequence (up to 40 characters) that you use to reach the postoffice from your location. If you dial 9 to reach an outside line first, you must first include 9 followed by a comma and then the number.
X.121 Address	Appears only if you are configuring an X.25 connection. The X.121 address (up to 16 numeric characters) of the external postoffice. This is necessary only if you are configuring an X.25 connection. For X.121 format information, see Appendix A.

Setting Options for an Asynchronous or X.25 Connection

After performing the previous task, "Setting Up an Asynchronous or X.25 Connection," you can set connection options for individual MS Mail (PC) postoffices using the **Connections** property page. You can configure message limits, parameters for dialing, and registered mail configuration for the connection.

For information on getting to the **Connections** property page, see "LAN Connection Setup" earlier in this chapter.

1. Select the **Connections** tab.
2. Select a connection, and choose **Modify**.
3. Choose **Options**.
4. Type the **Maximum Message Size** and **Intervals** values.

Option	Description
Maximum Message Size	Set maximum message size (0 to 9999 KB) including attachments and excluding routing information to be transferred. The default is **No Limit**.
Failed connection retry for Urgent Mail	Set interval range (1 to 999 minutes) for urgent mail connection attempts. The default is 10 minutes.
Failed connection retry for Normal Mail	Set interval range (1 to 999 minutes) for normal mail connection attempts. The default is 10 minutes.
Dial Every	Set interval range (1 to 999 minutes) for the modem to dial. The default is 30 minutes.
Allow mail reception after sending	Select to send and then receive messages from an MS Mail postoffice during the same connection session. If this option is not selected, the Microsoft Mail Connector receives mail only during connections initiated by the external postoffice.
Return registered mail confirmation	Select to issue a confirmation receipt automatically when users send registered mail to and from this MS Mail postoffice.

Asynchronous and X.25 MTA Configuration

Use the **Connector MTAs** property page to define and configure MS Mail Connector (PC) MTAs for transferring messages between the Connector postoffice and one or more MS Mail postoffices. Each Connector (PC) MTA you define in the **Connector MTAs** property page becomes a separate Windows NT service that can be started or stopped using the Windows NT Server Manager or Control Panel. You can run as many instances of the Connector (PC) MTA as necessary on a single Microsoft Exchange Server computer.

Connector (PC) MTAs can service MS Mail postoffices over connections in three configurations:

- LAN only
- Asynchronous and LAN
- X.25 and LAN

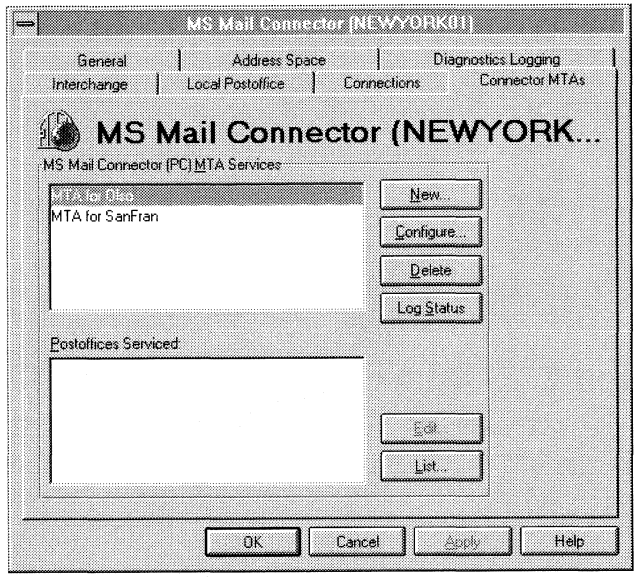
Asynchronous and X.25 MTA Services

Use the **Connector MTAs** property page to define and configure MS Mail Connector (PC) MTAs. The Connector MTA transfers messages between the Connector postoffice and one or more MS Mail postoffices over an asynchronous or X.25 connection.

Note A Connector (PC) MTA set up to provide asynchronous or X.25 message transfer can also service MS Mail postoffices available over a LAN connection. However, each instance of the Connector (PC) MTA should generally service one primary type of connection, such as LAN, asynchronous, or X.25. To optimize performance, you should create a separate instance of the Connector (PC) MTA to service a group of postoffices based on the type of connection used.

Getting to the Connector MTAs property page

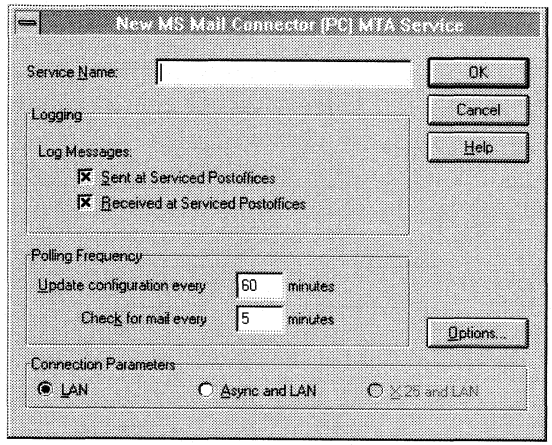
1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and then choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Connector MTAs** tab.



Setting Up an MTA for an Asynchronous Connection

Use the **Connector MTAs** property page to set up an MTA service for an asynchronous connection. Before configuring the MTA service, confirm that a modem is installed and functioning on the Microsoft Exchange Server computer and the external MS Mail postoffice.

1. Select the **Connector MTAs** tab.
2. Choose **New** to create a new Connector (PC) MTA.



3. Under Connections Parameters, select Async and LAN.

Option	Description
Service Name	This name used to register a new Connector (PC) MTA instance as a Windows NT service. You can use up to 30 characters, including a-z (lowercase), A-Z (uppercase), and the space.
Sent at Serviced Postoffices	Logs messages delivered to MS Mail postoffices. The log is stored in the LOG directory of the Connector postoffice.
Received at Serviced Postoffices	Logs messages received from MS Mail postoffices. The log is stored in the LOG directory of the Connector postoffice.
Polling Frequency	These options apply to the LAN component of an async and LAN connection only. If you are using this MTA service exclusively for asynchronous communication, you should accept the default settings. For information on LAN polling, see "Setting Up a Microsoft Mail Connector (PC) MTA for LAN Connections" earlier in this chapter.
Communication Port	The communication port (COM1 to COM256) configured for asynchronous communication. The default is COM1.
Modem Script	A list of modem scripts provided by the MS Mail Connector. Modem scripts are located in the GLB subdirectory of the Connector postoffice. The default is Usgeneric.Scr.
Modem Timeout	The amount of time (0 to 999 seconds) the modem will attempt to establish a connection. The default is 60 seconds.
Two-way mail transfer	Sets the MTA to transfer both incoming and outgoing mail. This option is selected by default.
Transfer incoming mail only	Sets the MTA to transfer incoming mail only.
Transfer out going mail only	Sets the MTA to transfer outgoing mail only.

Setting Up an MTA for an X.25 Connection

Use the **Connector MTAs** property page to set up an MTA service for an X.25 connection. The X.25 adapter must be installed and configured on the Microsoft Exchange Server computer prior to setting up an MTA instance.

1. Select the **Connector MTAs** tab.
2. Choose **New** to create a new Connector (PC) MTA.
3. Under **Connections Parameters**, select **X.25 and LAN**.

Option	Description
Service Name	This name used to register a new Connector (PC) MTA instance as a Windows NT service. You can use up to 30 characters, including a-z (lowercase), A-Z (uppercase), and the space.
Sent at Serviced Postoffices	Logs messages delivered to MS Mail postoffices. The log is stored in the LOG directory of the Connector postoffice.
Received at Serviced Postoffices	Logs messages received from MS Mail postoffices. The log is stored in the LOG directory of the Connector postoffice.
Polling Frequency	These options apply to the LAN component of an async and LAN connection only. If you are using this MTA service exclusively for asynchronous communication, you should accept the default settings. For information on LAN polling, see "Setting Up a Microsoft Mail Connector (PC) MTA for LAN Connections" earlier in this chapter.
X.121 Address	The X.121 address (up to 16 characters) for the location of this connector's MTA instance.
Port Number	The X.25 adapter port number (0 to 255). The default is 255. For more information, see your X.25 adapter documentation.
X.25 Listen User Data	The listen user data information (up to 218 hexadecimal characters) as specified by your X.25 service provider.
X.25 Listen User Facilities	The listen user facilities information (up to 218 hexadecimal characters) as specified by your X.25 service provider.

Modifying an MTA for an X.25 Connection

Use the **Connector MTAs** property page to modify connection and service options for an X.25-connected MS Mail (PC) postoffice.

1. Select the **Connector MTAs** tab.
2. Under **MS Mail Connector (PC) MTA Services**, select an X.25 MTA.
3. Under **Postoffices Serviced**, select a postoffice.
4. Choose **Edit**.
5. Type **Call User Data** and **User Facilities** information.

Note To change the network or postoffice name or to change the X.121 address, use the **Connections** property page.

Option	Description
Call User Data	The call user data information as specified by your X.25 service provider.
User Facilities	The user facilities information as specified by your X.25 service provider.

MS Mail (PC) Postoffice Configuration

When you finish setting up the Microsoft Mail Connector, you must configure each MS Mail (PC) postoffice that you identified in the Microsoft Mail Connector. You can use the MS Mail 3.*x* Administrator program to create an external postoffice listing for the Microsoft Exchange Server you are communicating with.

Use the **Local Postoffice** property page in the Microsoft Mail Connector to obtain the postoffice and network name of the Microsoft Mail Connector. This information will be used in the MS Mail (PC) Administrator program to configure the Microsoft Mail Connector postoffice as an external postoffice. You must do this for every MS Mail (PC) postoffice that uses the Microsoft Exchange Connector, whether the connection is direct or indirect. The type of connection specified in the MS Mail (PC) Administrator program will depend on how that postoffice is configured on the Microsoft Mail Connector.

For more information about creating external postoffices, see the *MS Mail for PC Networks Administrator's Guide*.

Testing an Asynchronous or X.25 Connection

After you have set up an asynchronous or X.25 connection to an MS Mail (PC) postoffice, you will need to test the connection between the two mail systems.

For information on sending test messages, see "Test the Connection" earlier in this chapter.

Indirect Connections to MS Mail Postoffices

The Microsoft Mail Connector allows Microsoft Exchange clients access to MS Mail (PC) postoffices not connected directly through the connector. You can use the **Connections** property page to configure routing information from an indirectly connected postoffice regardless of the transport medium used. Establishing an indirect connection to an external postoffice can be useful when connecting Microsoft Exchange Server to an existing MS Mail (PC) system.

Very little set up is required to establish an indirect connection. For example, you may have an existing MS Mail (PC) system of multiple, mutually communicating postoffices. You can establish a connection through the Microsoft Mail Connector to any one of the MS Mail (PC) postoffices using either a LAN, asynchronous, or X.25 connection. Once the connection is established from the Microsoft Mail Connector, you can then configure an indirect connection to any of the remaining MS Mail postoffices through this MS Mail postoffice. You establish an indirect connection only. You do not have to create a Connector MTA instance for an indirect connection.

Indirect Connection Setup

You set up an indirect connection to an MS Mail postoffice by specifying a directly connected MS Mail postoffice through which messages can be routed in one of two ways:

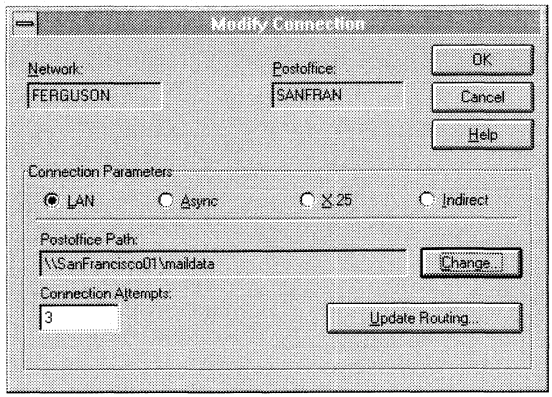
- Upload routing information about indirectly connected postoffices from an MS Mail (PC) postoffice available on the same LAN to the Microsoft Mail Connector.
- Specify routing information about postoffices connected indirectly through an MS Mail postoffice with an asynchronous or X.25 connection.

Uploading Indirect Routing Information

Use the **Connections** property page to import routing information from any MS Mail postoffice available on the same LAN. This can be useful when configuring routing to a large number of postoffices. Instead of manually typing the network and postoffice information for each indirect postoffice, you can download the information to the connector.

1. Select the **Connections** tab.
2. Under **Connections**, select an existing LAN connection.

3. Choose **Modify**.



4. Choose **Upload Routing** or **Update Routing**.

   This button name changes depending on whether there are existing indirect connections through this postoffice.

5. Select any postoffice that you do not want to accept, and choose **Delete**.

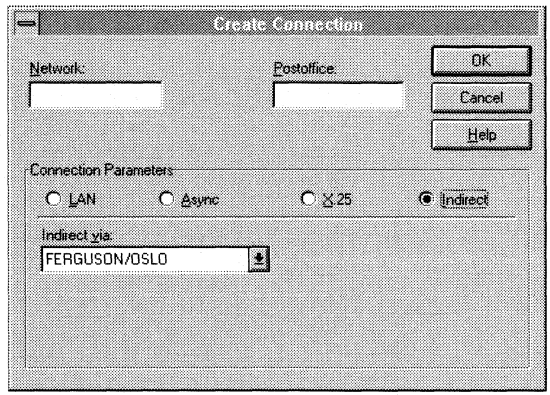
Option	Description
Upload Routing/Update Routing	Displays current routing information about other MS Mail postoffices (or gateways) reached indirectly through this LAN-connected postoffice. Each entry indicates a proposed change to the Microsoft Mail Connector routing information, such as adding or removing an indirect postoffice connection.
Delete	Removes the listing for a postoffice you do not want to connect to indirectly. Deleting postoffice information adjusts only routing information for the Microsoft Mail Connector. No changes are made to connected MS Mail postoffice routing information.

For information on getting to the **Connections** property page, see "LAN Connection Setup" earlier in this chapter.

Manually Creating Indirect Routing Information

You can create indirect connections to postoffices through an asynchronous or X.25 connected postoffice. For example, you may have an instance of the Microsoft Mail Connector transferring mail with an MS Mail (PC) postoffice asynchronously by modem. You can manually configure an indirect connection to any postoffice connected to this remote postoffice. These indirect postoffices may be on the same LAN or connected by asynchronous or X.25 communication type.

1. Select the **Connections** tab.
2. Choose **Create**.
3. Under Connection Parameters, select Indirect.



4. Under **Indirect via**, select a directly connected postoffice.
5. In the **Network** box, type the network name of the indirect postoffice.
6. In the **Postoffice** box, type the postoffice name of the indirect postoffice.

Option	Description
Indirect via	Select an existing directly connected postoffice through which messages will be routed to the indirect postoffice.
Network	The network name for the indirect MS Mail (PC) postoffice. Can be found by the MS Mail 3.*x* Administrator program (Config Password).
Postoffice	The postoffice name for the indirect MS Mail (PC) postoffice. Can be found by the MS Mail 3.*x* Administrator program (Config Password).

For information on importing routing information from a LAN-connected postoffice, see "Uploading Indirect Routing Information" earlier in this chapter.

Testing an Indirect Connection

After you have set up an indirect connection to an MS Mail (PC) postoffice, you will need to test the connection between the two systems.

For information on sending test messages, see "Test the Connection" earlier in this chapter.

MS Mail Gateway on Microsoft Exchange Server

You can use several MS Mail (PC) gateways to provide service between Microsoft Exchange Server and other messaging systems. Within a mixed messaging environment, the Microsoft Mail Connector can act as a gateway postoffice to most MS Mail (PC) gateways and third party gateways.

You can also install an MS Mail Gateway access component on a Connector postoffice. This allows Microsoft Exchange clients access to a foreign system using an existing MS Mail Gateway postoffice. For many mail systems, this is an alternative to installing a gateway postoffice on the Connector postoffice.

The following gateways can be used with Microsoft Exchange Server:

- AT&T Easylink
- Fax
- IBM PROFS and OfficeVision
- MHS
- SNADS
- MCI Mail Gateway

The Microsoft Exchange Server X.400 Connector and Internet Mail Service provide functions that go beyond those of the MS Mail X.400 and SMTP gateways. Thus, the MS Mail X.400 and SMTP gateways cannot be installed on the Connector postoffice. Instead, both the Internet Mail Service or X.400 Connector are used to access either foreign system.

MS Mail Gateway on the Connector Postoffice

When installing an MS Mail gateway on the Microsoft Exchange Server computer, the Microsoft Mail Connector postoffice assumes the role of a gateway postoffice. The gateway access component installed on the Connector postoffice functions identically to an access component installed on an MS Mail postoffice. However, there are no recipient mailboxes on the Connector postoffice.

The gateway access component and the gateway pick up outgoing messages from and place incoming messages in the Connector postoffice. Instead of incoming messages being distributed on the Connector postoffice, they are retrieved by the Connector interchange for Microsoft Exchange Server recipients and recipients on other systems. The messages are then placed in an outbound queue for transfer to the destination mail system.

Each gateway requires:

- A dedicated personal computer running MS-DOS.
- Network software and hardware required to connect to both Microsoft Exchange Server and the foreign system.
- Gateway access component installed on all postoffices using the gateway.
- MS Mail 3.*x* Administrator program for some setup and maintenance tasks.

For more information on MS Mail (PC) gateways on a Microsoft Exchange Server, see *Microsoft Exchange Server Concepts and Planning.*

Installing an MS Mail (PC) Gateway

You can install an MS Mail (PC) gateway on a Microsoft Exchange Server for access to a foreign mail system that is not currently supported by a Microsoft Exchange Server connector. Before installing a gateway on the Connector postoffice, you should verify that the Microsoft Mail Connector is set up correctly using the procedures earlier in this chapter. Moreover, confirm that message transfer is working correctly between Microsoft Exchange Server and all connected MS Mail postoffices.

Note To use an MS Mail gateway, each indirect MS Mail postoffice must have a separate copy of the gateway access component installed and configured. For more information, see your gateway documentation and license agreement.

---

1. Install the gateway component on the Microsoft Exchange Server computer.

   When prompted to specify the gateway postoffice, use the Microsoft Mail Connector postoffice. The mail data files are located in the \Exchsrvr\Connect\Msmcon\Maildata directory.

2. Install the gateway access component on the Microsoft Exchange Server computer.

   When prompted to specify the gateway postoffice, use the \Exchsrvr\Connect\Msmcon\Maildata directory.

3. Install and configure the gateway software on a dedicated gateway computer.

   The configuration procedure varies depending on the type of gateway you are setting up. For more information, see your gateway documentation.

4. Configure the gateway access component for MS Mail (PC) postoffices using the procedures in your gateway documentation. For SNADS and IBM PROFS gateway access components, you must type a gateway name during installation. This gateway name must be the same name that was used for the configuration of the dedicated gateway computer in the previous step.
5. On the Microsoft Exchange Server computer, add entries in the Microsoft Mail Connector **Address Space** property page to direct the MTA to place messages for the gateway in the Connector postoffice.
6. On the foreign system, configure routing.
7. On the dedicated gateway computer, start the gateway program.
8. Restart the Microsoft Mail Connector interchange service.
9. Rebuild the routing table for the Microsoft Exchange Server MTA.
10. Verify that messages can be exchanged between Microsoft Exchange Server and the foreign system.

For information on rebuilding the routing table for Microsoft Exchange Server MTA, see *Microsoft Exchange Server Getting Started.*

Viewing the Gateway Postoffice Queue

After the gateway component and gateway access component have been installed on the Microsoft Mail Connector postoffice, a connections listing for the gateway is added to the **Connections** property page. You can then view the queue for all messages pending transfer. You can also return messages to the originator or delete messages from the queue.

1. Select the **Connections** tab.
2. Under **Connections**, select a gateway listing.
3. Choose **Queue**.
4. Select **Refresh** to update the queue status information.

Option	Description
Refresh	Updates the display to reflect the current queue status.
Delete	Deletes a message from the queue.
Return	Returns a message and removes it from the queue.
Send Non-Delivery Reports when messages deleted	Sends a notice to the sender when a message is deleted from the queue. This option is selected by default.

MS Mail (PC) Gateway Access Component

When you install an MS Mail (PC) gateway access component on the Connector postoffice, Microsoft Exchange Server clients can access a foreign system through an existing MS Mail (PC) gateway postoffice. If you have existing postoffices configured with gateway access components pointing to a gateway postoffice, this is an alternative to installing an MS Mail (PC) gateway on the Connector postoffice.

For more information on the MS Mail (PC) gateway access component on a Connector postoffice, see *Microsoft Exchange Server Concepts and Planning*.

Getting to the MS Mail (PC) Administrator program

When you install an MS Mail (PC) gateway access component on the Connector postoffice, you may need to use the MS Mail Administrator program to perform configuration tasks. A copy of the MS Mail Administrator program is installed along with the Microsoft Mail Connector. The administrator program functions the same way for the Connector postoffice as for an ordinary MS Mail (PC) postoffice. However, there are no mailboxes or mail groups on the Connector postoffice.

1. At the command prompt, switch to the \Exchsrvr\Connect\Msmcon\Bin directory.
2. Type **admin.exe**.

Installing a Gateway Access Component

You install an MS Mail (PC) gateway access component on the Microsoft Exchange Connector postoffice the same as if you were installing it on an MS Mail (PC) postoffice. When the gateway access component is installed, a message from a Microsoft Exchange client intended for a foreign system is passed to the Connector postoffice. The Connector MTA moves the message from the Connector postoffice to the MS Mail (PC) gateway postoffice where it is queued for the foreign system. The MS Mail (PC) gateway process then moves the message to the foreign system.

1. Install the gateway access component on the Microsoft Exchange Server computer. When prompted to specify the gateway postoffice, use the \Exchsrvr\Connect\Msmcon\Maildata directory.
2. Install and configure the gateway software on a dedicated gateway computer.

   The configuration procedure varies depending on the type of gateway you are setting up. For more information, see your gateway documentation.
3. On the Microsoft Exchange Server computer, add entries in the Microsoft Mail Connector **Address Space** property page to direct the MTA to place messages for the gateway in the Connector postoffice.

4. On the dedicated gateway computer, start the gateway program.
5. Restart the Microsoft Mail Connector interchange service.
6. Verify that messages can be exchanged between Microsoft Exchange Server and the foreign system.

Microsoft Mail Connector (PC) Address Space

After the procedures for configuring a connection to an MS Mail (PC) postoffice are completed, an address listing for the external postoffice is automatically added to the Connector address space. This new address space listing is designated as type MS, for Microsoft Mail (PC) systems. The network and postoffice address information for the postoffice is also added automatically. Additional address types can be added to the address space for other mail systems serviced by the Microsoft Mail Connector.

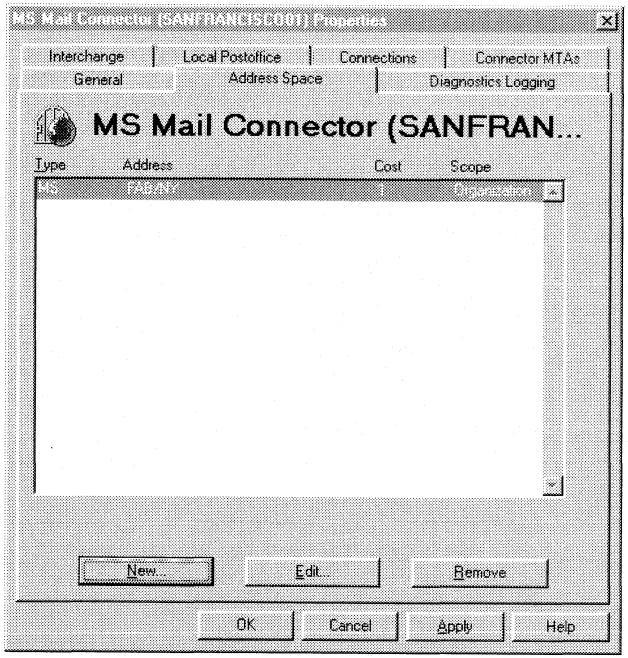
Address Space Configuration

You can configure message routing for the Microsoft Mail Connector in the **Address Space** property page. The address space can be configured to route messages to specific MS Mail postoffices or to route messages intended for a foreign system.

For example, you may want Microsoft Exchange clients to access a PROFS system through an MS Mail PROFS gateway postoffice. You need to configure the Connector address space to accept PROFS message types through the connector. The connector can then route PROFS message types to the MS Mail (PC) gateway postoffice and eventually to the PROFS system.

Getting to the Address Space property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and choose **Connections**.
2. Double-click MS Mail Connector.
3. Select the **Address Space** tab.



For more information on routing or for information on setting up address space types other than MS Mail, see Chapter 4, "Address Spaces."

Configuring Address Spaces for Foreign Systems

You add address space information when the address type and routing cost is not automatically created. When you configure a connection to an MS Mail (PC) postoffice, the address type (MS) and routing cost are automatically entered into the connector address space. However, for a foreign mail system accessed through a gateway on an MS Mail system, you must configure the connector address space.

Note Wildcard characters are implicit in the address space. For example, if you enter the MS address space entry CORP/S, it matches the recipient address for both Corp/Sales/Mark and Corp/Shipping/Marie. You can type a wildcard (* or ?) when necessary to specify a group of addresses. For example, entering SITE?? specifies all entries that contain SITE followed by two alphanumeric characters such as SITE01 and SITE11.

---

1. Select the **Address Space** tab.
2. Choose **New General**.
3. In the **Type** box, type the address type.
4. In the **Address** box, type the address.

Option	Description
Type	Address type used to identify the remote or foreign system, for example, PROFS.
Address	Type enough address information for routing. To route all traffic for a message type through the connector, leave the **Address** box blank. For example, all PROFS message types will be routed through the connector when address information is not entered.
Cost	The routing cost (0 to 100) for messages sent to a foreign system through this connector. The routing cost determines the preference between multiple routes. The default routing cost is 1.

Modifying the Address Space

Use the **Address Space** property page to edit existing address space information. The address type, address format, and routing cost can be modified for any address listing in the connector address space.

1. Select the **Address Space** tab.
2. Select an entry.
3. Choose **Edit**.
4. Make the necessary changes.

For more information on routing, or for information on setting up address space types other than MS Mail, see Chapter 4, "Address Spaces."

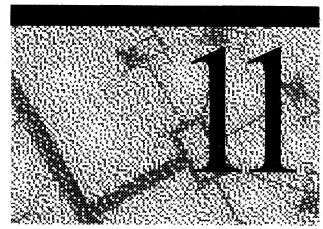
Removing an Address Space Listing

You can remove an address listing that is no longer necessary.

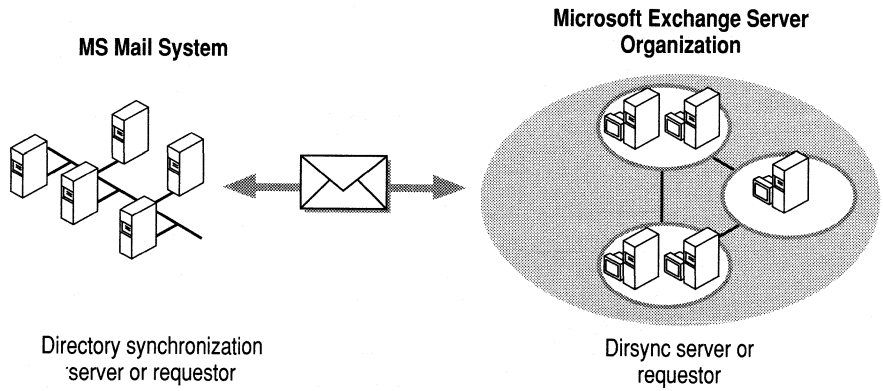
1. Select the **Address Space** tab.
2. Select an entry.
3. Select **Remove**.

CHAPTER 11

Directory Synchronization for Microsoft Mail



Microsoft Exchange Server uses *directory synchronization* to share address information with other messaging systems. Directory synchronization (dirsync) is the process of exchanging address information between your organization and any system that uses the MS Mail directory synchronization protocol.



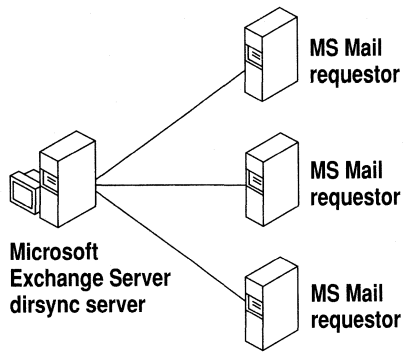
Microsoft Exchange Server uses a component called the directory synchronization agent that can be configured to function in two roles:

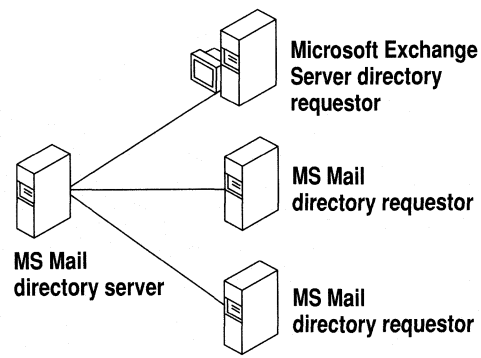
Dirsync requestor Periodically queries the Microsoft Exchange Server directory for changes to recipient information. When Microsoft Exchange Server recipients are added, deleted, or modified, the directory synchronization component sends, according to schedule, an update message to the MS Mail directory server postoffice. It also requests MS Mail address updates from the MS Mail directory server postoffice.

Dirsync server Processes incoming update messages from one or more MS Mail requestors and incorporates the updates in the directory as custom recipient objects. In addition, when the MS Mail directory requestor postoffice requests an update on Microsoft Exchange Server recipients, the dirsync server responds with the changes. You can configure only one directory synchronization server to service all requestors on a site.

The directory synchronization component on a single Microsoft Exchange Server computer can be configured as either a directory synchronization server or requestor. It cannot be configured to function in both roles. Thus, a single Microsoft Exchange Server computer cannot participate in more than one directory synchronization process at the same time. It can be either a requestor to an MS Mail directory server postoffice or a directory synchronization server for other MS Mail requestor postoffices.

For example, the first illustration shows a single Microsoft Exchange Server computer configured to act as a dirsync server to multiple MS Mail remote directory requestors. The second illustration shows the Microsoft Exchange Server computer acting as a directory synchronization requestor.





You must have the MS Mail Dispatch program on a local area network (LAN) to service MS Mail directory requestors. The Dispatch program launches programs necessary to carry out directory synchronization requests on the network. Without Dispatch, automatic dirsync will not run on MS Mail postoffices.

Before setting up directory synchronization, verify that the Microsoft Exchange Server computer in your site and the MS Mail systems you want to include are installed and running correctly. Make sure you can exchange messages between systems. Without mail flow, dirsync will not work. The Microsoft Mail Connector must be installed on the Microsoft Exchange Server you plan to use as either a dirsync requestor or dirsync server.

If you want to include a messaging system other than Microsoft Mail and Microsoft Exchange Server in the directory synchronization process, see the *Microsoft Mail for PC Networks Administrator's Guide,* or use your Internet browser to visit the Microsoft Knowledge Base at http://www.microsoft.com and search for Knowledge Base article PC DirSync: WA0725: Directory Synchronization (Dir-Sync).

For information on planning your organization and directory synchronization, see *Microsoft Exchange Server Concepts and Planning.*

Dirsync Requestor Installation

You can set up Microsoft Exchange Server as a dirsync requestor to one MS Mail (PC) directory synchronization server. A Microsoft Exchange Server dirsync requestor functions similar to an MS Mail directory requestor. Address list updates are sent from the dirsync requestor to the MS Mail (PC) directory server. The MS Mail (PC) directory server compiles a master list of all recent changes to the global address list and sends it to the Microsoft Exchange Server dirsync requestor. The new entries are added to the Microsoft Exchange Server global address list.

Caution You should not configure more than one requestor in the same organization to use a single directory synchronization server. Doing so can result in duplicate or corrupt directory information between sites that use directory replication.

Setting up a Microsoft Exchange Server dirsync requestor to an MS Mail (PC) directory server includes the following:

- Define and configure a dirsync requestor.
- Configure the MS Mail (PC) directory synchronization server to recognize the new requestor.

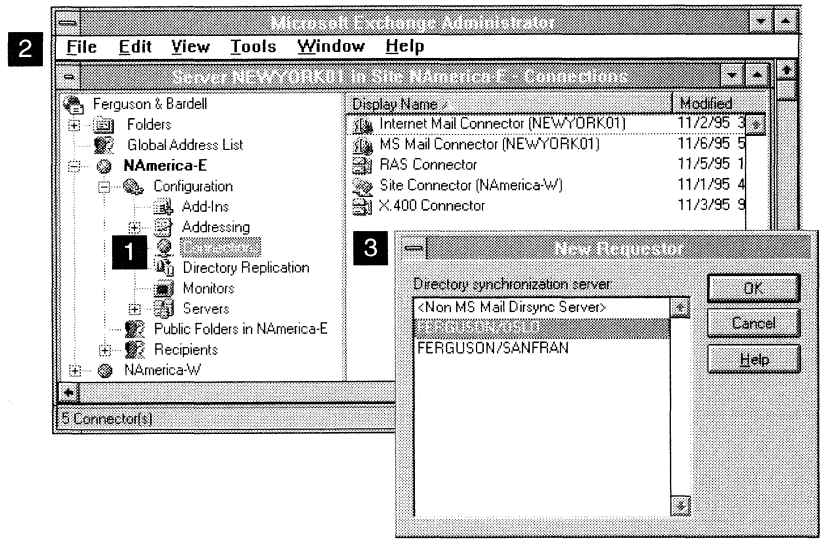
When you have completed the procedures in this section, you should start the directory synchronization process using the procedures in "Starting and Stopping Directory Synchronization" later in this chapter.

Creating the dirsync requestor

The minimum requirements for creating a dirsync requestor object include specifying a display name for the dirsync requestor object in the **General** property page and choosing a recipient import container in the **Import Container** property page.

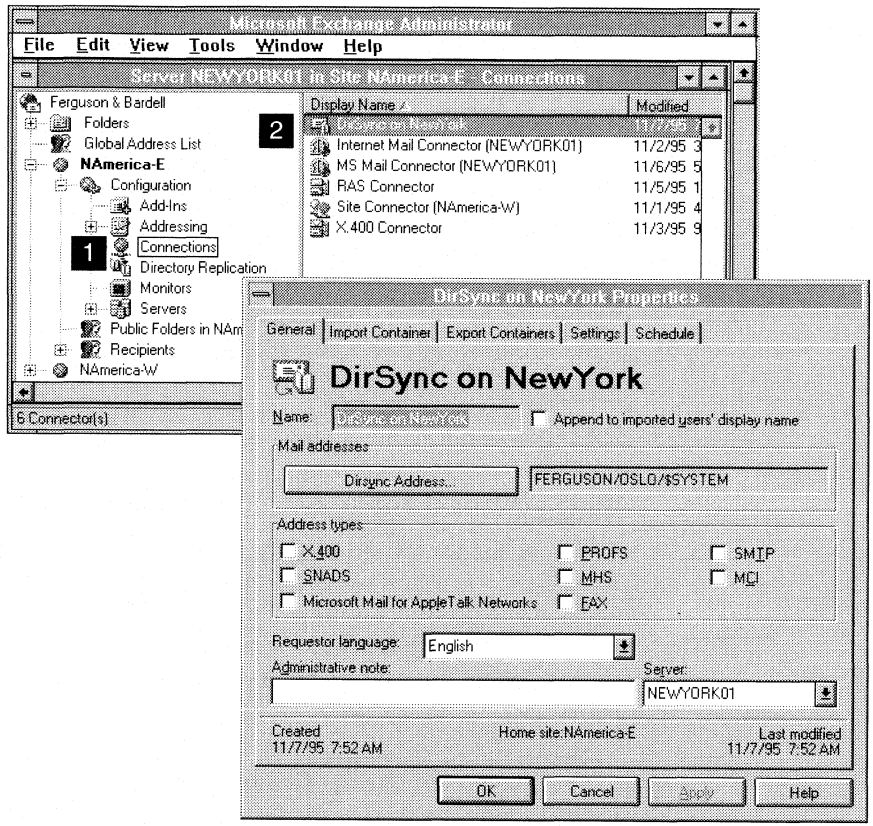
Create the import container before you create the requestor object.

1. In the Administrator window, choose **Connections**.
2. From the **File** menu, choose **New Other**, and then choose **Dirsync Requestor**.
3. Select the directory synchronization server from the list of MS Mail postoffices.



Getting to the Dirsync property pages

1. In the Administrator window, choose **Connections**.
2. Double-click the dirsync requestor.



General Dirsync Requestor Properties

Use the **General** property page to set the basic properties for a Microsoft Exchange Server dirsync requestor. When you configure a dirsync requestor for the first time, you must specify a display name to be viewed in the Microsoft Exchange Server Administrator program. You can also select the address types that you want to exchange during directory synchronization.

Note When a dirsync requestor object is being configured, it is given a unique display name (up to 64 characters). This name appears in the Connections container. For the remainder of this chapter, the dirsync requestor object will be referred to as dirsync requestor.

Getting to the General property page

1. In the Administrator window, choose **Connections**.
2. Double-click the dirsync requestor.
3. Select the **General** tab.

Setting General Requestor Properties

You can choose foreign address types that the dirsync requestor will request from the dirsync server. If you select a foreign address type, for example PROFS, you will receive all PROFS addresses that the dirsync server has processed in its master list. You should not select a foreign address type unless you have the access component for the foreign mail gateway installed on the Connector postoffice.

Note When you configure the **General** property page for a dirsync requestor, you must specify a dirsync server mailbox for sending and receiving system messages. By default, a hidden mailbox on the dirsync server is chosen. Generally, you should not specify a different mailbox to handle dirsync messages.

---

1. Select the **General** tab.
2. In the **Name** box, type a name for this requestor.
3. Select **Append to imported users' display name** if appropriate.
4. Under **Mail addresses**, accept the default dirsync address.
5. Specify any foreign address types required and a requestor language.

Option	Description
Name	Creates a unique name (up to 64 characters) for this requestor instance. This name appears in the Connections container.
Append to imported users' display name	An optional setting. If selected, puts the requestor name after each custom recipient that is created by the dirsync process.
Dirsync Address	The hidden recipient mailbox ($SYSTEM) on the MS Mail (PC) directory server is selected by default. Directory synchronization messages are sent to this mailbox. You should not change this address when setting up a Microsoft Exchange Server dirsync requestor.
Address types	MS Mail (PC) addresses are sent and received by default. Select other address types that this requestor will receive and request.
Requestor language	The primary language used in your MS Mail (PC) system. The default is English.
Server	The Microsoft Exchange Server in your site that will act as the dirsync requestor. The default is the server you are currently connected to in the Administrator program.

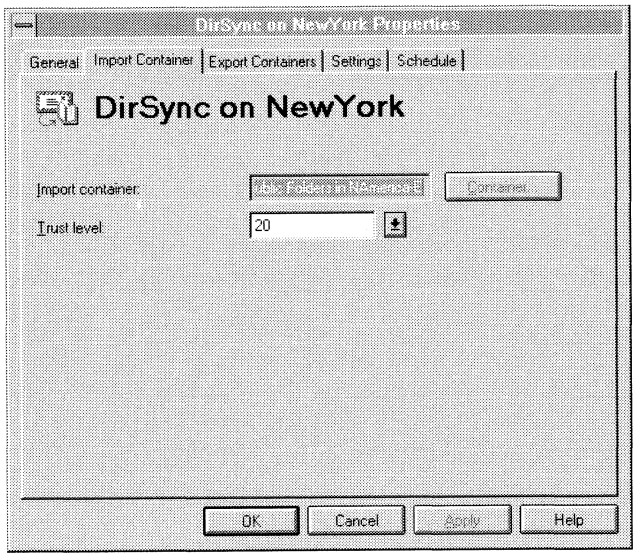
For information on installing gateway access components on the Connector postoffice, see Chapter 10, "Microsoft Mail for PC Networks."

Import Container Properties

You use import containers to store imported addresses sent from the MS Mail directory server to the Microsoft Exchange Server dirsync requestor.

Getting to the Import Container property page

1. In the Administrator window, choose **Connections**.
2. Double-click the dirsync requestor.
3. Select the **Import Container** tab.



For information on directory synchronization import containers, see *Microsoft Exchange Server Concepts and Planning*.

Selecting a Requestor Import Container

Use the **Import Container** property page to specify which recipient container receives imported address information. You can also assign a trust level to objects being imported.

You cannot select another directory import container after one has been specified. If you want to modify where imported directory information is placed, you must delete the existing requestor and configure a new one.

It is a good idea to create a container (separate from Recipients) to hold MS Mail addresses that have been synchronized. This can help prevent duplicate addresses from appearing in the MS Mail global address list.

If you want to make address information from more than one directory synchronization server available to Microsoft Exchange Server recipients, but you do not want to combine information between the directory synchronization servers, create a separate container for each group of imported recipients.

Note MS Mail and other messaging systems do not have directory objects or trust levels. When a recipient address is imported from a directory synchronization server, a recipient object is created in the container with the trust level specified in the **Import Container** property page. If you modify trust levels associated with a recipient object after it is added to the Microsoft Exchange Server directory, those modifications are overwritten during any subsequent directory synchronization import cycle that includes this recipient.

---

1. Select the **Import Container** tab.
2. Choose **Container**.
3. Select the container to place imported recipients in.
4. In the **Trust level** box, type a trust level.

Option	Description
Import container	The container on the Microsoft Exchange Server dirsync requestor where recipient listings are placed during dirsync.
Trust level	The trust level set for the import container. When recipient addresses are imported, a recipient object is created in the container with the trust level specified by this setting. The default is 20.

Export Container Properties

You use export containers to specify the Microsoft Exchange Server recipients that you want exported to the MS Mail directory server.

Getting to the Export Containers property page

1. In the Administrator window, choose **Connections**.
2. Double-click the dirsync requestor.
3. Select the **Export Containers** tab.

For information on directory synchronization export containers, see *Microsoft Exchange Server Concepts and Planning*.

Selecting Requestor Export Containers

Use the **Export Containers** property page to specify containers to use when exporting directory information. You can also assign a trust level for the connection so that only certain recipients are exported. By default, a Microsoft Exchange Server directory exchange requestor does not export any recipient containers.

1. Select the **Export Containers** tab.
2. Under **Site**, select a site to view available containers in that site.
3. Under **Recipient Containers**, select a recipient container, and then choose **Add**.
4. In the **Trust level** box, type a trust level.
5. Clear the **Export custom recipients** check box if you do not want to send information about Microsoft Exchange Server custom recipients.

Option	Description
Trust level	The trust level set for the connection. Only recipients with a trust level equal to or less than the trust level specified for the export container are exported during directory synchronization. The default is 100.
Export custom recipients	When selected, the custom recipients in the export container will be exported to the directory server. This option is selected by default.

Removing Export Containers

You can remove an export container used by the Microsoft Exchange Server dirsync requestor to stop the export of recipients in that container. When an export container is removed, directory information in transit is delivered. However, new update messages contain no information from the removed container. This will cause the remaining export containers to do a full export of recipient entries during the next directory synchronization cycle.

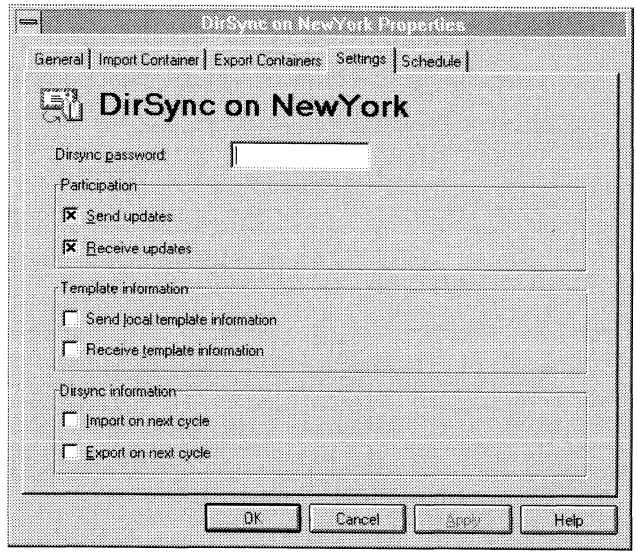
1. Select the **Export Containers** tab.
2. From **Export these recipients**, select the container you want to remove.
3. Choose **Remove**.

Settings Properties

Use the **Settings** property page to specify whether the Microsoft Exchange Server dirsync requestor will send address updates, receive address updates, or both from the MS Mail directory server. You can also specify whether to send and receive address template information during directory synchronization.

Getting to the Settings property page

1. In the Administrator window, choose **Connections**.
2. Double-click the dirsync requestor.
3. Select the **Settings** tab.



Configuring Dirsync Requestor Settings

Use the **Settings** property page to configure advanced directory synchronization functions.

Note If you are starting directory synchronization for the first time, all local directory information is automatically exported, and all available information from the directory synchronization server is automatically imported.

---

1. Select the **Settings** tab.
2. In the **Dirsync password** box, type a password for this directory requestor if required. This password must be the same as the password on the MS Mail dirsync server.
3. Under **Participation**, select or clear options.
4. Under **Template information**, select or clear options.
5. Under **Dirsync information**, select or clear options.

Option	Description
Dirsync password	A password for this directory requestor. Using a password for a dirsync requestor is optional. If used, you must also set the password on the dirsync server.
Send updates	If selected, allows this dirsync requestor to send address updates to the dirsync server.
Receive updates	If selected, allows this dirsync requestor to request address updates from the dirsync server.
Send local template information	If selected, you must configure template mappings in the directory synchronization object.
Receive template information	If selected, you must configure template mappings in the directory synchronization object.
Import on next cycle	Requests every address available on the directory synchronization server to be imported during the next directory synchronization cycle.
Export on next cycle	Sends every address available on the dirsync requestor during the next directory synchronization cycle.

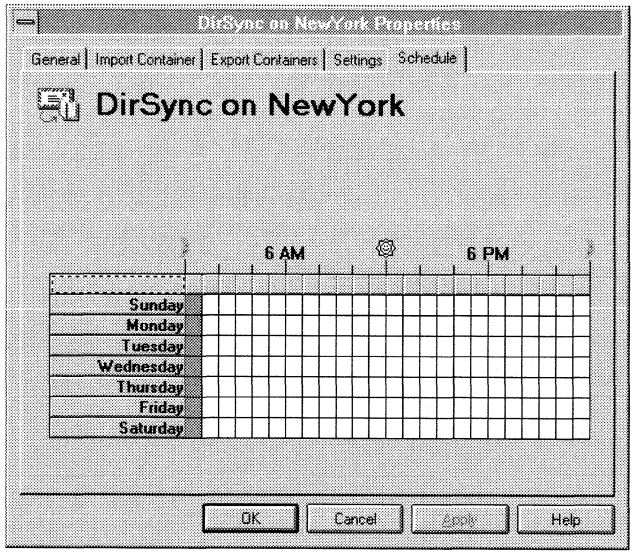
For more information on configuring template mappings on the Dirsync object, see "Directory Synchronization Configuration" later in this chapter.

Schedule Properties

You can configure the Microsoft Exchange Server dirsync requestor to send address updates to the MS Mail directory synchronization server. An MS Mail directory server processes directory updates a maximum of once a day. You should set the dirsync requestor schedule to coincide with your MS Mail directory server schedule. Updates should be received by the dirsync server prior to the scheduled process time for the server. You can check the schedule of the MS Mail directory server by checking the Administrator program on the MS Mail computer.

Getting to the Schedule property page

1. In the Administrator window, choose **Connections**.
2. Double-click the dirsync requestor.
3. Select the **Schedule** tab.



Setting the Requestor Schedule

Use the **Schedule** property page to set the time when update messages are sent to the MS Mail directory synchronization server. For administrators familiar with MS Mail dirsync, this is known as "T1" time. The default is to send an update message at midnight. Directory synchronization messages are sent at the beginning of the selected time.

Note Directory synchronization server updates are handled automatically as they are received by the dirsync requestor.

---

1. Select the **Schedule** tab.
2. In the schedule grid, select a time to send directory update messages to the directory synchronization server.

Configuring an MS Mail Directory Server

When you have finished configuring the Microsoft Exchange Server dirsync requestor, you must configure the MS Mail (PC) directory synchronization server to recognize the Microsoft Exchange Server as a requestor. You use the MS Mail (PC) Administrator program to register the Microsoft Exchange Server dirsync requestor with the MS Mail directory server.

When configuring an MS Mail (PC) directory synchronization server to recognize this Microsoft Exchange Server dirsync requestor, you must specify the Microsoft Mail Connector postoffice. These names can be viewed in the Microsoft Mail Connector **Local Postoffice** property page.

After the Microsoft Exchange Server dirsync requestor has been registered with the MS Mail directory server, you must start the directory synchronization services
on the Microsoft Exchange dirsync requestor computer.

For more information on configuring an MS Mail directory synchronization server, see your Microsoft Mail for PC Networks documentation.

Dirsync Server Installation

You can use a Microsoft Exchange Server as a dirsync server to update and distribute address information to remote dirsync requestors. Setting up a dirsync server includes the following:

- Create and configure a dirsync server for the local Microsoft Exchange Server site.
- Define remote directory synchronization requestor objects in the Microsoft Exchange Server directory that correspond to each requestor that will use this server.
- Configure a requestor on each system that will use this server.

When you have completed the tasks in this section, you should start the directory synchronization process using the procedures in "Starting and Stopping Directory Synchronization" later in this chapter.

Creating a dirsync server

The minimum requirement for creating a dirsync server object is specifying a display name in the **General** property page for the dirsync server object.

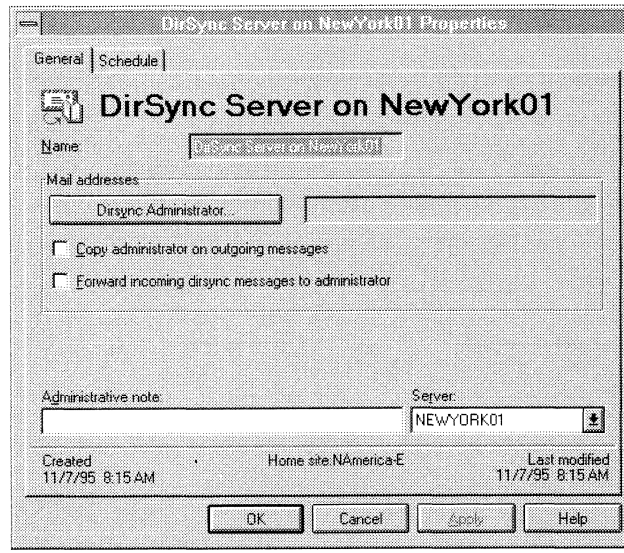
1. In the Administrator window, choose **Connections**.
2. From the **File** menu, choose **New Other**, and then choose **Dirsync Server**.

General Dirsync Server Properties

Use the **General** property page to set the basic properties for a Microsoft Exchange Server dirsync server. When you configure a dirsync server for the first time, you must specify a display name to be viewed in the Microsoft Exchange Server Administrator program. You can also specify a dirsync administrator mailbox to receive copies of incoming and outgoing dirsync system messages. These messages can be useful for troubleshooting directory synchronization processes.

Getting to the General property page

1. In the Administrator window, choose **Connections**.
2. Double-click the dirsync server.
3. Select the **General** tab.



Setting General Dirsync Server Properties

Use the **General** property page to configure fundamental parameters for the Microsoft Exchange Server dirsync server.

Note When a dirsync server object is being configured, it is given a unique display name (up to 64 characters). This name appears in the Connections container. For the remainder of this chapter, the dirsync server object will be referred to as dirsync server.

---

1. Select the **General** tab.
2. In the **Name** box, type a name for this directory synchronization server.
3. Choose **Dirsync Administrator**.
4. Select a mailbox, public folder, or distribution list for receiving directory synchronization messages.
5. Select **Copy administrator on outgoing messages** to receive each update message to each requestor.
6. Select **Forward Incoming Dirsync Messages to administrator** to view each update message from each requestor.
7. Under **Server**, select a Microsoft Exchange Server.

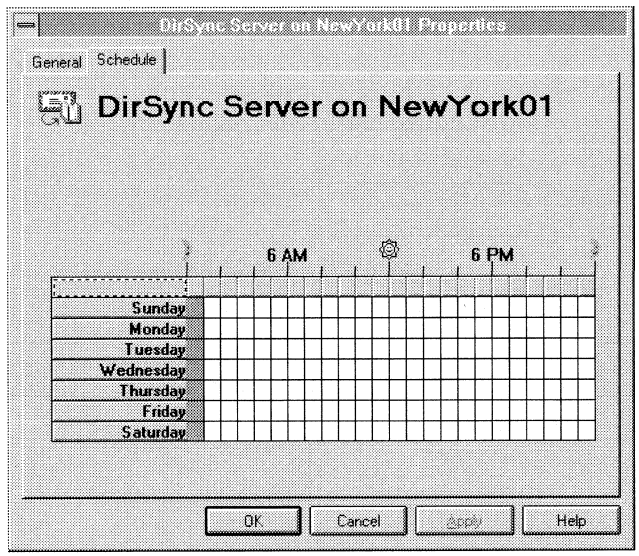
Option	Description
Name	The name (up to 64 characters) of the dirsync server.
Copy administrator on outgoing messages	This option is cleared by default and is typically used for troubleshooting.
Forward incoming dirsync messages to administrator	This option is cleared by default and is typically used for troubleshooting.
Server	The Microsoft Exchange Server in your site that will act as the dirsync server.

Schedule Properties

You can schedule the time when a Microsoft Exchange Server dirsync server sends master address list updates to remote dirsync requestors. You should schedule your remote dirsync requestors to send local address list updates prior to your dirsync server's scheduled process time.

Getting to the Schedule property page

1. In the Administrator window, choose **Connections**.
2. Double-click the dirsync server.
3. Select the **Schedule** tab.



Setting the Directory Exchange Server Schedule

Use the **Schedule** property page to specify when directory synchronization messages are sent from the server to each requestor. If you are familiar with MS Mail Dirsync, this is known as "T3" time. The default is to send one update message each day at midnight. Directory synchronization messages are sent at the beginning of each hour selected in the schedule grid. Requestor messages to the server are processed when they are received.

1. Select the **Schedule** tab.
2. In the schedule grid, select a time to send directory update messages to the directory requestors.

Remote Dirsync Requestor Installation

Each requestor to a Microsoft Exchange Server dirsync server must be defined in the Microsoft Exchange Server directory as a remote dirsync requestor. You must complete the following tasks to set up a remote dirsync requestor:

- Define a remote directory exchange requestor object in the Microsoft Exchange Server directory.
- Specify which directory containers to use when importing and exporting address information from the remote dirsync requestor.

When you have completed the procedures in this section, you should verify that each remote MS Mail directory requestor is set up as a requestor to the dirsync server configured earlier in the chapter.

For more information on setting up MS Mail directory requestors, see your Microsoft Mail for PC Networks documentation.

Creating a remote dirsync requestor

The minimum requirements for creating a remote dirsync requestor object include specifying a display name for the remote dirsync requestor object in the **General** property page, and choosing a recipient import container in the **Import Container** property page.

Note The **Remote Dirsync Requestor** command is unavailable until you set up a Microsoft Exchange Server dirsync server as described in "Dirsync Server Installation" earlier in this chapter.

---

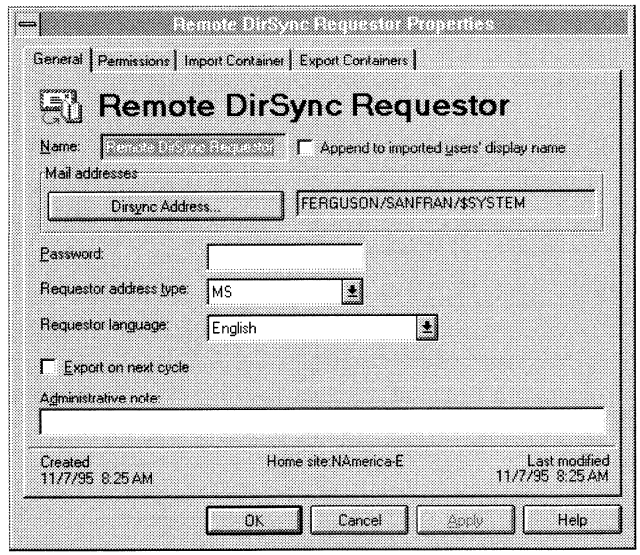
1. In the Administrator window, choose **Connections**.
2. Select the dirsync server.
3. From the **File** menu, choose **New Other**, and then choose **Remote Dirsync Requestor**.
4. Select a requestor from the list of MS Mail postoffices.

General Remote Dirsync Requestor Properties

Use the **General** property page to set the primary properties for a Microsoft Exchange Server remote dirsync requestor. When you configure a remote dirsync requestor for the first time, you must specify a display name to be viewed from the Microsoft Exchange Server Administrator program. You can also specify the requestor password if required.

Getting to the General property page

1. In the Administrator window, choose **Connections**.
2. Double-click the remote dirsync requestor.
3. Select the **General** tab.



Setting General Remote Dirsync Requestor Properties

You can specify the address type for a remote dirsync requestor in the **General** property page. If the remote dirsync requestor is an MS Mail (PC) postoffice, the address type is MS. If the remote dirsync requestor is an MS Mail (AppleTalk) server, the address type is MSA. When you configure the **General** property page for a remote dirsync requestor, you must specify a mailbox for sending and receiving system messages. By default, a hidden mailbox is chosen. Generally, you should not specify a different mailbox for handling dirsync messages.

Note When a remote dirsync requestor object is being configured, it is given a unique display name (up to 64 characters). This name appears in the dirsync server container.

---

1. Select the **General** tab.
2. In the **Name** box, type a display name for the remote requestor postoffice.
3. Select **Append to imported users' display name**.
4. Under **Mail Addresses**, accept the default dirsync address.
5. In the **Password** box, type the password used by the remote requestor if required.
6. In the Requestor address type box, select MS.
7. In the **Requestor language** box, select the language used by the remote dirsync requestor.
8. Select **Export on next cycle**.

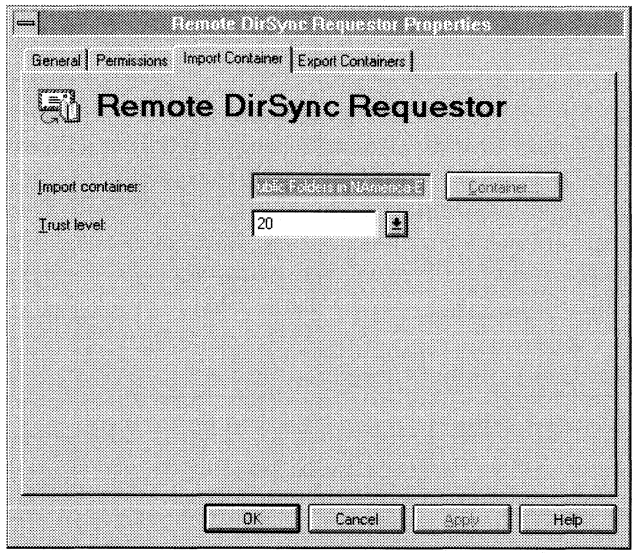
Option	Description
Name	The display name (up to 64 characters) for this remote dirsync requestor. A requestor name is specified when creating the remote requestor. You cannot rename an existing remote dirsync requestor. You must delete the object and re-create a new object.
Append to imported users' display name	An optional setting. If selected, puts the requestor name after each custom recipient that is created by the directory synchronization process for this remote dirsync requestor.
Dirsync Address	The hidden recipient mailbox ($SYSTEM) on the MS Mail (PC) directory requestor is selected by default. Directory synchronization messages are sent to this mailbox. Do not change this address when setting up a remote dirsync requestor.
Password	A password for this remote directory requestor. If used, it must match the password set for the MS Mail requestor. By default, no password is used.
Requestor address type	MS is used by MS Mail (PC) and all foreign directory exchange requestors. Select MSA to send directory synchronization messages in MS Mail (AppleTalk) format. The default address type is MS.
Export on next cycle	Select to send all address information to the remote requestor during the next directory synchronization cycle.

Import Container Properties

You use import containers to store imported addresses sent from the MS Mail remote directory requestor to the Microsoft Exchange Server dirsync server.

Getting to the Import Container property page

1. In the Administrator window, choose **Connections**.
2. Double-click the remote dirsync requestor.
3. Select the **Import Container** tab.



For information on directory synchronization import containers, see *Microsoft Exchange Server Concepts and Planning*.

Selecting a Remote Dirsync Requestor Import Container

Use the **Import Container** property page to specify which recipient container receives imported address information. You can also assign trust levels to objects being imported.

You cannot choose another directory import container once one has been specified. If you want to modify where imported directory information is placed, you must delete the existing requestor and configure a new one.

If you want to make address information from more than one directory synchronization server available to Microsoft Exchange Server recipients, but you do not want to combine information between the directory synchronization servers, create a separate container for each group of imported recipients.

Note MS Mail and other messaging systems do not have directory objects or trust levels. When a recipient address is imported from a directory synchronization server, a recipient object is created in the container with the trust level you specify in the **Import Container** property page. If you modify trust levels associated with a recipient object after it is added to the Microsoft Exchange Server directory, those modifications are overwritten during any subsequent directory synchronization import cycle that includes this recipient.

---

1. Select the **Import Container** tab.
2. Choose **Container**.
3. Select a container for placing imported address listings.
4. In the **Trust level** box, type a trust level.

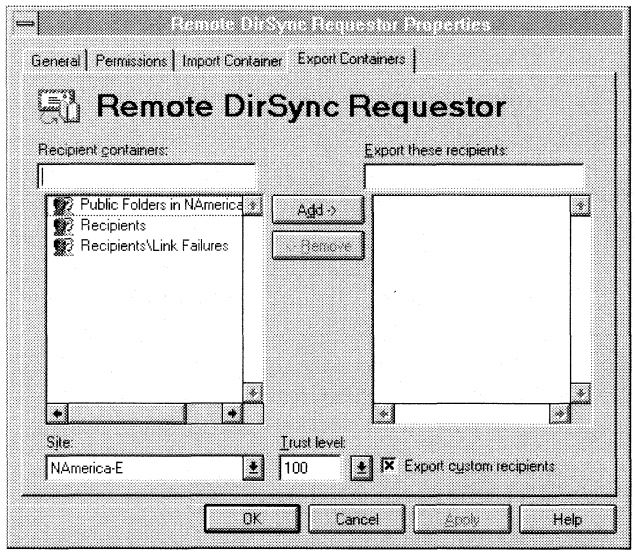
Option	Description
Import container	The container where recipient listings are placed during directory synchronization. You specify an import container the first time the remote dirsync requestor is created. Once chosen, you cannot select another container for import. To choose another container for import, you must delete the remote dirsync object and re-create it.
Trust level	The trust level set for the import container. When recipient addresses are imported, a recipient object is created in the container with the trust level specified by the import container. The default is 20.

Export Container Properties

You use export containers to specify the Microsoft Exchange Server recipients that you want exported to the MS Mail remote directory requestor.

Getting to the Export Containers property page

1. In the Administrator window, choose **Connections**.
2. Double-click the remote dirsync requestor.
3. Select the **Export Containers** tab.



For information on directory synchronization export containers, see *Microsoft Exchange Server Concepts and Planning*.

Selecting Remote Dirsync Requestor Export Containers

Use the **Export Containers** property page to specify containers to use when exporting directory information. You can also assign a single trust level for the connection so that only recipients with a trust level less than or equal to the specified trust level will be exported. By default, a Microsoft Exchange Server directory exchange requestor does not export any recipient containers.

1. Select the **Export Containers** tab.
2. Under **Site**, select a site to view available containers in that site.
3. Under **Recipient containers**, select a recipient container, and then choose **Add**.
4. Under **Trust level**, type a trust level.
5. Clear **Export custom recipients** if you do not want to send information about Microsoft Exchange Server custom recipients.

Option	Description
Trust level	The trust level set for the connection. Only recipients with a trust level equal to or lower than the trust level specified for the connection are exported during directory synchronization. The default is 100.
Export custom recipients	When selected, the custom recipients in the export container will be exported to the directory server. This option is selected by default.

Removing Export Containers

You can remove an export container used by the remote dirsync requestor to stop the export of recipients in that container. When an export container is removed, directory information in transit is delivered. However, new update messages contain no information from the removed container. This will cause the remaining export containers to do a full export of recipient entries during the next directory synchronization cycle.

1. Select the **Export Containers** tab.
2. Under **Export these recipients**, select the container you want to remove.
3. Choose **Remove**.

Permissions Properties

You can assign permissions for the remote dirsync requestor object. Any user who has permissions assigned for the configuration container will inherit those permissions for the remote dirsync requestor object. You may want to assign explicit permissions to a user, such as a directory synchronization administrator, for the dirsync requestor object.

For example, you could assign Administrator permissions for a remote dirsync requestor object to a user but not assign User permissions for the configuration container. The user will have permissions to the remote dirsync requestor only.

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

Remote Directory Requestor Configuration

After you have defined Microsoft Exchange Server remote dirsync requestor objects on the dirsync server, you must then configure the respective MS Mail directory synchronization requestor computers. These requestor computers can be MS Mail (PC), MS Mail (AppleTalk), or any foreign system that supports the MS Mail (PC) 3.*x* directory synchronization protocol.

MS Mail 3.*x* Directory Synchronization Requestor Setup

You can configure an MS Mail (PC) postoffice to be a directory synchronization requestor to a Microsoft Exchange Server dirsync server. You follow the same process for setting up a directory synchronization requestor as you would to an MS Mail directory synchronization server. The directory synchronization requestor is an integral part of MS Mail 3.*x* and can be configured using the MS Mail Administrator program.

For information on how to configure and start an MS Mail directory exchange requestor, see your Microsoft Mail for PC Networks documentation.

Before configuring the directory exchange requestor, you should verify the following:

- Microsoft Exchange Server processes are started and working correctly.
- Both the Microsoft Mail Connector and the dirsync server are correctly installed on the Microsoft Exchange Server computer.
- Messages can be exchanged between the two systems.

- The MS Mail External or Multitasking MTA program is correctly installed and running if the MS Mail (PC) postoffice and Microsoft Exchange Server are not on the same LAN.
- The Dispatch program is installed and running on every LAN that has an MS Mail directory requestor postoffice.

For information on configuring the Microsoft Mail Connector, see Chapter 10, "Microsoft Mail for PC Networks."

MS Mail (AppleTalk) Directory Exchange Requestor Setup

The directory exchange requestor program for MS Mail (AppleTalk) is installed with the Microsoft Exchange Connection. The requestor sends and receives address updates to and from the Microsoft Exchange Server using system messages delivered through the Microsoft Mail Connector.

You configure the following settings on the directory exchange requestor:

- Directory exchange requestor scheduling for sending and receiving address updates.
- Network name, postoffice name, and password for the Microsoft Exchange Server dirsync server.
- The MS Mail (AppleTalk) network manager name and password.

Before configuring the directory exchange requestor, you should verify the following:

- The Microsoft Mail Connector is correctly installed on the Microsoft Exchange dirsync server computer.
- The Microsoft Exchange Connection gateway software is installed on the MS Mail (AppleTalk) server.
- A remote dirsync requestor object has been defined in the Microsoft Exchange Server directory, and is configured to send messages in MSA (MS Mail for AppleTalk Networks) format.

Directory Exchange Requestor

The Directory Exchange Requestor program included on the Microsoft Exchange Connection floppy disk provides address information transfer between MS Mail (AppleTalk) and Microsoft Exchange Server. To transmit address information, the directory exchange requestor must:

- Be configured on the MS Mail (AppleTalk) server that has the Microsoft Exchange Connection installed.
- Receive update messages from Microsoft Exchange Server dirsync server in MSA format.

Note If this requestor does not receive update messages in MSA format, duplicate entries are created in the MS Mail (AppleTalk) address list. You set the message type on Microsoft Exchange Server in the remote directory exchange requestor object that corresponds to this requestor.

When you first configure and start the directory exchange requestor, it exports a complete list of local addresses to the Microsoft Exchange Server dirsync server and issues a request for all entries in the dirsync server address list. The server returns a confirmation that the local addresses were incorporated and a list of all recipients in the export containers for the requestor.

After the first time the requestor is started, the requestor sends and receives only updates to the local and global address lists. If an error should occur, you can correct this by manually importing or exporting the required information as described in "Importing Address Changes Manually" and "Exporting Address Changes Manually" later in this chapter.

Caution Directory update messages are sent from Microsoft Exchange Server to the MS Mail (AppleTalk) network manager. These messages are picked up by the Microsoft Exchange Connection Directory Exchange Requestor program and should not be deleted, moved, or modified. Doing so will interrupt the directory synchronization process and may cause loss of data. Large imports from the directory exchange server will take a number of hours to complete. During this time, messages will not be transferred through the gateway.

You can establish the following requestor parameters for the Microsoft Exchange Connection Directory Exchange Requestor program on the MS Mail (AppleTalk) server:

- General application settings
- Which gateway to use
- Which address types to request

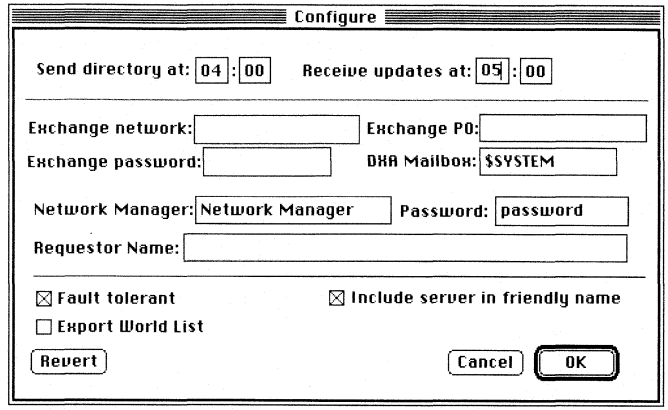
If you start the directory exchange requestor program without logging on as network manager, all configuration and administrative functions are unavailable. However, the program will process directory synchronization messages.

Configuring Requestor Settings

Use the Microsoft Exchange Connection Directory Exchange Requestor program to specify which Microsoft Exchange Server will receive the dirsync messages. You can also specify when to send address updates to the dirsync server and when to process global updates received from the dirsync server.

1. Open the MS Exchange Connection folder.
2. Open the DER folder.
3. Double-click **Exchange Connection DER**.
4. If this is the first time the requestor has been started, type the password for network manager.

5. From the **Configure** menu, choose **Application**.



6. Type the values for sending and receiving updates.
7. Type the network name, postoffice name, and password, if required, for the Microsoft Exchange Server dirsync server.
8. In the **DXA Mailbox** box, the $System mailbox, which is a hidden mailbox, will be displayed by default.

   In a typical configuration, this setting should not be changed.
9. Specify the network manager mailbox, password, and the remote requestor name.
10. Specify options for fault tolerance, exporting the world list, and server name inclusion with the friendly name.

Option	Description
Send directory at	The time in 24-hour format (*hh:mm*) to send directory updates to the Microsoft Exchange Server dirsync server. The default is 04:00 (4:00 A.M.).
Receive updates at	The time in 24-hour format (*hh:mm*) the directory exchange requestor will scan the Network Manager inbox for directory updates from the Microsoft Exchange Server dirsync server. The default is 05:00 (5:00 A.M.).
Exchange network	The network name of the Microsoft Mail Connector. Found in the Connector **Local Postoffice** property page.
Exchange PO	The postoffice name of the Microsoft Mail Connector. Found in the Connector **Local Postoffice** property page.

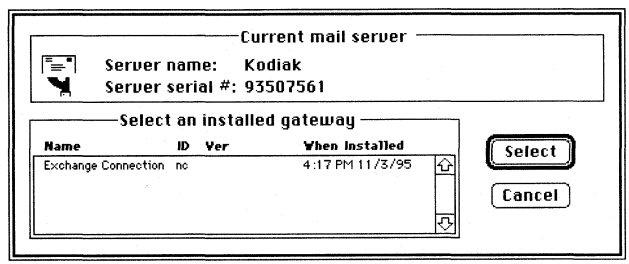
(continued)

Option	Description
Exchange password	This setting is optional and blank by default. If used, it must match the password set in the **General** property page of the Microsoft Exchange Server remote directory exchange requestor object that corresponds with this requestor.
DXA Mailbox	The Microsoft Exchange Server mailbox to which the requestor sends update messages. The default is $SYSTEM.
Network Manager	The mailbox name for the network manager's account. The default account is Network Manager.
Requestor Name	The name of the remote directory exchange requestor object in the Microsoft Exchange Server directory that corresponds with this requestor.
Fault tolerant	Tracks which address updates have been processed using synchronization numbers. These numbers are used to recover a failed synchronization without manual directory import and export. This option is selected by default.
Include server in friendly name	Send all MS Mail (AppleTalk) user addresses in *friendlyname@servername* format. This option is selected by default.
Export World List	If selected, addresses and updates will be sent to the dirsync server. This option is cleared by default.

Selecting a Gateway

You can select which installed gateway you want to use to communicate with Microsoft Exchange Server. If you are configuring this requestor for the first time, the **Current Mail Server** dialog box will appear after completing the tasks in the previous section. Otherwise, start the Microsoft Exchange Connection Directory Exchange Requestor. Use the procedure in the following section to configure gateway and server settings.

1. From the **Configure** menu, choose **Select Gateway**.



2. In the **Select an installed gateway** box, select the gateway to use when communicating with the Microsoft Exchange Server dirsync server.
3. Choose **Select**.

   If you are configuring this requestor for the first time, the **Address Filter** dialog box appears, and you can specify filter settings.

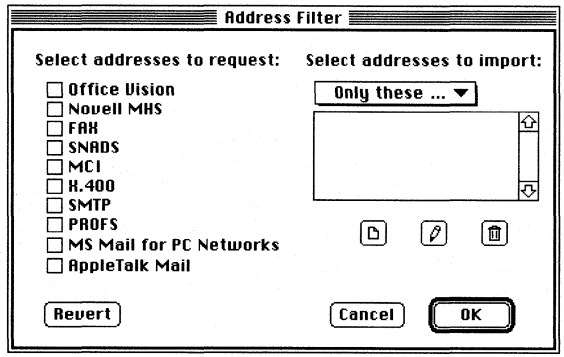
Setting Address Filters

You can choose the address types you want to receive from Microsoft Exchange Server. These address types correspond to foreign mail systems accessed using an X.400 Connector, the Internet Mail Service, or an MS Mail gateway.

Note Foreign mail addresses are processed in MS Mail (PC) proxy format (NETWORK/POSTOFFICE/USERID) when an address type is not requested for the foreign mail type. For example, not selecting a PROFS address type will convert a PROFS address to MS Mail (PC) proxy format.

---

1. From the **Configure menu**, choose **Address Filtering**.



2. Select each address type you want to request from the directory synchronization server.

3. Under **Select addresses to import**, select an option.

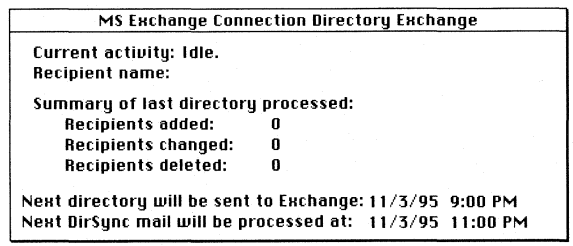
Option	Description
Select addresses to request	The format for addresses you would like to request from the dirsync server.
Select addresses to import	Import parameters for remote postoffices.
Only these postoffices	Imports addresses from the postoffices you specify.
Omit these postoffices	Does not request addresses from the postoffices you specify.
Revert	Rolls back all address filter changes to the recently saved configuration.

Starting the Directory Exchange Requestor

The Microsoft Exchange Connection must be installed and the directory exchange requestor must be started for address information to be transferred between an MS Mail (AppleTalk) requestor and a Microsoft Exchange Server dirsync server. The requestor is updated periodically as address information is processed. After each directory synchronization cycle is completed, a confirmation or error message is sent to the network manager. If you want to stop the requestor, you should verify that there are no updates currently being processed.

Note If the requestor is supplied with the network manager name and password, or if you are currently logged in as network manager, it automatically logs on and runs in the background without locking the desktop. If you start the requestor without providing the network manager name and password and are not currently logged on as network manager, the desktop is locked while the requestor runs as a foreground application.

1. Open the folder that contains the Microsoft Exchange Connection files.
2. Double-click **Exchange Connection DER**.



Making the Directory Exchange Requestor a Startup Item

You can add an alias for the requestor to your Startup Items folder on the MS Mail (AppleTalk) requestor to ensure that the requestor starts when the server is started.

1. Select the **Microsoft Exchange DER**.
2. From the **File** menu, choose **Make Alias**.
3. Move the alias to the Startup Items folder in the System folder.

Viewing Directory Synchronization Updates

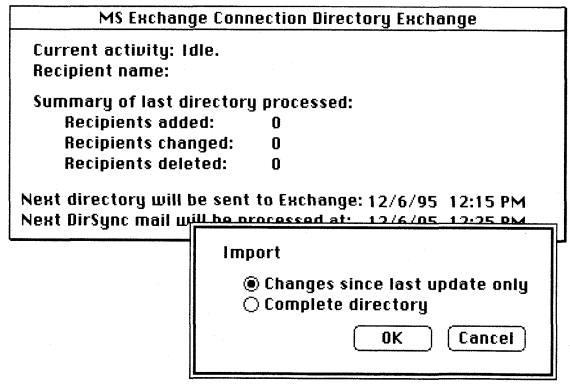
You can view gateway recipient information to verify that address updates are being correctly imported. You must be logged on as a network manager to view gateway recipient information.

1. Start MS Mail (AppleTalk).
2. From the **Mail** menu, choose **Gateway Recipients**.

Importing Address Changes Manually

Address information updates are automatically exchanged according to the schedule you specify for the directory exchange requestor. In addition, you can manually request all address changes since the last time the directory was updated, or the complete list of known addresses. When the import reply is received and processed, a confirmation message is sent to the network manager with the status of the import request.

1. Open the folder that contains the Microsoft Exchange Connection files.
2. Double-click **Exchange Connection DER**.
3. From the **File** menu, choose **Import Directory**.



Option	Description
Changes since last update only	Request only addresses that have changed since the last exchange of address updates.
Complete directory	Request all available address information from Microsoft Exchange Server dirsync server.

Exporting Address Changes Manually

Address information updates are automatically sent according to the schedule you specify in the requestor. In addition, you can manually export all address changes since the last time the directory was updated or the complete list of known addresses. When the export is received and processed by Microsoft Exchange Server dirsync server, a confirmation message is sent to the network manager with export status information.

Note Directory export is unavailable if the **Export World List** check box is not selected in the **Gateway Configuration** dialog box.

1. Open the folder that contains the Microsoft Exchange Connection files.
2. Double-click **Exchange Connection DER**.
3. From the **File** menu, choose **Export Directory**.

Option	Description
Changes since last update only	Export only addresses that have changed since the last exchange of address updates.
Complete directory	Export all available address information from the remote dirsync requestor.

Exporting a World List to a Text File Manually

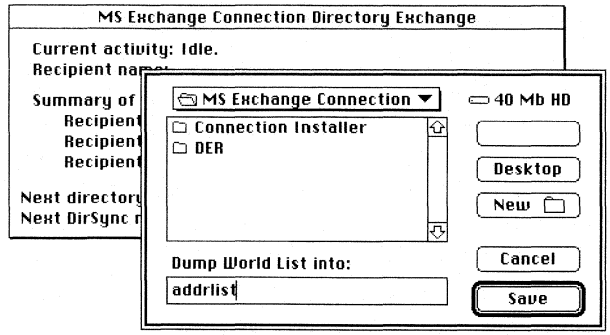
You can also export the MS Mail (AppleTalk) world list to a text file in the format required by the MS Mail (PC) import utility. This file can then be used to manually import addresses into an MS Mail (PC) postoffice.

When the file is saved, you can view it using Microsoft Word or another word processor to verify that the addresses were saved correctly. The file consists of a replace transaction followed by an add transaction for each address. The format of each add transaction is:

A *30_character_alias* **MSMAIL:***address*

Note MSMAIL indicates the address type. To import this list to an MS Mail (PC) postoffice, it must have the Microsoft Mail Connection gateway access component installed.

1. Open the folder that contains the Microsoft Exchange Connection files.
2. Double-click Exchange Connection DER.
3. From the **File** menu, choose **Save To File**.



4. Select a folder to place the world list in.
5. Under **Dump World List into**, type a name for the address file.

For more information about the format of address transaction files and the Import utility, see your Microsoft Mail documentation.

Removing MS Mail (AppleTalk) Addresses

You can remove all MS Mail (AppleTalk) recipients from the Microsoft Exchange Server global address list. This is useful when you no longer want to exchange mail with an MS Mail (AppleTalk) server. When you remove MS Mail (AppleTalk) recipients from your global address list, the change is reflected in your messaging topology.

Important This removes addresses from all address lists, aliases, and personal address books. Once addresses have been removed, you must import them to restore entries to the directory. The next directory synchronization cycle will replace only address information about recipients that has been changed in the global address list.

---

1. Open the folder that contains the Microsoft Exchange Connection files.
2. Double-click **Exchange Connection DER**.
3. From the **File** menu, choose **Remove Mac Names From Exchange**.
4. When you receive a confirmation message, choose **OK**.

Removing Microsoft Exchange Server Addresses

You can remove all Microsoft Exchange Server recipients and gateway recipients from the MS Mail (AppleTalk) world list. This is useful when you no longer want to exchange mail with a Microsoft Exchange Server.

Important This removes addresses from all address lists, aliases, and personal address books. Once addresses have been removed, you must import them to restore entries to the directory. The next directory synchronization cycle will replace only address information about recipients that has been changed in the exported containers.

---

1. Open the folder that contains the Microsoft Exchange Connection files.
2. Double-click **Exchange Connection DER**.
3. From the **File** menu, choose **Remove Exchange Names From Mac**.
4. When you receive a confirmation message, choose **OK**.

Resynchronizing Address Information

In a successful directory synchronization cycle, confirmation messages are sent to the network manager indicating that the directory synchronization server has accepted and incorporated the changes. If you believe directory synchronization has not been completed correctly or is out of synchronization, you can attempt to resynchronize the cycle. This process includes an import of the current global address list.

The global address list is requested, and the send-receive cycle is reset. If you receive a message stating that the directory synchronization cycle is out of phase, you should import the global address list from Microsoft Exchange Server and export the MS Mail (AppleTalk) world list to Microsoft Exchange Server.

Note All requestor activities are recorded in the directory exchange requestor log, located in the Preferences folder in the System folder. You can use TeachText or another text editor to view the file.

The directory exchange requestor log is continually updated and should be cleared periodically. You should verify that the directory synchronization process is functioning correctly before deleting this log file.

---

1. Open the folder that contains the Microsoft Exchange Connection files.
2. Double-click **Exchange Connection DER**.
3. From the **File** menu, choose **Resync Cycle**.

Foreign Directory Exchange Requestors

You can set up directory synchronization with any messaging system that can export and import address information using the MS Mail 3.*x* directory synchronization protocol.

For information on the MS Mail 3.*x* directory synchronization protocol and developing a requestor for a foreign system, see the *Directory Synchronization with Foreign Mail Systems Guide*.

Before configuring a directory exchange requestor on a foreign system, you should verify the following:

- Microsoft Exchange Server processes are started and working correctly.
- Both the gateway to the foreign system and the directory synchronization server are correctly installed and running on the Microsoft Exchange Server.
- The gateway to the Microsoft Exchange Server (if required) is correctly installed and running on the foreign system.
- Messages can be sent between recipients on the two systems by manually entering the recipient's address.

Directory Synchronization Configuration

When you configure a directory synchronization server or requestor in a Microsoft Exchange Server site, a separate server is selected to run each synchronization process. By default, the server selected is the one you are currently connected to in the Administrator window. The directory synchronization object on that server imports and exports information during directory synchronization. The default settings for the directory synchronization object are designed to allow both server and requestor functions to be performed without making any changes. However, you can modify the directory synchronization object configuration.

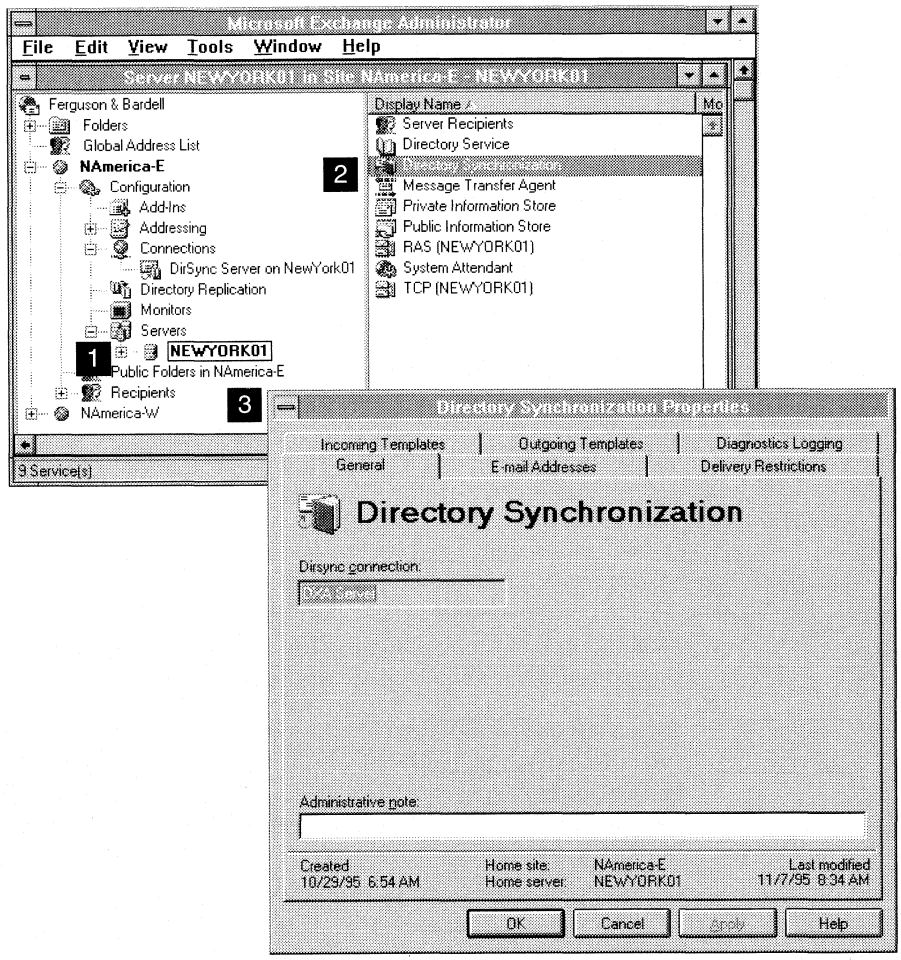
MS Mail uses templates to record extended information about recipients. If you want to exchange MS Mail template information along with other recipient information during directory synchronization, you can map this information to recipient attributes in the Microsoft Exchange Server directory.

General Properties

Use the **General** property page to view basic properties for the selected directory synchronization object.

Getting to the General property page

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



E-mail Addresses for Directory Synchronization

Use the **E-mail Addresses** property page to create, modify, or remove e-mail addresses. Microsoft Exchange Server automatically generates the following e-mail address types for the directory synchronization object:

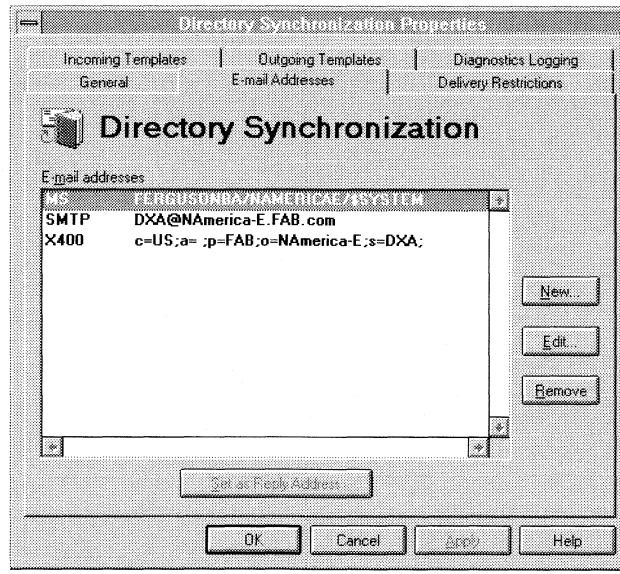
- MS Mail (PC)
- X.400
- Internet

You can modify these addresses, create new addresses, or create custom addresses.

Caution Many other Microsoft Exchange Server services use these default addresses. Changing or removing the default addresses can cause directory synchronization to fail.

Getting to the E-mail Addresses property page

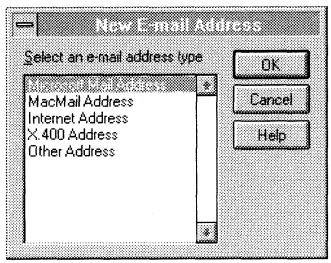
1. In the Administrator window, choose **Servers**, and then choose the server you want to configure.
2. Double-click **Directory Synchronization**.
3. Select the **E-mail Addresses** tab.



Creating Directory Synchronization E-mail Addresses

Use the **E-mail Addresses** property page to create new e-mail addresses for the directory synchronization object to send and receive directory synchronization system messages.

1. Select the **E-mail Addresses** tab.
2. Choose **New**.



3. Select an e-mail address type.

For information on configuring other address types, see Chapter 4, "Address Spaces."

Modifying Directory Synchronization E-Mail Addresses

Use the **E-mail Addresses** property page to modify e-mail addresses that the directory synchronization object uses to send and receive directory synchronization system messages.

Caution Changing default addresses can cause directory synchronization to fail.

1. Select the **E-mail Addresses** tab.
2. Choose **Edit**.

Removing Directory Synchronization E-mail Addresses

You can use the **E-mail Addresses** property page to remove e-mail addresses that the directory synchronization object uses to send and receive directory synchronization system messages.

Caution Changing default addresses can cause directory synchronization to fail.

1. Select the **E-mail Addresses** tab.
2. Choose **Remove**.

Delivery Restrictions

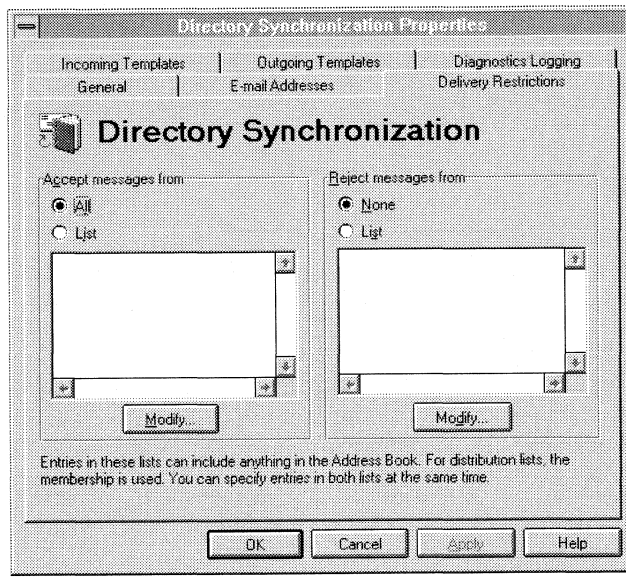
Use the **Delivery Restrictions** property page to specify addresses from which the Microsoft Exchange Server dirsync server will or will not accept messages. All rejected messages are returned to the original sender.

Use the dirsync administrator's mailbox to view the system messages delivered to the dirsync server. From the dirsync administrator's mailbox, you can determine if unwanted messages are being sent to the dirsync server. Typically, you do not need to specify individual recipients for message reception or rejection.

For information on specifying the dirsync administrator's mailbox, see "Setting General Dirsync Server Properties" earlier in this chapter.

Getting to the Delivery Restrictions property page

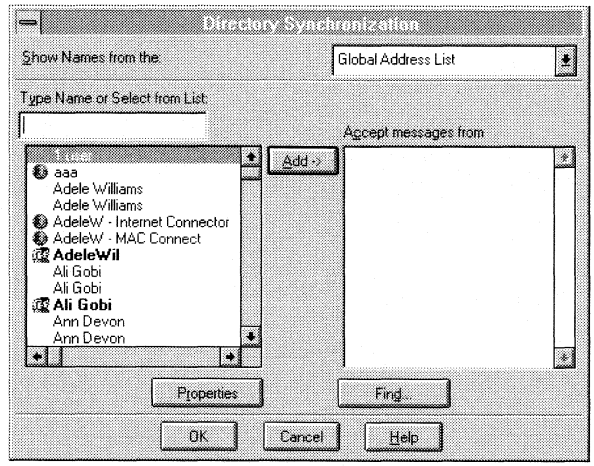
1. In the Administrator window, choose **Servers**, and then choose the server you want to configure.
2. Double-click **Directory Synchronization**.
3. Select the **Delivery Restrictions** tab.



Setting Restrictions for Message Reception

You can specify whether the dirsync server will accept messages from every recipient in the Address Book or only the recipients you have selected. You can prevent messages unrelated to directory synchronization from being delivered to the dirsync server by selecting recipient names from the Address Book.

1. Select the **Delivery Restrictions** tab.
2. Under **Accept messages from**, select **List**.
3. Choose **Modify**.

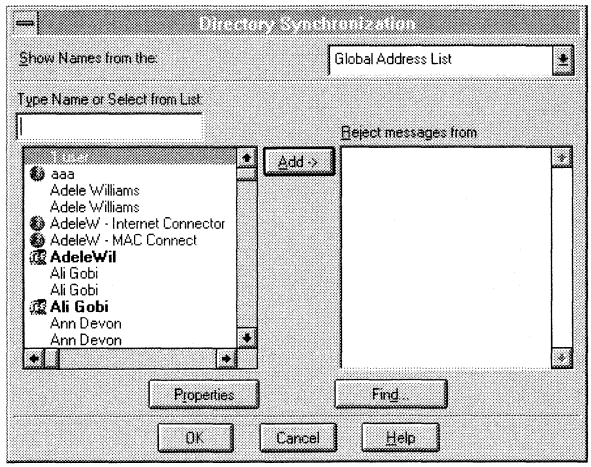


Option	Description
Show Names from the	Select the global address list or a container.
Type Name or Select from List	Type or select one or more names.

Setting Restrictions for Message Rejection

You can specify whether the dirsync server will reject messages from all recipients in the Address Book or reject messages from recipients you have selected. You can prevent messages unrelated to directory synchronization from being delivered to the dirsync server by selecting recipient names from the Address Book.

1. Select the Delivery Restrictions tab.
2. Under **Reject messages from**, select **List**.
3. Choose **Modify**.



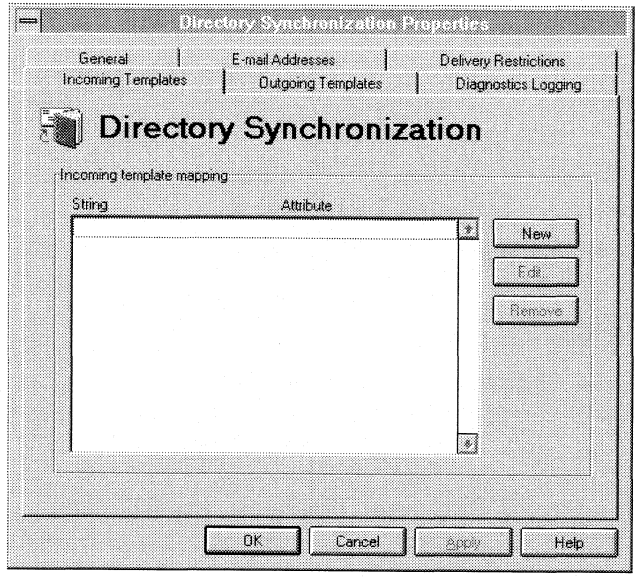
Incoming Template

You can map incoming template information to Microsoft Exchange Server directory recipient attributes. For example, you can map MS Mail phone, telephone, and extension templates to the recipient office phone attribute so that information stored differently on other systems is displayed consistently in the Microsoft Exchange Server directory.

Note When typing incoming string information, all template strings must match the template information specified in the MS Mail Administrator program. For example, if the Template information is **Employee Number:**, the exact string must be entered.

Getting to the Incoming Templates property page

1. In the Administrator window, choose **Servers**, and then choose the server you want to configure.
2. Double-click Directory Synchronization.
3. Select the **Incoming Templates** tab.



Configuring Incoming Template Mappings

Use the **Incoming Templates** property page to map MS Mail user information strings to the Microsoft Exchange Server attributes during directory synchronization.

1. Select the **Incoming Templates** tab.
2. To specify a new MS Mail template to Microsoft Exchange Server attribute mapping, choose **New**.

Option	Description
Map the string	The template identifier string used by MS Mail.
To the attribute	The recipient attribute in which you want to store the incoming information.

Modifying Incoming Template Mappings

Use the **Incoming Templates** property page to modify incoming MS Mail template information mapped to a Microsoft Exchange Server attribute.

1. Select the **Incoming Templates** tab.
2. Select a template, and choose **Edit**.
3. Modify the attribute mapping.

Removing Incoming Template Mappings

Use the **Incoming Templates** property page to remove incoming MS Mail template information mapped to a Microsoft Exchange Server attribute.

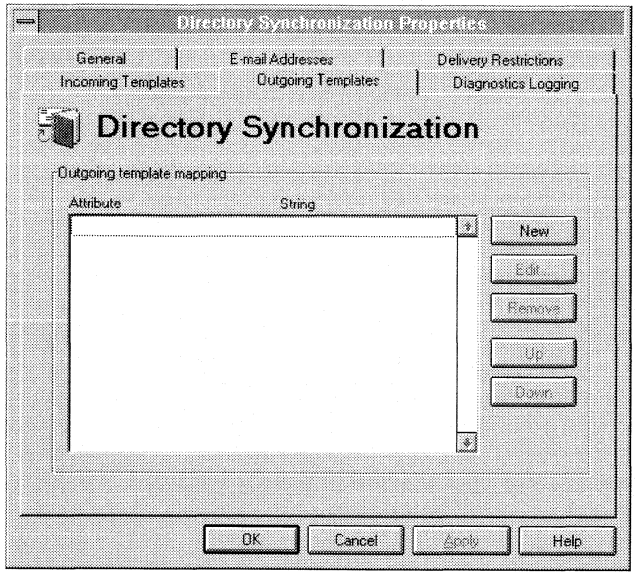
1. Select the **Incoming Templates** tab.
2. Select a template, and choose **Remove**.

Outgoing Templates

You can map Microsoft Exchange Server directory recipient attributes to outgoing MS Mail-compatible template information. For example, you can map Microsoft Exchange Server recipient location attributes to an MS Mail room template.

Getting to the Outgoing Templates property page

1. In the Administrator window, choose **Servers**, and then choose the server you want to configure.
2. Double-click **Directory Synchronization**.
3. Select the **Outgoing Templates** tab.



Configuring Outgoing Template Mappings

Use the **Outgoing Template** property page to map Microsoft Exchange Server attributes to MS Mail user information strings during directory synchronization.

Note Adding, modifying, or removing template mappings will result in a full export of directory information during the next directory synchronization cycle.

1. Select the **Outgoing Templates** tab.
2. To specify a new MS Mail template to Microsoft Exchange Server attribute mapping, choose **New**.

Option	Description
Map the attribute	The recipient attribute to map to an MS Mail template.
To the string	The MS Mail template identifier string in which you want to place outgoing attribute information.

Modifying Outgoing Template Mappings

Use the **Outgoing Template** property page to modify outgoing Microsoft Exchange Server attributes mapped to MS Mail template information.

1. Select the **Outgoing Templates** tab.
2. Select a template, and choose **Edit**.
3. Modify the attribute mapping.

Removing Outgoing Template Mappings

Use the **Outgoing Template** property page to remove a Microsoft Exchange Server attribute mapped to MS Mail template information.

1. Select the **Outgoing Templates** tab.
2. Select a template, and choose **Remove**.

Diagnostics Logging

You can control how logging information for the directory synchronization server is written to the Windows NT Event Log. You can also specify a logging level for the directory synchronization service. Viewing the event log for a dirsync server is helpful when troubleshooting the directory synchronization process.

For more information about diagnostics logging, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

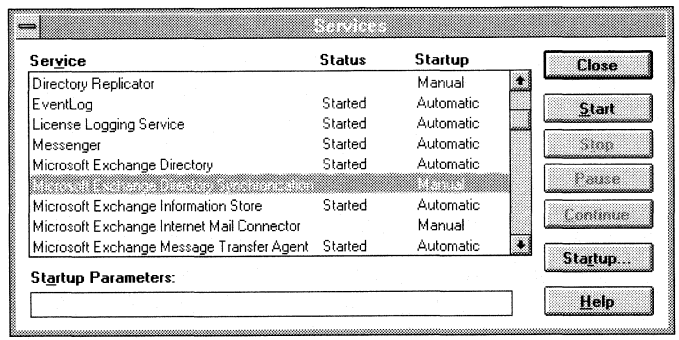
Starting and Stopping Directory Synchronization

When configuration of a dirsync server or dirsync requestor is complete, you can start the directory synchronization service using the Control Panel.

Starting Directory Synchronization

You will need to start the Microsoft Exchange Directory Synchronization service for the directory synchronization process to begin. You can set the directory synchronization service to start when the Windows NT Server starts, or you can start it manually from the Control Panel.

1. In Windows NT Control Panel, choose **Services**.



2. Select **Microsoft Exchange Directory Synchronization**.
3. Choose **Start** to start the exchange of address information.

Stopping Directory Synchronization

Before stopping directory synchronization, you should notify users and the administrator of the other system that directory synchronization will be stopped.

1. In Windows NT Control Panel, choose **Services**.
2. Select **Microsoft Exchange Directory Synchronization**.
3. Choose **Stop** to stop the exchange of address information.

For more information on starting and stopping services, see *Microsoft Exchange Server Getting Started.*

Deleting Dirsync Requestors and Servers

If you no longer want to exchange directory information with MS Mail 3.*x* systems, you can delete a dirsync requestor or dirsync server.

Deleting a Dirsync Requestor

If you delete a dirsync requestor, all addresses from the dirsync requestor are removed from the Microsoft Exchange Server global address list.

1. In the Administrator window, choose **Connections**.
2. Choose the dirsync requestor you want to remove.
3. From the **Edit** menu, choose **Delete**.

Deleting a Dirsync Server

You must remove all remote dirsync requestor objects from the organization hierarchy before you can remove a dirsync server. When you have removed the appropriate items, delete the custom recipient objects for each remote dirsync requestor.

Caution Do not delete a dirsync server object from a Microsoft Exchange Server organization until all active requestors have been configured to use another server. Deleting a dirsync server with active requestors can result in messaging and directory failures and possible data loss.

---

1. In the Administrator window, choose **Connections**.
2. Choose the dirsync server you want to remove.
3. From the **Edit** menu, choose **Delete**.

Manual Directory Synchronization

As an alternative to automated directory synchronization, you can start the process manually. Directory synchronization messages are sent at the beginning of each hour selected in the schedule grid for the directory synchronization server object. If you do not want to wait for the next scheduled directory synchronization event, you can manually start the directory synchronization process. You must add a value to the Windows NT Server registry to use this function. Manual directory synchronization can be done from the command prompt or from the **Services** application in Control Panel.

To start a directory synchronization process manually from the Windows NT Server command prompt:

1. At the command prompt, type **Net pause msexchangedx**.

Note Ignore the error message "The Microsoft Exchange Directory Synchronization service failed to pause. More help is available by typing NET HELPMSG3539." The directory synchronization process has started successfully and can be viewed from the Windows NT Event Viewer if diagnostics logging has been enabled for the directory synchronization object (MSExchangeDX).

---

2. Quit the MS-DOS session.

To start a directory synchronization process manually from the **Services** application in Control Panel:

1. In Control Panel, open the **Services** application.
2. Select **Microsoft Exchange Directory Synchronization**.
3. Choose **Pause**.

Note Ignore the error message "Could not pause the Microsoft Exchange Directory Synchronization service on \\<servername>. Error 2140: An internal Windows NT error occurred." The directory synchronization process was successfully started by issuing the pause command. Logging can be viewed from the Windows NT Event Viewer if diagnostics logging has been enabled for the directory synchronization object (MSExchangeDX).

---

4. Choose **OK**, and then close the **Services** application.

Note If your Microsoft Exchange Server computer has been configured as a directory synchronization server, manual directory synchronization checks the current status of remote directory synchronization requestors. If your Microsoft Exchange Server has been configured as a directory synchronization requestor, manual directory synchronization searches for updates from the directory synchronization server.

Importing the Directory Synchronization Master List Manually

If you are configuring Microsoft Exchange Server as a directory synchronization server for one or more MS Mail (PC) remote directory synchronization requestors, the initial export of the directory synchronization master list may be large. In particular, if the export is done over a slow network link or through an asynchronous connection, the time required for export may be significant.

For the remote directory synchronization requestor, the limit you specified in the MS Mail (PC) Administrator program may be less than the size of the master list you are importing, and you cannot import the list. You must import the directory synchronization master list manually.

To import the directory synchronization master list manually from a Microsoft Exchange Server directory server to one or more MS Mail (PC) remote directory synchronization requestors, do the following:

- Edit the Windows NT Server registry.
- Restart the Microsoft Exchange Directory Synchronization service.
- Copy the directory synchronization master list (Resync.glb) to an external storage device.
- Import the master list to the remote directory synchronization requestor and run the MS Mail (PC) Import utility.

Editing the Windows NT Registry

The following procedure describes how to configure the Windows NT registry to generate the directory synchronization master list for export.

1. Open Regedt32, and then open the following registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeDX`

2. Choose **Edit**, and then choose **Add Value**.
3. In the **Value name** box, type ResyncConnectionRDNs.

4. In the **Data type** box, select **REG_MULTI_SZ,** and then choose **OK**.
5. Under **Data**, type the common name or RDN given to the remote directory synchronization requestor object for which you are generating the master list. If there is more than one postoffice, type each postoffice name, and press ENTER.
6. Choose **OK**.
7. Stop and restart the Microsoft Exchange Directory Synchronization service.

Restarting the Microsoft Exchange Directory Synchronization Service

After successful generation of the Resync.glb file, restart the Microsoft Exchange Directory Synchronization service from the Windows NT Control Panel.

Copying the Resync.glb File to an External Storage Device

After the manual directory synchronization cycle is completed, copy the Exchsrvr\Dxadata\Resync.glb file to an external storage device (for example, disk or tape device) for transport to the remote directory synchronization requestor.

Importing the Resync.glb File to the Remote Directory Synchronization Requestor

When the Resync.glb file is received for the remote directory synchronization requestor, it must be imported manually. The remote requestor administrator copies the Resync.glb file to the remote requestor's Glb directory.

To import the list immediately, run the Import utility with the **-q** command line option. For information on using the Import utility, see the *Microsoft Mail for PC Networks Administrator's Guide*.

Because of the flexibility of Microsoft Exchange Server (for example, export of custom recipients, trust levels, and containers), you can generate unique master address lists for individual remote directory synchronization requestors or groups of requestors. The directory synchronization server can be configured for:

- All remote directory synchronization requestors with identical configurations.
- Groups of remote directory synchronization requestors with identical configurations.
- Unique configurations for each remote directory synchronization requestor.

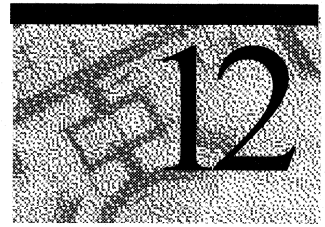
Several requestors with identical configurations If you have one or more remote directory synchronization requestors and they share similar configurations, be sure to enter all postoffice names when you create the ResyncConnectionRDNs value.

Multiple groups of requestors with identical configurations For multiple groups of remote directory synchronization requestors that have identical configurations, be sure to enter the names of all postoffices for each group, when you create the ResyncConnectionRDNs value.

You must create a ResyncConnectionRDNs value for each group. For each manual generation of the master directory synchronization list, copy the Resync.glb file from the Exchsrvr\Dxadata directory before manually importing the next group of MS Mail (PC) requestors. After the Resync.glb file has been generated for a group, restart the Microsoft Exchange Directory Synchronization service.

Individual requestors with unique configurations For individual remote directory synchronization requestors that have unique configurations, be sure to enter only the name of the requestor postoffice when creating the ResyncConnectionRDNs value. You must create a ResyncConnectionRDNs value for each requestor. For each manual generation of the master directory synchronization list, copy the Resync.glb file from the Exchsrvr\Dxadata directory before manually importing the next MS Mail (PC) requestor. After the Resync.glb file has been generated for a requestor, restart the Microsoft Exchange Directory Synchronization service.

CHAPTER 12



Microsoft Schedule+ Free/Busy Connector for Microsoft Mail

The Microsoft Schedule+ Free/Busy Connector enables Microsoft Exchange Server to share Schedule+ free and busy information with Microsoft Mail for PC Networks [MS Mail (PC)].

A user's *free and busy times* are the times when the user is either available or unavailable for meetings. The connector processes users' free and busy information from MS Mail (PC) postoffices and updates the information in the Schedule+ Free/Busy system folder. The connector then sends updated free and busy information from Microsoft Exchange Server to the MS Mail (PC) postoffices.

The Schedule+ Free/Busy Connector supports the exchange of free and busy information between MS Mail (PC) users and Microsoft Exchange Server users on the following:

- Microsoft Outlook for 32-bit platforms
- Microsoft Outlook Calendar for 16-bit platforms
- Schedule+ version 7.0
- Schedule+ version 1.0

For a description of how the Schedule+ Free/Busy Connector works, see *Microsoft Exchange Server Concepts and Planning*. For more information about calendar interoperability with MS Mail (PC), see *Microsoft Exchange Server Migration*.

Schedule+ Free/Busy Connector Setup

Setting up the Schedule+ Free/Busy Connector to transfer schedule information between Microsoft Exchange Server recipients and MS Mail (PC) recipients requires the following:

- Installing the Microsoft Mail Connector.
- Creating an AdminSch account on all postoffices participating in schedule sharing.
- Installing the Schedule+ program files on an MS Mail (PC) postoffice server.
- Installing the Schedule+ Administrator program.
- Configuring the Schdist.exe program.
- Configuring the Schedule+ Free/Busy Connector.

Note The MS Mail (PC) External program is not required if the Microsoft Mail Connector is configured as the message transfer agent (MTA) for servicing all MS Mail (PC) postoffices that share Schedule+ free and busy information. However, if you have an existing Schedule+ system and are using External as the MTA to send free and busy information, you can continue to use the External program for this purpose.

Installing Microsoft Mail Connector

You must install the Microsoft Mail Connector on Microsoft Exchange Server to share Schedule+ free and busy information between MS Mail (PC) systems and Microsoft Exchange Server. The Microsoft Mail Connector is responsible for information transfer between a Microsoft Exchange Server site and an MS Mail (PC) system. The postoffices on the MS Mail (PC) system consider a Microsoft Exchange Server site as a single MS Mail (PC) postoffice. This postoffice is the Microsoft Mail Connector postoffice, and is identified in the Schedule+ Administrator program as a typical MS Mail (PC) postoffice that conforms to the Network/Postoffice convention. You must define a Microsoft Mail Connector for every site.

Assigning AdminSch Accounts

When the Microsoft Mail Connector is installed, Microsoft Exchange Server creates an AdminSch account in the Recipients container for the Schedule+ Free/Busy Connector. To use the Schedule+ Free/Busy Connector, you must configure the AdminSch account by specifying an administrator's mailbox. This mailbox delivers status messages including non-delivery reports (NDRs). You can also specify settings, such as logging levels and polling intervals, which determine how often the Schedule+ Free/Busy Connector sends free and busy information to the MS Mail (PC) system.

Every postoffice that shares free and busy information must have an AdminSch account. You should run directory synchronization between Microsoft Exchange Server and the MS Mail (PC) system to distribute all AdminSch accounts across both systems.

Installing Schedule+ Program Files

If your mail system has multiple MS Mail (PC) postoffices and your Schedule+ users share schedule information with other postoffices, you must install the Schedule+ program files on at least one of the MS Mail (PC) postoffices.

Installing the Schedule+ Administrator Program

Use the Schedule+ Administrator program (Adminsch.exe) to configure and administer the Schedule+ system. This includes sharing schedule information across the network and specifying schedule storage duration. You must run the Schedule+ Administrator program from a Windows-based workstation that is connected to the MS Mail (PC) postoffice that contains the Schedule+ program files.

Configuring Schdist.exe

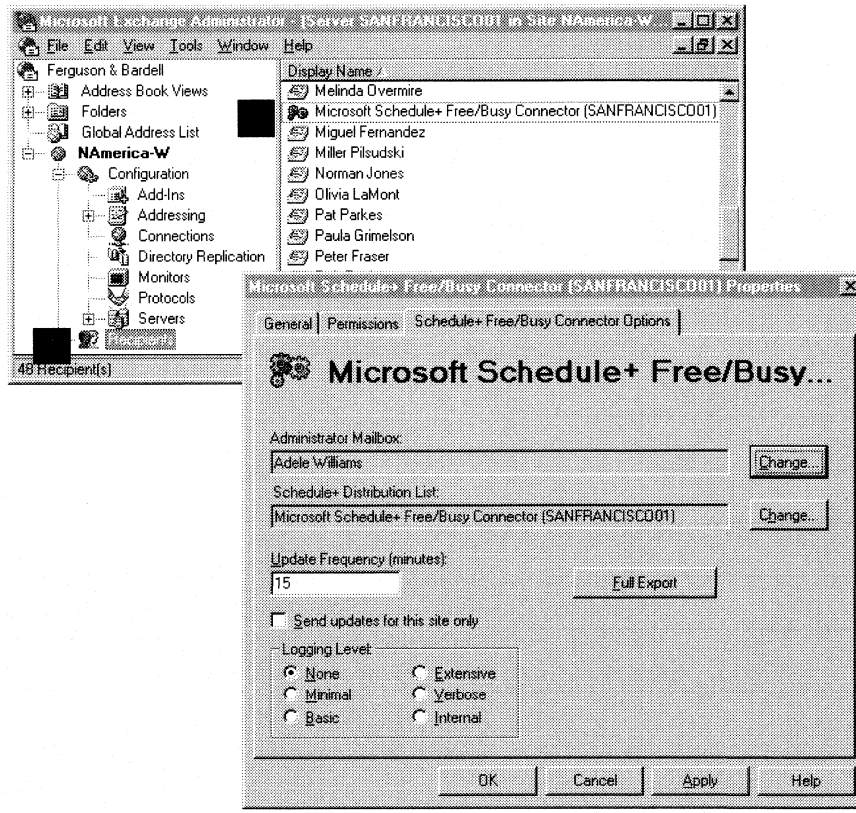
Schedule distribution is performed by the Microsoft Mail 3.*x* program Schdist.exe. It sends users' free and busy times and resource information between MS Mail (PC) postoffices and Microsoft Exchange Server. This information is sent as a formatted mail message and is delivered to the Schedule+ administrator account.

Schedule+ Free/Busy Connector Configuration

The Schedule+ Free/Busy Connector is installed when the Microsoft Mail Connector is installed. During installation, Microsoft Exchange Server creates an object with the display name Microsoft Schedule+ Free/Busy Connector (*servername*). This object is stored in the Recipients container with the alias name AdminSch assigned automatically. Configuration settings for the Schedule+ Free/Busy Connector are changed from this object.

Getting to the Schedule+ Free/Busy Connector property pages

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed, and then double-click **Recipients**.
2. Double-click **Microsoft Schedule+ Free/Busy Connector** (*servername*).



Schedule+ Free/Busy Connector Options Configuration

Use the **Schedule+ Free/Busy Connector Options** property page to configure Microsoft Exchange Server to exchange Schedule+ free and busy information between Microsoft Exchange Server sites and MS Mail (PC) postoffices. After you configure the Schedule+ Free/Busy Connector, choose the Services icon in Control Panel to start it.

Getting to the Schedule+ Free/Busy Connector Options property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed.
2. Double-click **Recipients**.
3. Double-click **Microsoft Schedule+ Free/Busy Connector** (*servername*).
4. Select the **Schedule+ Free/Busy Connector Options** tab.

Assigning an Administrator's Mailbox

Use the **Schedule+ Free/Busy Connector Options** property page to assign an administrator's mailbox. Any mail addressed to the Schedule+ Free/Busy Connector that cannot be processed, such as NDRs, is forwarded to this mailbox. An administrator's mailbox must be specified to use the Schedule+ Free/Busy Connector.

1. Select the **Schedule+ Free/Busy Connector Options** tab.
2. Choose **Change**.
3. Select a recipient for the administrator's mailbox.

Assigning a Schedule+ Distribution List

Use the **Schedule+ Free/Busy Connector Options** property page to assign a distribution list. A Schedule+ distribution list must be specified to use the Schedule+ Free/Busy Connector. The distribution list contains MS Mail (PC) postoffices that share free and busy information with the Microsoft Exchange Server site. The list should contain all AdminSch accounts.

1. Select the **Schedule+ Free/Busy Connector Options** tab.
2. Choose **Change**.
3. Select a distribution list.

Exporting the Schedule+ Distribution List

Use the **Schedule+ Free/Busy Connector Options** property page to export free and busy information for all Schedule+ users to postoffices in the Schedule+ distribution list. A full export is necessary when new members have been added to the Schedule+ distribution list.

1. Select the **Schedule+ Free/Busy Connector Options** tab.
2. Choose **Full Export**.

Setting the Schedule+ Free/Busy Connector Update Frequency

Use the **Schedule+ Free/Busy Connector Options** property page to specify how often the Schedule+ Free/Busy Connector sends free and busy information to MS Mail (PC) postoffices in the Schedule+ distribution list. The update frequency in the **Schedule+ Free/Busy Connector Options** property page should be equal to the polling interval for the Schdist program in the Microsoft Mail system. Otherwise, Schdist may receive new Schedule+ updates before it has finished processing the old set of updates.

1. Select the **Schedule+ Free/Busy Connector Options** tab.
2. In the **Update Frequency** (**minutes**) box, type a value (between 1 and 10080).

   The default polling interval for the Schedule+ Free/Busy Connector and Schdist is 15 minutes.

Exporting Free and Busy Updates for the Microsoft Exchange Server Site Only

You can configure the Schedule+ Free/Busy Connector to send free and busy information for an individual Microsoft Exchange Server site to the postoffices on the Schedule+ distribution list. Use this option if your organization has more than one Schedule+ Free/Busy Connector and you want to control the sharing of free and busy information between Microsoft Exchange Server sites and MS Mail (PC) postoffices on the distribution list.

1. Select the **Schedule+ Free/Busy Connector Options** tab.
2. Select **Send updates for this site only**.

Setting the Schedule+ Free/Busy Connector Logging Level

You can specify whether to log events in the Windows NT Server Event Log for the Schedule+ Free/Busy Connector. Setting a logging level is useful when troubleshooting the Schedule+ Free/Busy Connector. You should enable logging only if you are having problems.

1. Select the **Schedule+ Free/Busy Connector Options** tab.
2. Under **Logging Level**, select a logging option.

Option	Description
None	Logs only critical events and error events. This includes NDRs, shutdowns, initiation, and termination. Only events with a logging level of 0 are logged. This is the default.
Minimal	Equivalent to None.
Basic	Logs events with a logging level of 2 or lower. This level records the number of messages received and the number of informational messages created.
Extensive	Logs events with a logging level of 3 or lower. Logs the aliases of users receiving messages from the Schedule+ Free/Busy Connector.
Verbose	Equivalent to Extensive.
Internal	Logs all events. This includes debug strings, configuration changes, unknown address notifications, and account validations.

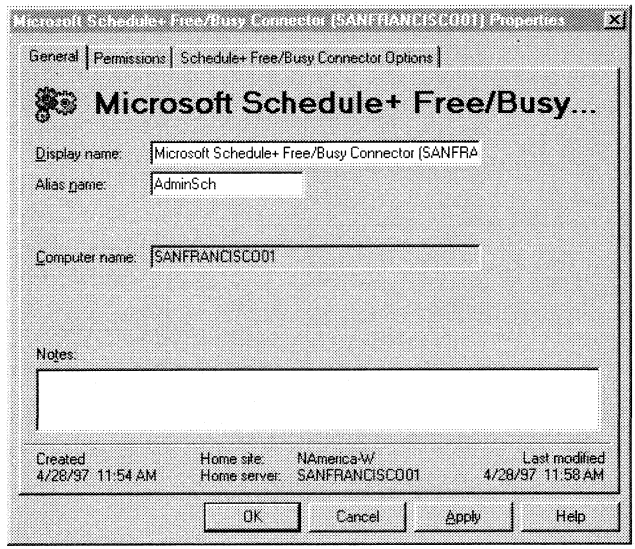
General Properties

Use the **General** property page to specify the name and location of the Schedule+ Free/Busy Connector.

Note You can view but not change the computer name on which the Schedule+ Free/Busy Connector is installed. The computer name can be changed only in Control Panel.

Getting to the General property page

1. In the Administrator window, choose the site where the Microsoft Mail Connector is installed.
2. Double-click **Recipients**.
3. Double-click Microsoft Schedule+ Free/Busy Connector (*servername*).
4. Select the **General** tab.



Specifying the Display Name and Alias Name

A *display name* is the name you specify to appear in the Administrator window and in the Address Book.

1. Select the **General** tab.
2. In the **Display name** box, type a display name (up to 256 characters) for the Schedule+ Free/Busy Connector object.

   The default is Microsoft Schedule+ Free/Busy Connector (*servername*).
3. In the **Alias name** box, type an alias name for the Schedule+ Free/Busy Connector object.

   This name must be AdminSch.
4. In the **Notes box**, type any information (up to 1024 characters) that pertains to this object.

   This information is visible only in the Administrator program.

Unresolved Schedule+ Messages

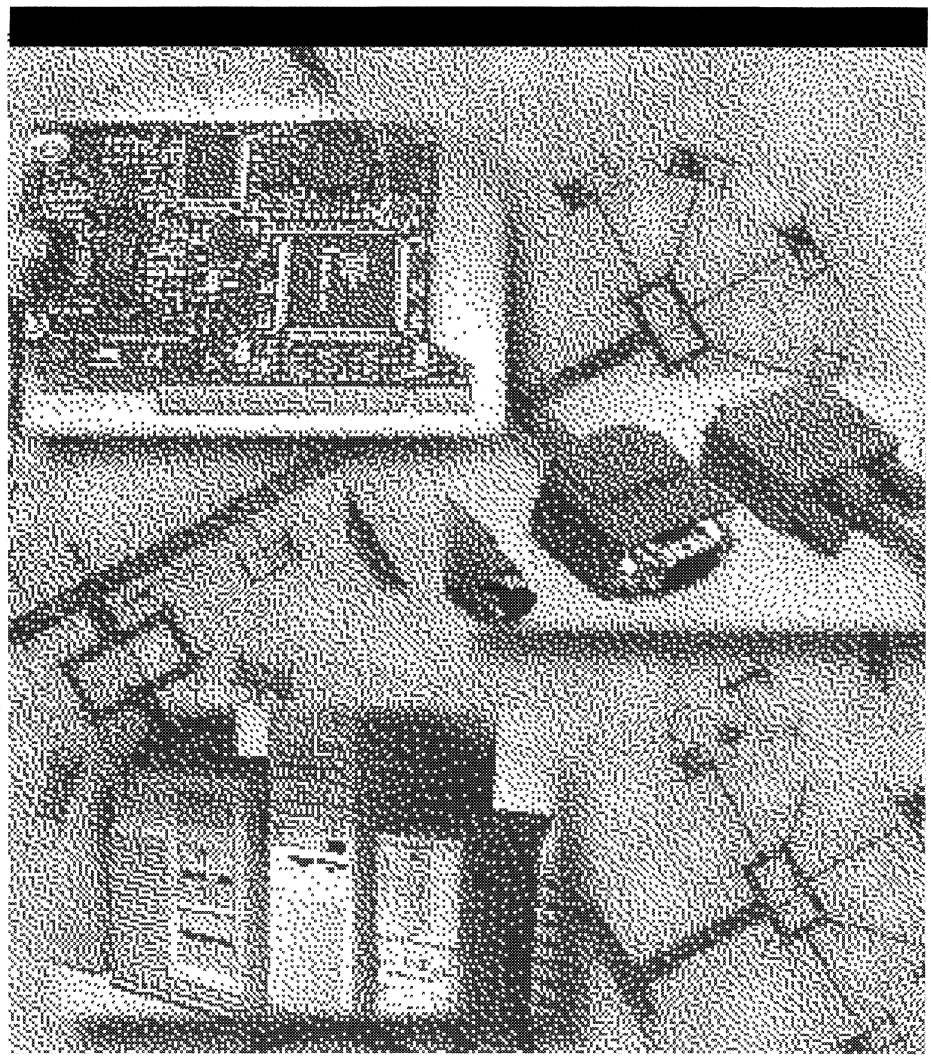
After a recipient has been moved or deleted from a Microsoft Exchange Server site, there may still be Schedule+ messages and data remaining in the Schedule+ Free/Busy system folder for the recipient. Because the recipient has been removed, the Schedule+ Free/Busy Connector cannot validate the existence of the recipient and the Schedule+ messages cannot be resolved. If a full export of the Schedule+ free and busy information is performed from the Schedule+ Free/Busy Connector, the following error message is displayed in the Windows NT Server Event Log:

```
Event ID 1049: The Directory Import process indicates that error(s)
have been logged while creating Microsoft Schedule+ Free/Busy
Connector.
```

Unresolved Schedule+ messages and data cannot be removed manually. By default, the Schedule+ Free and Busy system folder removes any recipient's Schedule+ data messages after 100 days of inactivity. Active Schedule+ accounts are not affected.

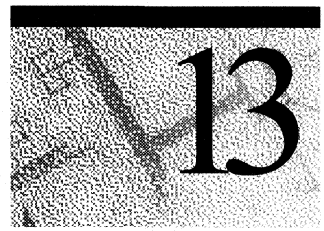
PART 3

Setting Up Internet Protocols



CHAPTER 13

Internet Protocols



The Internet is a collection of networks and gateways that use Transport Control Protocol/Internet Protocol (TCP/IP) to handle data transfer and message conversion from the sending network to the receiving network. An Internet protocol is a set of standards designed to enable different types of computers to communicate with one another and to exchange information through the Internet.

In addition to providing Simple Mail Transfer Protocol (SMTP) support, Microsoft Exchange Server supports the following:

- Internet News Service/Network News Transfer Protocol (NNTP)
- Post Office Protocol version 3 (POP3)
- Internet Message Access Protocol Version 4 rev1 (IMAP4rev1)
- Lightweight Directory Access Protocol (LDAP)
- Hypertext Transfer Protocol (HTTP) and Microsoft Outlook Web Access

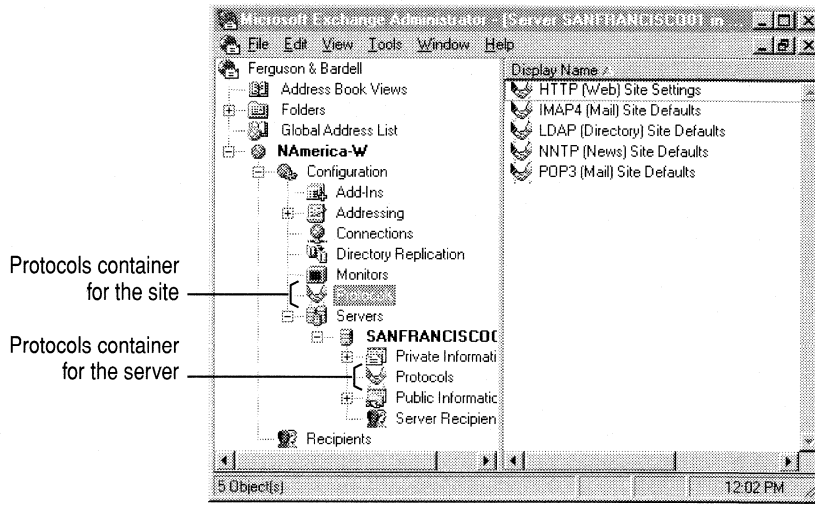
You can set properties for Internet protocols at either the site or server level using the Microsoft Exchange Server Administrator program. You can also set properties on specific Internet protocols. For more information on configuring each protocol, see the appropriate chapter in *Microsoft Exchange Server Operations*.

Configuring Site and Server Properties

Each site and server has a container called Protocols that contains configuration objects for each Internet protocol. You can configure default settings that apply to all protocols in the site using the site Protocols container. Alternatively, you can configure settings that apply only to individual servers. If you configure default settings for protocols at the site level, those settings apply to all servers in the site; they are not replicated between sites. If you want to use different settings on one server in the site, you can change the protocol settings for that server only.

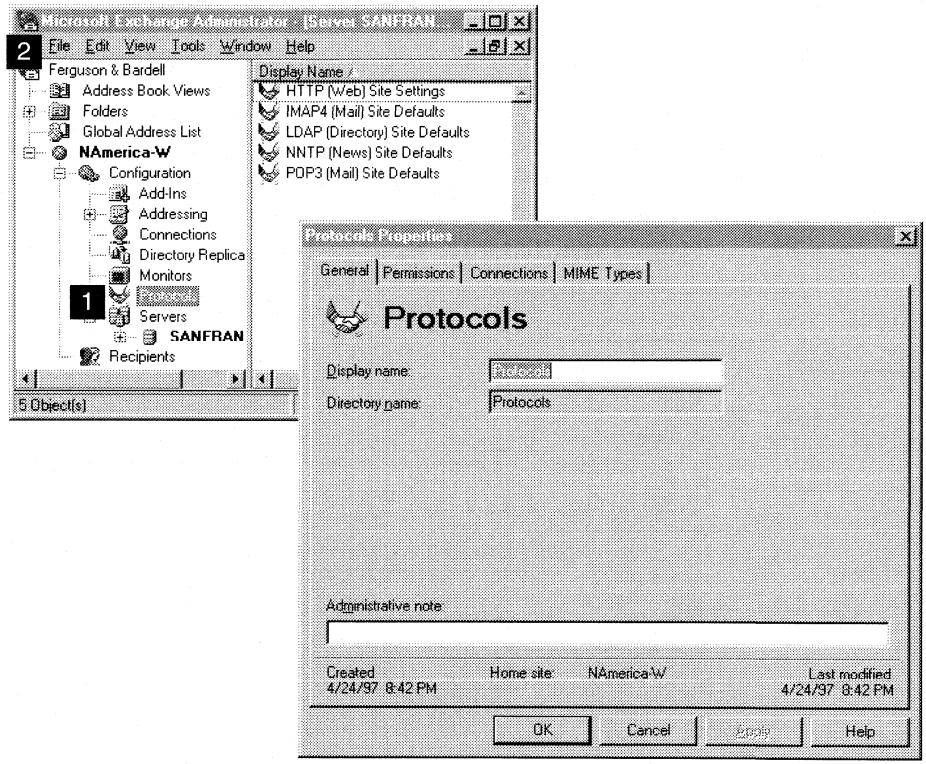
The following illustration shows the Internet protocol objects in the site and server containers.

Note The HTTP (Web) Site Settings object is configurable only at the site level.



Getting to the Site and Server property pages

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. From the **File** menu, choose **Properties**.



General Properties

Use the **General** property page for the site Protocols container to set the defaults for all servers in the site. Use the **General** property page for the server Protocols container to specify different settings for that server.

Getting to the General property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. From the **File** menu, choose **Properties**.
3. Select the **General** tab.

Defining a Display Name

Use the **General** property page to define the protocol's display name.

1. Select the **General** tab.
2. Type a display name.

Option	Description
Display name	Type a maximum of 256 alphanumeric characters, which can include spaces and special characters. If no name is provided, the system prompts for a value.
Directory name	The name is defined during installation and cannot be changed.

Using the Site Defaults

Use the **General** property page to view or set the site defaults for all Internet protocols at the site level.

Note This option is available only for Internet protocol properties in the Server container.

1. Select the **General** tab.
2. Select or clear the **Use site defaults for all properties** check box.

Option	Description
Use site defaults for all properties	Select to use the options you have set for permissions and message format options.

Permissions

You can set permissions to control user access to all objects in the Protocols container. You grant permission to a user (or group) by assigning the user a role, which defines how much and what type of access a user has. Microsoft Exchange Server provides a number of predefined roles, but you can also create custom roles to meet your needs.

If you have configured the Administrator program to display the **Permissions** property page for all objects, you can set permissions on each protocol object in the site and server Protocols containers.

Note If you want to use Secure Socket Layer (SSL) encryption with NNTP, POP3, IMAP4, and LDAP, the Microsoft Exchange Server service account must be granted Administrator permissions for the local computer. SSL provides secure data communications using data encryption and decryption.

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

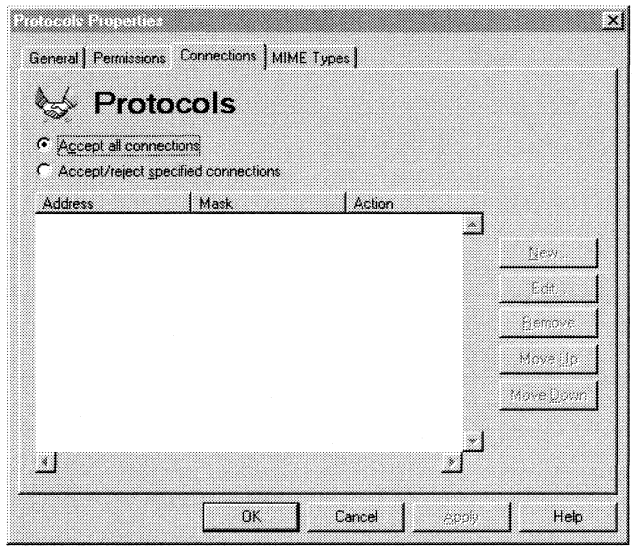
Connections

You can accept or reject POP3, NNTP, IMAP4 and LDAP access based on the client's Internet protocol (IP) address. For example, if you don't want a client to access information on your server, you can configure Microsoft Exchange Server to reject connections from that client.

Note Settings in the **Connections** property page do not apply to HTTP. You can restrict HTTP connections by configuring settings available in the **Advanced** property page in the Microsoft Internet Information Server Internet Service Manager.

Getting to the Connections property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. From the **File** menu, choose **Properties**.
3. Select the **Connections** tab.



Accepting or Rejecting Connections

Use the **Connections** property page to accept or reject connections by their IP address.

1. Select the **Connections** tab.
2. Select an option.

Option	Description
Accept all connections	Select to accept all connections regardless of the IP address. The default is to accept all connections.
Accept/reject specified connections	Select to specify the IP address from which to accept or reject connections.

Adding a Rule

Use the **Connections** property page to add a new rule that accepts or rejects connections by IP address and mask. A mask (also called a subnet mask) is a value used with an IP address that identifies the network location of the client computer. The IP addresses of hosts connecting to the server are matched against the rules, and the connections will be accepted or denied accordingly. If no rule exists that matches an IP address, the connection is accepted by default.

Note To specify a range of IP addresses, use the IP address and subnet mask. For example, specifying an IP address, such as 11.103.41.0, and a subnet mask, such as 255.255.255.0, restricts the range to all IP addresses that start with 11.103.41. To specify an individual IP address, use the IP address and a subnet mask of 255.255.255.255. For example, if you specify an IP address of 11.103.41.20 and a subnet mask of 255.255.255.255, the address is restricted to 11.103.41.20.

1. Select the **Connections** tab.
2. Choose **New**.
3. Select an option to accept or reject a connection.
4. In the **IP Address** box, type a numeric IP address.
5. In the **Mask** box, type a numeric mask.

Option	Description
Accept connection	Select to accept this new IP address connection.
Reject connection	Select to reject this new IP address connection.
IP Address	The Internet protocol address of the SMTP host that is accepted or rejected.
Mask	Identifies the network location of the client computer.

Removing a Rule

Use the **Connections** property page to remove a rule from the list.

1. Select the **Connections** tab.
2. Select the rule you want to remove.
3. Choose **Remove**.

Moving a Rule Up or Down

Use the **Connections** property page to move a rule up or down in the list. Because rules are processed in order from first to last, the most specific rules should be at the top of the list and the most general rules should be at the bottom. For example, suppose you want to configure three rules so that Microsoft Exchange Server accepts connections from all IP addresses, rejects connections from all hosts in a subnet, but accepts connections from an individual host within that subnet. You should specify the rule that accepts connections from an individual server first and the rule that accepts connections from all IP addresses last.

The IP accept and reject list in the **Connections** property page for the server Protocols container is processed before the list in the **Connections** property page for the site Protocols container.

1. Select the **Connections** tab.
2. Select the IP address you want to move.
3. Choose **Move Up** to move the address up in the list, or choose **Move Down** to move the address down in the list.

Editing a Rule

Use the **Connections** property page to modify the settings for an existing rule.

1. Select the **Connections** tab.
2. Choose **Edit**.
3. Select an option either to accept or reject a connection.
4. In the **IP Address** box, type a numeric IP address.
5. In the **Mask** box, type a numeric mask.

Option	Description
Accept connection	Select to accept this new IP address connection.
Reject connection	Select to reject this new IP address connection.
IP Address	The Internet protocol address of the SMTP host that is accepted or rejected.
Mask	Identifies the network location of the client computer.

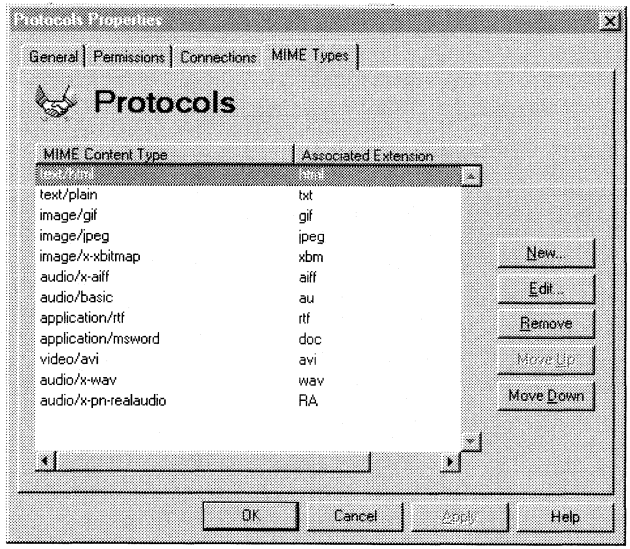
MIME Types

Microsoft Exchange Server can assign appropriate file extensions for inbound attachments if the Multipurpose Internet Mail Extensions (MIME) content type and corresponding file extensions are defined in the **MIME Types** property page. For example, you can specify that all attachments with a content type of text/HTML are automatically given an extension (such as .Htm). For outbound attachments, a MIME type is used for the file extensions listed in the **MIME Types** property page.

Note Duplicate entries are allowed for both the content type and the file extension. The first occurrence found in the list is the mapping that is used.

Getting to the MIME Types property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. From the **File** menu, choose **Properties**.
3. Select the **MIME Types** tab.



Creating a New MIME Type

Use the **MIME Types** property page to add a new MIME type to the list.

In MIME, there are *primary types*, which describe the general content of a message, and *subtypes*, which further describe the specific data. The two types are separated by a forward slash (/), such as text/plain.

1. Select the **MIME Types** tab.
2. Choose **New**.
3. In the **MIME content type** and **Associated extension** boxes, type the appropriate information.

Option	Description
MIME content type	Type the content for which you will associate an extension. Common types are text, application, multipart, image, audio, video, and message.
Associated extension	Type the extension that will be associated with the content type. Do not use a period before the extension.

Removing a MIME Type

Use the **MIME Types** property page to remove a MIME type from the list.

1. Select the **MIME Types** tab.
2. Select the MIME content type you want to remove.
3. Choose **Remove**.

Moving a MIME Type Up or Down

Use the **MIME Types** property page to specify the order of the MIME content type in the list. The order of content types is important if the same content type maps to multiple extensions. For example, an item with a .Doc extension can be mapped to application/msword, application/binary, or text/plain. By specifying the processing order, you can ensure that the .Doc item is mapped to the correct content type. Content types are processed in order from first to last.

1. Select the **MIME Types** tab.
2. Select the MIME content type you want to move.
3. Choose **Move Up** to move the MIME content type up in the list, or choose **Move Down** to move the MIME content type down in the list.

Mailbox and Custom Recipient Configuration

You can specify which protocols a client can use to connect to Microsoft Exchange Server. You can also specify which message formats will be used for these protocols. For example, you can configure whether users can connect to their mailbox using POP3. Users who don't have a Microsoft Exchange Server mailbox can connect to Microsoft Exchange Server as custom recipients.

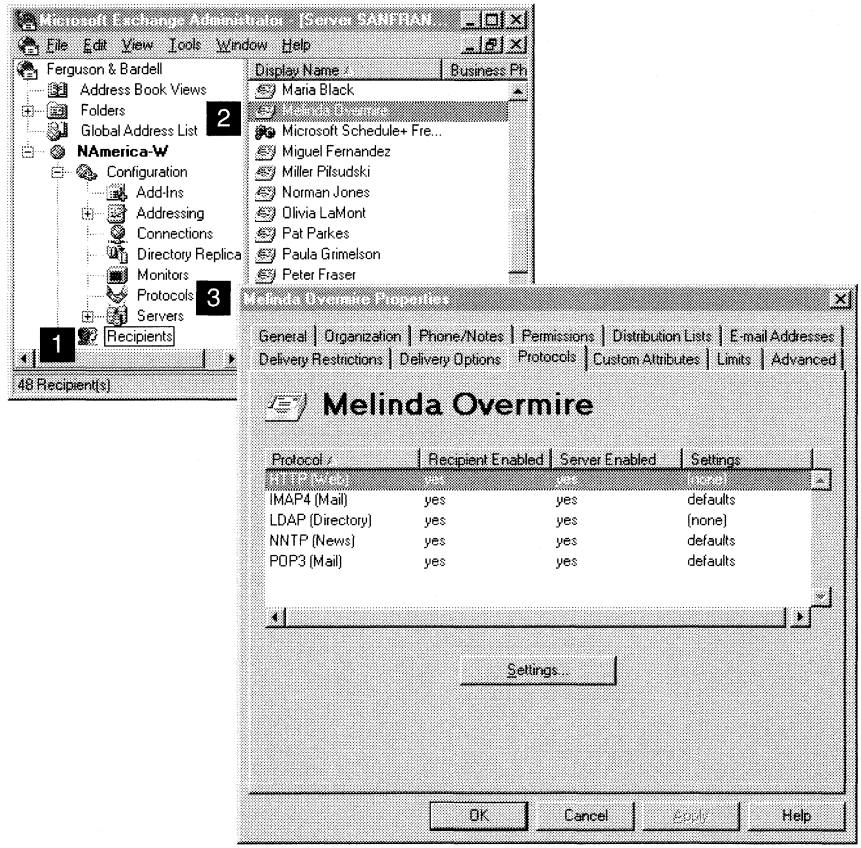
Note If you disable NNTP, HTTP, IMAP4 or POP3 on the server object, support for these protocols is also disabled for individual mailboxes and custom recipients. For Internet protocols to be enabled on a mailbox or custom recipient, the protocol must be enabled for both the server and the recipient.

For more information on configuring each type of protocol, see the appropriate chapter in *Microsoft Exchange Server Operations*.

Getting to the Protocols property page

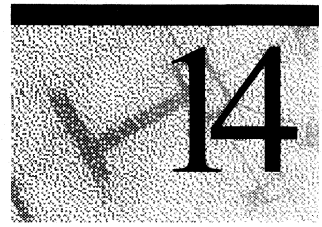
1. In the Administrator window, choose **Recipients**.
2. Double-click the mailbox or custom recipient you want to configure.

   You can enable support for NNTP, IMAP4, and HTTP on both mailboxes and custom recipients. You can enable POP3 support only on mailboxes.
3. Select the **Protocols** tab.



CHAPTER 14

POP3



The Post Office Protocol version 3 (POP3) enables users with POP3 clients to retrieve mail from their Microsoft Exchange Server Inbox. Any third-party e-mail client that supports POP3 can be used to connect to a Microsoft Exchange Server and access messages.

To set up POP3 support, you perform the following configuration tasks:

- Configure POP3 site and server properties.
- Configure the Internet Mail Service on the Microsoft Exchange Server computer so POP3 clients can send messages.
- Configure POP3 clients.

POP3 Site and Server Properties Configuration

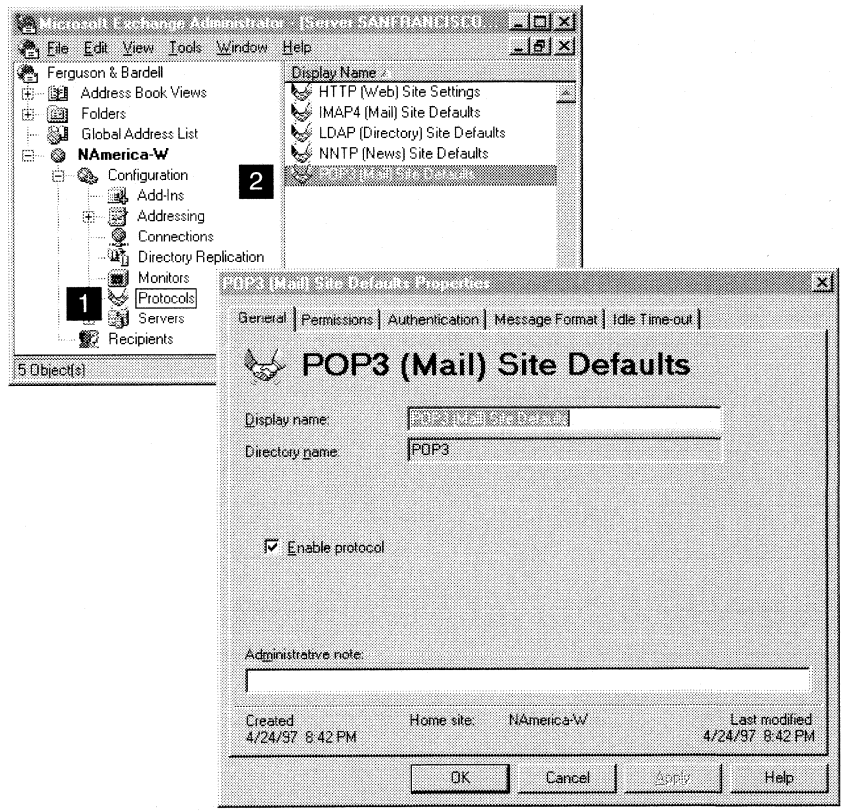
When Microsoft Exchange Server is installed, POP3 is enabled in the site by default so POP3 clients can retrieve their mail as soon as the server is set up. However, before POP3 clients can send mail, the Internet Mail Service must be installed and configured.

POP3 can be configured at the site, server, and mailbox levels:

- Site level POP3 protocol settings represent default values that can be inherited by servers.
- In the server POP3 property pages, you can use either the site defaults or configure options for each server.
- In the mailbox POP3 property pages, you can use either the server defaults or configure options on a mailbox-by-mailbox basis. Note, however, that if POP3 is disabled at the server, it is disabled for all mailboxes on that server, regardless of whether it is enabled at the mailbox level.

Getting to the POP3 property pages

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **POP3 (Mail) Site Defaults** to configure site POP3 defaults, or **POP3 (Mail) Settings** to configure a server's POP3 settings.



General Properties

Use the **General** property page to specify a display name for the POP3 object and to enable or disable POP3 for the site or server.

Getting to the General property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **POP3 (Mail) Site Defaults** to configure site POP3 defaults, or **POP3 (Mail) Settings** to configure a server's POP3 settings.
3. Select the **General** tab.

Defining a Display Name

Use the **General** property page to define the POP3 display name.

1. Select the **General** tab.
2. Type a display name.

Option	Description
Display name	A maximum of 256 alphanumeric characters, which can include spaces and special characters.
Directory name	A name defined automatically during installation that cannot be changed.

Using the Site Defaults

Use the **General** property page on the POP3 server object to use the default values from the POP3 site object.

Note This option is available only for POP3 properties in the server container.

1. Select the **General** tab.
2. Select or clear the **Use site defaults for all properties** check box. Select to use the options you've set for permissions and message format options.

Enabling or Disabling POP3

Use the **General** property page to enable or disable POP3 on the Microsoft Exchange Server computer or change the site default.

Note It can take several minutes for the change to take effect.

1. Select the **General** tab.
2. Select or clear the **Enable protocol** check box.

Authentication

Use the **Authentication** property page to specify methods of *authentication* that POP3 clients use when connecting to Microsoft Exchange Server. Authentication is the process the POP3 server uses to determine whether to grant the user permission to connect to the system. By default, Microsoft Exchange Server allows a POP3 client to connect using any of the supported authentication methods.

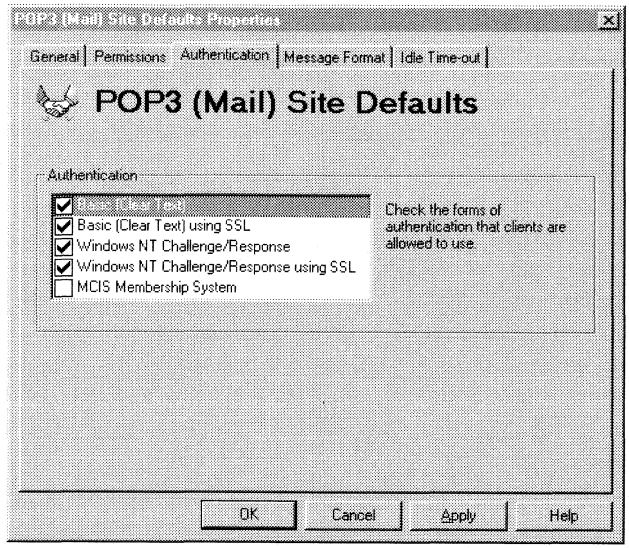
One method of authentication that you can specify is Secure Sockets Layer (SSL) encryption. SSL encrypts all data sent between clients and servers. To use SSL, Microsoft Internet Information Server (IIS) must be installed on the Microsoft Exchange Server computer before Microsoft Exchange Server is installed, and the Microsoft Exchange Server service account must be granted Administrator permissions for the local computer. In addition, you must complete the following procedure.

1. In Internet Information Server Key Manager, choose the POP3 icon.
2. Create a key request by choosing **Create New Key** from the **Key** menu and typing the required information.
3. Obtain a certificate from a Certificate Authority.
4. Under POP3, select the key request, and then choose **Install Key Certificate** from the **Key** menu.
5. Select the default server connection, or enter the server's IP address to bind the key to any inbound connection.
6. From the **Servers** menu, choose **Commit Changes Now**, and then choose **OK** to commit all the changes.

For more information about setting up SSL, see your IIS documentation.

Getting to the Authentication property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **POP3 (Mail) Site Defaults** to configure site POP3 defaults, or **POP3 (Mail) Settings** to configure a server's POP3 settings.
3. Select the **Authentication** tab.



Setting Authentication Methods

Use the **Authentication** property page to specify the authentication method a POP3 client uses to access information on the Microsoft Exchange Server computer. In order for a POP3 client to log on to the Microsoft Exchange Server computer, one of the authentication methods that the client supports must be enabled on the server. Check with your client's vendor if you are unsure of which authentication methods are available.

1. Select the **Authentication** tab.
2. In the **Authentication** box, select an authentication type.

Option	Description
Basic (Clear Text)	Enable authentication through an unencrypted user name and password. Most POP3 clients support this method.
Basic (Clear Text) using SSL	Uses SSL protocol to encrypt clear text on port 995.
Windows NT Challenge/Response	Enable authentication through Windows NT network security and an encrypted password. This method is supported by Microsoft Internet Mail and News version 3.0 and later.
Windows NT Challenge/Response using SSL	Enable authentication using Windows NT network security to occur through an SSL-encrypted channel on port 995. This method is supported by Microsoft Outlook Express.
MCIS Membership System	Enable authentication using Windows NT network security to occur through the Microsoft Commercial Internet Server (MCIS) Membership System.

Note If Windows NT Challenge/Response is enabled on the Microsoft Exchange Server computer, Microsoft Internet Mail and News version 3.0 attempts to connect to the Microsoft Exchange Server computer using Windows NT Challenge/Response. It ignores the specified POP3 account. If authentication using this method fails, Internet Mail tries to connect to the Microsoft Exchange Server computer using basic clear-text authentication and the specified POP3 account.

With Windows NT Challenge/Response and Internet Mail, it is not possible to specify the name of the Microsoft Exchange Server mailbox you want to access. By default, Microsoft Exchange Server attempts to access the mailbox associated with the Windows NT user account that the user is logged on as. For example, if you are logged on as Domain\Suzanf, with Windows NT Challenge/Response enabled, Microsoft Exchange Server attempts to access the mailbox called Suzanf.

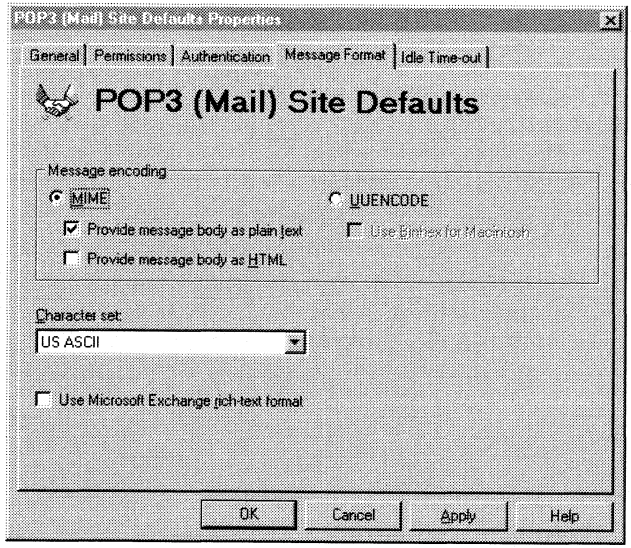
Message Format Properties

Use the settings in the **Message Format** property page to specify the format that Microsoft Exchange Server messages are converted to when they are retrieved by a POP3 client. These settings are based on the message format that the POP3 clients support when connecting to the server. The message content format and character set option can be configured for individual mailboxes, servers, and sites.

Note Messages sent by an Internet user are not converted. Instead they are retrieved by the POP3 client in the format that the message was composed in.

Getting to the Message Format property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **POP3 (Mail) Site Defaults** to configure site POP3 defaults, or **POP3 (Mail) Settings** to configure a server's POP3 settings.
3. Select the **Message Format** tab.



Enabling Rich Text Format

You can enable or disable support for rich text format. If rich text format is enabled, messages that are retrieved by the POP3 client contain Microsoft Exchange Server rich text format information as attachments to messages. POP3 clients, such as the Microsoft Internet Mail Provider, that understand rich text format use the information to display a rich text representation of the message. Rich text in messages retains character formatting, such as bold, color, and italic.

1. Select the **Message Format** tab.
2. Select the **Use Microsoft Exchange rich-text format** check box.

Specifying Message Format Options

When a user retrieves messages using POP3, you can specify how these messages are converted from the Microsoft Exchange Server format to various Internet mail formats.

Messaging Application Programming Interface (MAPI) clients such as Microsoft Outlook are capable of multilingual support, but they compose messages using Microsoft Windows code pages instead of Internet character sets. For most languages, there is a one-to-one correspondence between the character set and the code page. If this is the case, Microsoft Exchange Server automatically assigns the correct character set that corresponds to the code page that the message was composed in. However, if multiple character sets exist for the same code page, Microsoft Exchange Server uses the character setting specified in the **Character set** box in the **Message Format** property page. If the character set is not appropriate for the code page, a default character set is used. For example, suppose a message is received that uses Japanese code page 932. That code page can be mapped to one of several character sets including JIS, Shift-JIS, and EUC. If the **Character set** box is set to Shift-JIS, that character setting will be used. However, if the **Character set** box is set to US-ASCII, Microsoft Exchange Server will use the default character set for that code page, which is JIS.

Messages that are received from the Internet already have a character set specified or will have one assigned to it when the message is received by the Internet Mail Service.

1. Select the **Message Format** tab.
2. In the **Message encoding** box, select options for message format.
3. In the **Character set** box, select the default character set.

Option	Description
MIME	Text and attachments are encoded using MIME. If a MIME message is delivered to a non-MIME-aware client, the text and attachments may not be usable. This is the default.
Provide message body as plain text	A plain text MIME body part is generated for the message. If **Provide message body as HTML** is also selected, Microsoft Exchange Server provides both Hypertext Markup Language (HTML) and plain text in a MIME multipart alternative message.

(continued)

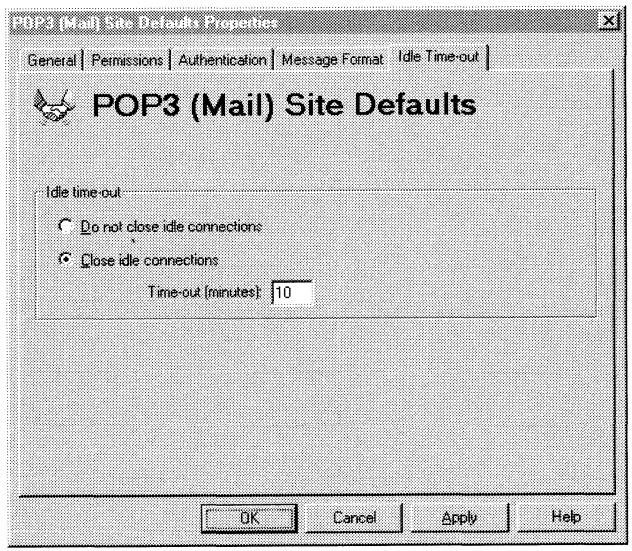
Option	Description
Provide message body as HTML	A MIME body part in HTML is generated for the message. If **Provide message body as plain text** is also selected, Microsoft Exchange Server provides both HTML and plain text in a MIME multipart alternative message. HTML is an Internet standard that enables rich-text formatting such as bold, color, and italic to appear in messages. Clients such as Microsoft Internet Mail and News version 3.0, Netscape Navigator version 3.0, and Eudora Pro version 3.0 can read HTML.
UUENCODE	Renders the message body as text with any attachments encoded by the uuencode method, which is commonly used in the UNIX operating system to encode 8-bit data transmitted on the Internet.
Use Binhex for Macintosh	Renders the message body as text with any attachments encoded by the BinHex method, which is commonly used in the Macintosh operating system to encode 8-bit data transmitted on the Internet.
Character set	Specifies the character set that is used when generating MIME and non-MIME messages that originate from Microsoft Exchange Server. The default character set varies according to the language installed on the server.

Idle Time-out

Use the **Idle Time-out** property page to specify how long POP3 connections can remain idle before they are closed.

Getting to the Idle Time-out property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **POP3 (Mail) Site Defaults** to configure site POP3 defaults, or **POP3 (Mail) Settings** to configure a server's POP3 settings.
3. Select the Idle **Time-out** tab.



Setting Idle Time-out Connections

Use the **Idle Time-out** property page to close POP3 connections after a specified interval of inactivity.

1. Select the **Idle Time-out** tab.
2. Select an option.

Option	Description
Do not close idle connections	Idle connections never close.
Close idle connections	Idle connections close after the time period specified in the **Time-out (minutes)** box.
Time-out (minutes)	The amount of time in minutes a connection can remain idle before being closed.

Diagnostics Logging

You can control how logging information for POP3 is written to the Windows NT Event Log. You can specify the types of events that are logged for POP3 and the level of logging information for each event. Viewing the event log for POP3 is useful when troubleshooting problems that occur.

Note Diagnostics logging is available only for POP3 properties in the server container.

For more information about diagnostics logging, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

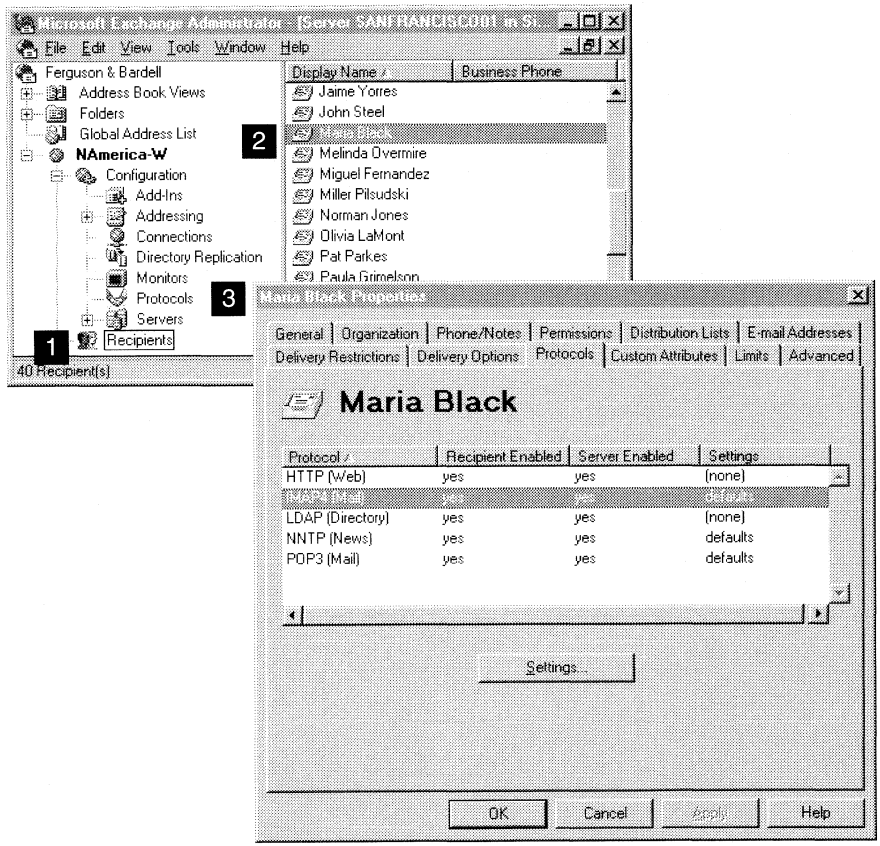
POP3 Mailbox Configuration

You can configure POP3 on a per-mailbox basis.

Note If you disable POP3 on the server object, POP3 support is also disabled for individual mailboxes. For POP3 to be enabled on a mailbox, it must be enabled on both the server and the mailbox.

Getting to the Protocols property page

1. In the Administrator window, choose **Recipients**.
2. Double-click the mailbox you want to configure.
3. Select the **Protocols** tab.



Enabling POP3 for a Mailbox

Use the **Protocols** property page to enable POP3 for individual mailboxes.

1. Select the **Protocols** tab.
2. Select **POP3 (Mail)**, and then choose **Settings**.
3. Select the **Enable POP3 for this recipient** check box.

Specifying POP3 Settings for Message Encoding

If POP3 is enabled on a mailbox, you can use default settings for message format. Alternatively, you can customize the settings for individual mailboxes. You can specify how text and attachments are encoded and the character set that your recipient uses.

The settings in the **Message Encoding** box determine the format that Microsoft Exchange Server messages are converted to when they are retrieved by a POP3 client.

Note Messages sent by an Internet user are not converted. Instead, they are retrieved by the POP3 client in the format that the message was originally composed in.

---

1. Select the **Protocols** tab.
2. Select **POP3 (Mail)** and choose **Settings**.
3. Select options for message encoding and default character sets. To use message format defaults that you set at the server level, select the **Use protocol defaults** check box. For information about message format options, see "Message Format Properties" earlier in this chapter.

Internet Mail Service Configuration

You must configure the Internet Mail Service so that POP3 clients can send mail.

Getting to the Internet Mail Service Routing property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service you want to configure.
3. Select the **Routing** tab.



Configuring the Internet Mail Service

Use the following procedure to configure the Internet Mail Service for POP3 clients.

Note If the Internet Mail Service was not configured to reroute incoming Simple Mail Transport Protocol (SMTP) mail, you may receive a non-delivery report (NDR) for any messages submitted by POP3 clients to recipients outside the organization. To resolve the problem, configure the Internet Mail Service and resend the messages.

---

1. Select the **Routing** tab.
2. Select the Reroute incoming SMTP mail (required for POP3/IMAP4 support) option.
3. Choose **Add**.
4. Type the SMTP domain name of your organization in the **E-mail sent to this domain** box.
5. Select the **Should be accepted as "inbound"** option.
6. Choose **OK**.
7. Stop and restart the Internet Mail Service.

POP3 Client Configuration

To connect to a Microsoft Exchange Server POP3 computer, you must specify the following information on the POP3 client:

- POP3 account name
- POP3 e-mail address
- POP3 server name
- SMTP server name

Because POP3 clients vary, the steps for configuring clients to connect to a Microsoft Exchange Server POP3 computer are different for each client. For information about how to configure the Microsoft Internet Mail POP3 client that is included with Microsoft Internet Explorer version 3.0, see "Sample POP3 Client Configuration" later in this chapter.

POP3 Account Name

A POP3 account is the alias name of a Microsoft Exchange Server mailbox that supports POP3. For example, the alias for Suzan Fine's mailbox is SuzanF.

Because Microsoft Exchange Server uses Windows NT user accounts for authentication, it may be necessary to specify the mailbox's Windows NT domain and user account and alias name. Note that performance may be improved by including the mailbox's Windows NT domain in the POP3 account name.

Keep the following in mind when you set your POP3 client's account name:

- If a Windows NT domain and user name are specified as the POP3 account name, they must precede the mailbox's alias name. For example, *Windows_NT_domain\user_account_name\mailbox_alias name*.
- If only an alias name is specified as the POP3 account, the Microsoft Exchange Server POP3 computer uses a Windows NT user name that is equivalent to the alias name. All Windows NT domains are searched for the first domain that contains that Windows NT user. For example, if you specify SuzanF as the POP3 account, all domains are searched for the first domain that contains user *Windows_NT_domain*\SuzanF\SuzanF.

Note You can use either a "\" or a "/" as a delimiter for the POP3 account name. If you cannot connect using one delimiter, try using the other delimiter.

- If only a Windows NT domain and user account are specified as the POP3 account, the Microsoft Exchange Server POP3 computer uses a mailbox alias that is equivalent to the Windows NT user account. For example, specifying *domain_name*\SuzanF as the POP3 account is equivalent to specifying *domain_name*\SuzanF\SuzanF as the POP3 account.

- The POP3 password for the mailbox is the Windows NT user account password that is associated with the Microsoft Exchange Server mailbox.

Note If Windows NT Challenge/Response is enabled on the Microsoft Exchange Server computer, Microsoft Internet Mail and News version 3.0 attempts to connect to the Microsoft Exchange Server computer using Windows NT Challenge/Response. It ignores the specified POP3 account. If authentication using this method fails, Internet Mail tries to connect to the Microsoft Exchange Server computer using basic clear text authentication and the specified POP3 account.

With Windows NT Challenge/Response and Internet Mail, it is not possible to specify the name of the Microsoft Exchange Server mailbox you want to access. By default, Microsoft Exchange Server attempts to access the mailbox associated with the Windows NT user account that the user is logged on as. For example, if you are logged on as Domain\Suzanf, with Windows NT Challenge/Response enabled, Microsoft Exchange Server attempts to access the mailbox called Suzanf.

POP3 E-mail Address

The POP3 e-mail address is the SMTP e-mail address that Internet users use to send messages. For example, the user's POP3 e-mail address could be SuzanF@FB.com.

POP3 Server Name

The POP3 server name is the computer name of the Microsoft Exchange Server computer that has the POP3 mailbox account that the POP3 client accesses.

Note Some POP3 clients, such as Eudora Light, do not allow you to specify the name of the POP3 server. If this option isn't available, you can often specify the name of the POP3 server in the POP3 account field. To do so, add an at sign (@) and the server name to the end of the POP3 account. For example, if your POP3 account is SuzanF, and the server your account is located on is called Exchange1, specify your POP3 account as SuzanF@Exchange1.

SMTP Server Name

The SMTP server name is the name of the computer running the Internet Mail Service that provides SMTP service for the POP3 client.

Sample POP3 Client Configuration

The following example shows how to set up a POP3 client for a Microsoft Exchange Server user named Suzan Fine at a company called Ferguson & Bardell (FB).

You create a Microsoft Exchange Server mailbox for Suzan with SuzanF as the alias name and Exchange1 as the computer name. The primary Windows NT account that is given permissions on this mailbox is FB\SuzanF. The Internet Mail Service that is providing SMTP service to the POP3 accounts is also running on the Exchange1 computer. The domain name of the company is FB.com. The following options must be specified for the Microsoft Internet Mail POP3 client that is included in Microsoft Internet Explorer 3.0:

Name Suzan Fine

Organization Ferguson & Bardell

E-mail address SuzanF@FB.com

Outgoing Mail (SMTP) server Exchange1

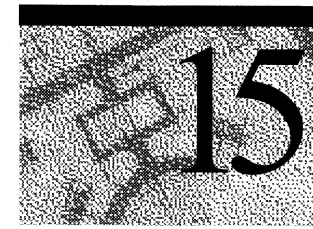
Incoming Mail (POP3) server Exchange1

POP3 account FB\SuzanF\SuzanF

Password Windows NT password for account FB\SuzanF

CHAPTER 15

IMAP4



The Internet Message Access Protocol, Version 4rev1 (IMAP4rev1) enables users with any IMAP4rev1 client (that is compliant with RFC 2060) to access mail in their Microsoft Exchange Server mailbox. It can also be used to read and post messages to public folders, or to access another user's mailbox that they have been granted access to.

Note Because of limitations in the IMAP4 protocol, you cannot use an IMAP4 client to access folders that use slash marks (/) in their name. To access these folders, you must rename them so they don't use a slash mark (/).

To set up IMAP4 support, you perform the following configuration tasks:

- Configure IMAP4 site and server properties.
- Configure the Internet Mail Service on the Microsoft Exchange Server computer so IMAP4 clients can send messages.
- Configure IMAP4 clients.

IMAP4 Site and Server Properties Configuration

When Microsoft Exchange Server is installed, IMAP4 is enabled in the site by default so IMAP4 clients can access their mail as soon as the server is set up. However, before IMAP4 clients can send mail, the Internet Mail Service must be installed and configured.

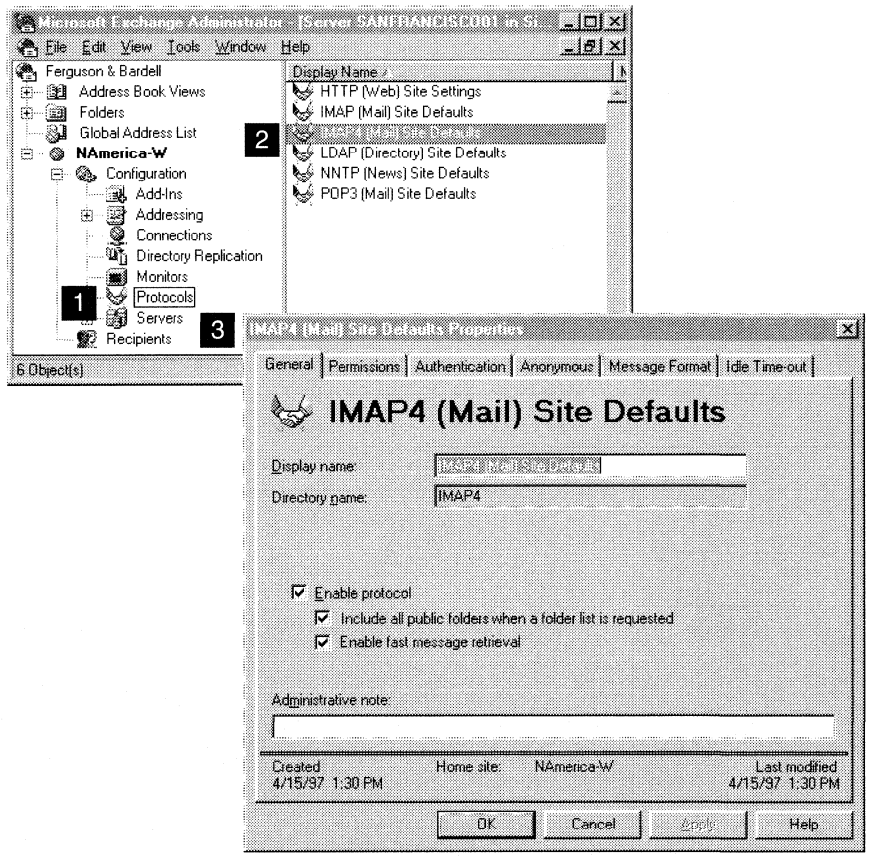
IMAP4 can be configured at the site, server, and mailbox levels:

- Site level IMAP4 protocol settings represent default values that can be inherited by servers.
- In the server IMAP4 property pages, you can use either the site defaults or configure options for each server.

- In the mailbox IMAP4 property pages, you can use either the server defaults or configure options on a mailbox-by-mailbox basis. Note, however, that if IMAP4 is disabled at the server, it is disabled for all mailboxes on that server, regardless of whether it is enabled at the mailbox level.

Getting to the IMAP4 property pages

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **IMAP4 (Mail) Site Defaults** to configure site IMAP4 defaults, or **IMAP4 (Mail) Settings** to configure a server's IMAP4 settings.



General Properties

Use the **General** property page to specify a display name for the IMAP4 object and to enable or disable IMAP4 for the site or server.

Getting to the General property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **IMAP4 (Mail) Site Defaults** to configure site IMAP4 defaults, or **IMAP4 (Mail) Settings** to configure a server's IMAP4 settings.
3. Select the **General** tab.

Defining a Display Name

Use the **General** property page to define the IMAP4 display name.

1. Select the **General** tab.
2. Type a display name.

Option	Description
Display name	A maximum of 256 alphanumeric characters, which can include spaces and special characters.
Directory name	A name defined automatically during installation that cannot be changed.

Using the Site Defaults

Use the **General** property page on the IMAP4 server object to use the default values from the IMAP4 site object.

Note This option is available only for IMAP4 properties in the server container.

1. Select the **General** tab.
2. Select or clear the **Use site defaults for all properties** check box. Select this check box to use the options you have set for permissions and message format.

Enabling or Disabling IMAP4

Use the **General** property page to enable or disable IMAP4 on the Microsoft Exchange Server computer or change the site default.

Note It can take several minutes for the change to take effect.

1. Select the **General** tab.
2. Select or clear the **Enable protocol** check box.

Disabling Public Folder Listings for the Site or Server

Some IMAP4 clients exhibit poor performance when listing a large number of public folders. By default, Microsoft Exchange Server enables public folders to be listed for all clients. Clear the **Include all public folders when a folder list is requested** check box to disable listing public folders. Disabling this option prevents listing public folders in response to the IMAP4 **LIST "" *** command and improves performance for clients that have problems listing public folders.

1. Select the **General** tab.
2. Clear the **Include all public folders when a folder list is requested** check box.

Disabling Fast Message Retrieval

Some IMAP4 clients require Microsoft Exchange Server to report exact message sizes. By default, Microsoft Exchange Server increases the speed of message retrieval by approximating message sizes. Clear the **Enable fast message retrieval** check box to disable fast message retrieval to support e-mail clients that require the reporting of exact message sizes.

1. Select the **General** tab.
2. Clear the **Enable fast message retrieval** check box.

Authentication

Use the **Authentication** property page to specify methods of *authentication* that IMAP4 clients use when connecting to Microsoft Exchange Server. Authentication is the process the IMAP4 server uses to determine whether to grant the user permission to connect to the system. By default, Microsoft Exchange Server allows an IMAP4 client to connect using any of the supported authentication methods.

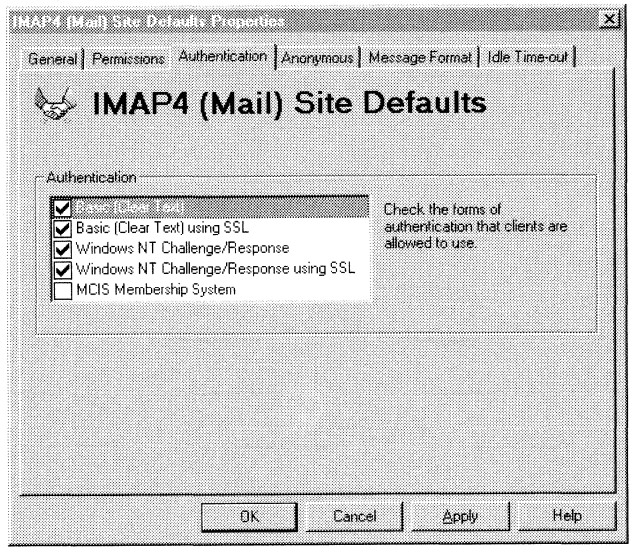
One method of authentication that you can specify is Secure Sockets Layer (SSL) encryption. SSL encrypts all data sent between clients and servers. To use SSL, Microsoft Internet Information Server (IIS) must be installed on the Microsoft Exchange Server computer before Microsoft Exchange Server is installed, and the Microsoft Exchange Server service account must be granted Administrator permissions for the local computer. In addition, you must complete the following procedure.

1. In IIS Key Manager, choose the IMAP4 icon.
2. Create a key request by choosing **Create New Key** from the **Key** menu and typing the required information.
3. Obtain a certificate from a Certificate Authority.
4. Under IMAP4, select the key request, and then choose **Install Key Certificate** from the **Key** menu.
5. Select the default server connection, or enter the server's Internet protocol (IP) address to bind the key to any inbound connection.
6. From the **Servers** menu, choose **Commit Changes Now**, and then choose **OK** to commit all the changes.

For more information about setting up SSL, see your IIS documentation.

Getting to the Authentication property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **IMAP4 (Mail) Site Defaults** to configure site IMAP4 defaults, or **IMAP4 (Mail) Settings** to configure a server's IMAP4 settings.
3. Select the **Authentication** tab.



Setting Authentication Methods

Use the **Authentication** property page to specify the authentication method an IMAP4 client uses to access information on the Microsoft Exchange Server computer. In order for an IMAP4 client to log on to the Microsoft Exchange Server computer, one of the authentication methods that the client supports must be enabled on the server. Check with your client's vendor if you are unsure of which authentication methods are available.

1. Select the **Authentication** tab.
2. In the **Authentication** box, select an authentication type.

Option	Description
Basic (Clear Text)	Enable authentication through an unencrypted user name and password. Most IMAP4 clients support this method.
Basic (Clear Text) using SSL	Use SSL protocol to encrypt clear text on port 993.
Windows NT Challenge/Response	Enable authentication through Windows NT network security and an encrypted password. This method is supported by Microsoft Outlook Express.
Windows NT Challenge/Response using SSL	Enable authentication using Windows NT network security to occur through an SSL-encrypted channel on port 993.
MCIS Membership System	Enable authentication using Windows NT network security to occur through the Microsoft Commercial Internet Server (MCIS) Membership System.

Note With Windows NT Challenge/Response and Outlook Express, it is not possible to specify the name of the Microsoft Exchange Server mailbox you want to access. By default, Microsoft Exchange Server attempts to access the mailbox with the same name as the Windows NT user account that the user is logged on as. For example, if you are logged on as Domain\Suzanf, with Windows NT Challenge/Response enabled, Microsoft Exchange Server attempts to access the mailbox called Suzanf.

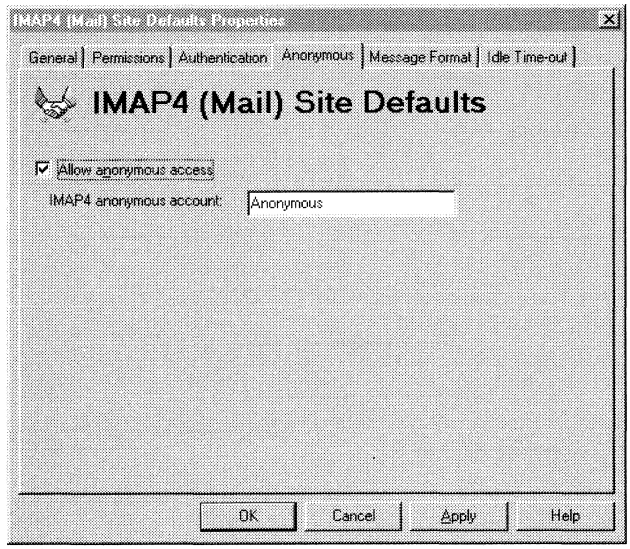
Anonymous Connections

You can specify whether IMAP4 users can connect to Microsoft Exchange Server anonymously. For example, if you want certain public folders to be accessible to users outside of your organization, you can enable anonymous connections. IMAP4 users connecting to Microsoft Exchange Server anonymously don't need a Windows NT user account to access information. Microsoft Exchange Server doesn't perform password verification; however, it does log the user's password in the Windows NT Event Log.

Note If a Microsoft Exchange Server mailbox exists on a Microsoft Exchange Server computer that uses the same alias as the anonymous IMAP4 account, the anonymous IMAP4 user can also access that mailbox.

Getting to the Anonymous property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **IMAP4 (Mail) Site Defaults** to configure site IMAP4 defaults, or **IMAP4 (Mail) Settings** to configure a server's IMAP4 settings.
3. Select the **Anonymous** tab.



Setting Anonymous Access

Use the **Anonymous** property page to specify whether IMAP4 users can connect anonymously to Microsoft Exchange Server.

Note In order for users to connect anonymously to Microsoft Exchange Server public folders, you must select the **Allow anonymous access** check box on the **Anonymous** tab. You must also grant anonymous users permissions on the public folder by using the Administrator program or Microsoft Outlook.

---

1. Select the **Anonymous** tab.
2. Select the **Allow anonymous access** check box. To specify the name of the anonymous account, type the name in the **IMAP4 anonymous account** box. The default name is Anonymous.

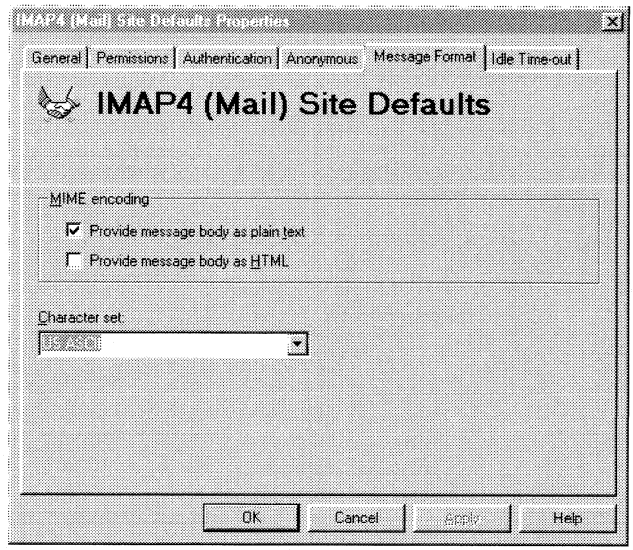
Message Format Properties

Use the settings in the **Message Format** property page to specify the format that Microsoft Exchange Server messages are converted to when they are retrieved by an IMAP4 client. These settings are based on the message format that the IMAP4 clients support when connecting to the server. The message content format and character set option can be configured for individual mailboxes, servers, and sites.

Note Messages sent by an Internet user are not converted. Instead they are retrieved by the IMAP4 client in the format that the message was originally composed in.

Getting to the Message Format property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **IMAP4 (Mail) Site Defaults** to configure site IMAP4 defaults, or **IMAP4 (Mail) Settings** to configure a server's IMAP4 settings.
3. Select the **Message Format** tab.



Specifying Message Format Options

When a user retrieves messages using IMAP4, you can specify how these messages are converted from the Microsoft Exchange Server format to various Internet mail formats.

Messaging Application Programming Interface (MAPI) clients such as Outlook are capable of multilingual support, but they compose messages using Microsoft Windows code pages instead of Internet character sets. For most languages, there is a one-to-one correspondence between the character set and the code page. If this is the case, Microsoft Exchange Server automatically assigns the correct character set that corresponds to the code page that the message was composed in. However, if multiple character sets exist for the same code page, Microsoft Exchange Server uses the character setting specified in the **Character set** box in the **Message Format** property page. If the character set is not appropriate for the code page, a default character set is used. For example, suppose a message is received that uses Japanese code page 932. That code page can be mapped to one of several character sets including JIS, Shift-JIS, and EUC. If the **Character set** box is set to Shift-JIS, that character setting will be used. However, if the **Character set** box is set to US-ASCII, Microsoft Exchange Server will use the default character set for that code page, which is JIS.

Messages that are received from the Internet already have a character set specified or will have one assigned to it when the message is received by the Internet Mail Service.

1. Select the **Message Format** tab.
2. In the **MIME encoding** box, select the appropriate options for message format.
3. In the **Character set** box, select the default character set.

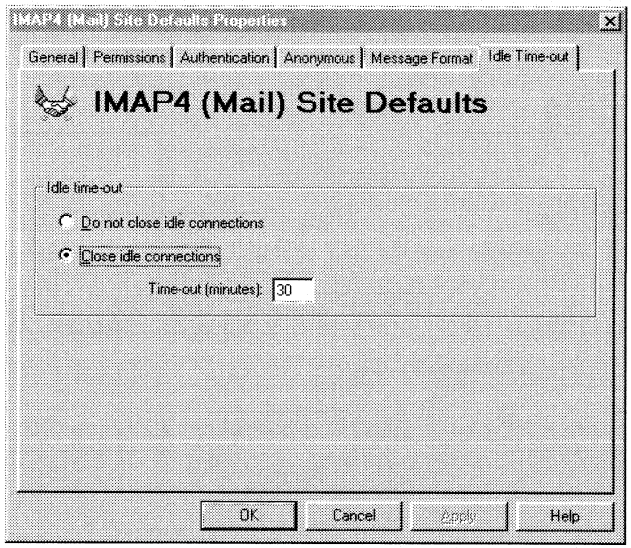
Option	Description
Provide message body as plain text	A plain text Multipurpose Internet Mail Extensions (MIME) body part is generated for the message. If **Provide message body as HTML** is also selected, Microsoft Exchange Server provides both Hypertext Markup Language (HTML) and plain text in a MIME multipart alternative message.
Provide message body as HTML	A MIME body part in HTML is generated for the message. If **Provide message body as plain text** is also selected, Microsoft Exchange Server provides both HTML and plain text in a MIME multipart alternative message. HTML is an Internet standard that enables rich-text formatting such as bold, color, and italic to appear in messages. Clients such as Outlook Express can read HTML.
Character set	The character set that is used when generating MIME messages that originate from Microsoft Exchange Server. The default character set varies according to the language installed on the server.

Idle Time-out

Use the **Idle Time-out** property page to specify how long IMAP4 connections can remain idle before they are closed.

Getting to the Idle Time-out property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **IMAP4 (Mail) Site Defaults** to configure site IMAP4 defaults, or **IMAP4 (Mail) Settings** to configure a server's IMAP4 settings.
3. Select the **Idle Time-out** tab.



Setting Idle Time-out Connections

Use the **Idle Time-out** property page to close IMAP4 connections after a specified interval of inactivity.

1. Select the **Idle Time-out** tab.
2. Select an option.

Option	Description
Do not close idle connections	Idle connections never close.
Close idle connections	Idle connections close after the time period specified in the **Time-out (minutes)** box.
Time-out (minutes)	The amount of time in minutes a connection can remain idle before being closed.

Diagnostics Logging

You can control how logging information for IMAP4 is written to the Windows NT Event Log. You can specify the types of events that are logged for IMAP4 and the level of logging information for each event. Viewing the event log for IMAP4 is useful when you are troubleshooting problems that occur.

Note Diagnostics logging is available only for IMAP4 properties in the server container.

For more information about diagnostics logging, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

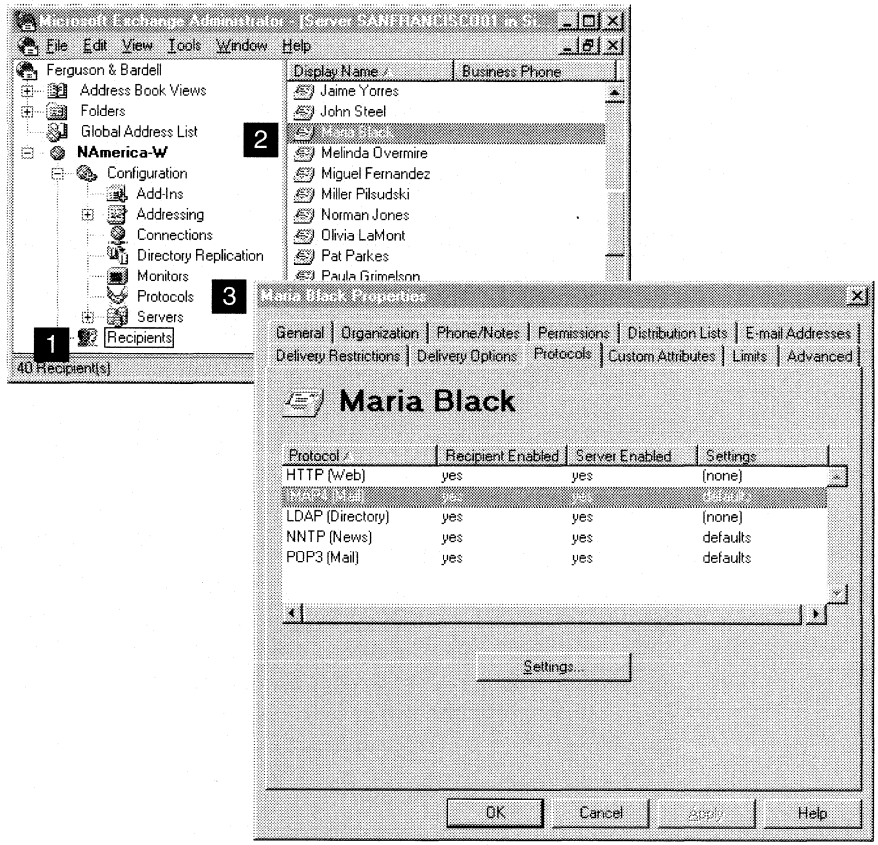
IMAP4 Mailbox Configuration

You can configure IMAP4 on a per-mailbox basis.

Note If you disable IMAP4 on the server object, IMAP4 support is also disabled for individual mailboxes. For IMAP4 to be enabled on a mailbox, it must be enabled on the server and on the mailbox.

Getting to the Protocols property page

1. In the Administrator window, choose **Recipients**.
2. Double-click the mailbox you want to configure.
3. Select the **Protocols** tab.



Enabling IMAP4 for a Mailbox

Use the **Protocols** property page to enable IMAP4 for individual mailboxes.

1. Select the **Protocols** tab.
2. Select **IMAP4 (Mail)** and choose **Settings**.
3. Select the Enable IMAP4 for this recipient check box.

Specifying IMAP4 Settings for Message Encoding

If IMAP4 is enabled on a mailbox, you can use default settings for message format. Alternatively, you can customize the settings for individual mailboxes. You can specify how text and attachments are encoded and the character set that your recipient uses.

The settings in the **Message Encoding** box determine the format that Microsoft Exchange Server messages are converted to when they are retrieved by an IMAP4 client.

Note Messages sent by an Internet user are not converted. Instead, they are retrieved by the IMAP4 client in the format that the message was originally composed in.

---

1. Select the **Protocols** tab.
2. Select **IMAP4 (Mail)** and choose **Settings**.
3. Select options for message encoding and default character sets. To use message format defaults that you set at the server level, select the **Use protocol defaults** check box. For information about these options, see "Message Format Properties" earlier in this chapter.

Disabling Public Folder Listings for a Mailbox

Some IMAP4 clients exhibit poor performance when listing a large number of public folders. By default, Microsoft Exchange Server enables public folders to be listed for all clients. Clear the **Include all public folders when a folder list is requested** check box to disable listing public folders. Disabling this option prevents listing public folders in response to the IMAP4 **LIST "" *** command and improves performance for clients that have problems listing public folders.

1. Select the **Protocols** tab.
2. Select **IMAP4 (Mail)** and choose **Settings**.
3. Clear the **Include all public folders when a folder list is requested** check box.

Enabling an IMAP4 Delegate User to View Another User's Folders

You can enable an IMAP4 delegate user to access another user's mailbox to view personal folders in the other user's mailbox.

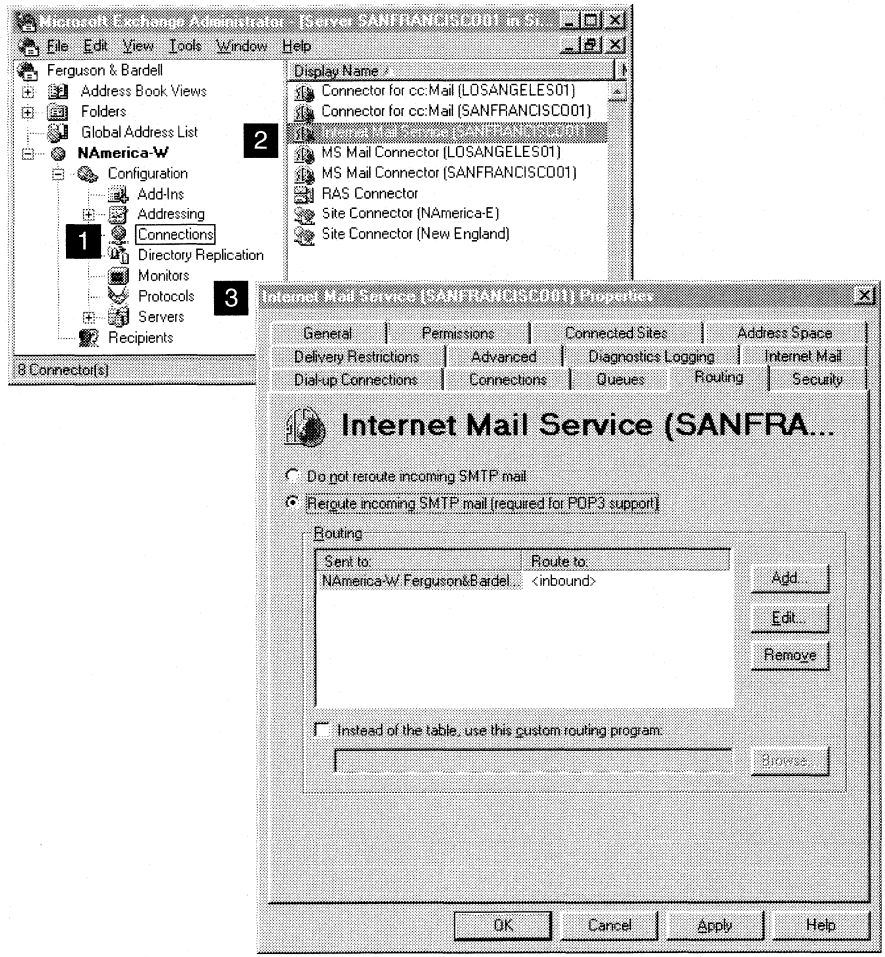
1. Select the **Protocols** tab.
2. Select **IMAP4 (Mail)** and choose **Settings**.
3. Select **User acts as a delegate**.

Internet Mail Service Configuration

You must configure the Internet Mail Service so that IMAP4 clients can send mail.

Getting to the Routing property page for the Internet Mail Service

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click the Internet Mail Service you want to configure.
3. Select the **Routing** tab.



Configuring the Internet Mail Service

Use the following procedure to configure the Internet Mail Service for IMAP4 clients.

Note If the Internet Mail Service was not configured to reroute incoming Simple Mail Transport Protocol (SMTP) mail, you may receive a non-delivery report (NDR) for any messages submitted by IMAP4 clients to recipients outside the organization. To resolve the problem, configure the Internet Mail Service, and resend the messages.

---

1. Select the **Routing** tab.
2. Select Reroute incoming SMTP mail (required for POP3/IMAP4 support) option.

3. Choose **Add**.
4. Type the SMTP domain name of your organization in the **E-mail sent to this domain** box.
5. Select the **Should be accepted as "inbound"** option.
6. Choose **OK**.
7. Stop and restart the Internet Mail Service.

IMAP4 Client Configuration

To connect to a Microsoft Exchange Server IMAP4 computer, you must specify the following information on the IMAP4 client:

- An IMAP4 account name
- An IMAP4 e-mail address
- An IMAP4 server name
- An SMTP server name

Because IMAP4 clients vary, the steps for configuring clients to connect to a Microsoft Exchange Server IMAP4 computer are different for each client. For information about how to configure the Microsoft Internet Mail IMAP4 client that is included with Outlook Express, see "Sample IMAP4 Client Configuration" later in this chapter.

Note By default, some clients, such as Outlook Express, only display folders you have subscribed to. If you do not see all of the folders after connecting to the Microsoft Exchange Server computer, you should subscribe to the folders and then refresh the folder list.

IMAP4 Account Name

An IMAP4 account name is the alias name of a Microsoft Exchange Server mailbox that supports IMAP4. For example, the alias for Suzan Fine's mailbox is SuzanF.

Because Microsoft Exchange Server uses Windows NT user accounts for authentication, it may be necessary to specify the mailbox's Windows NT domain, user account, and alias name. Performance can be improved by including the mailbox's Windows NT domain in the IMAP4 account name.

Keep the following in mind when you set up your IMAP4 client's account name:

- If a Windows NT domain and user name are specified as the IMAP4 account name, they must precede the mailbox's alias name. For example, *Windows_NT_domain\user_account_name\mailbox_alias name*.
- If only an alias name is specified as the IMAP4 account, the Microsoft Exchange Server IMAP4 computer uses a Windows NT user name that is equivalent to the alias name. All Windows NT domains are searched for the first domain that contains that Windows NT user. For example, if you specify SuzanF as the IMAP4 account, all domains are searched for the first domain that contains user *Windows_NT_domain*\SuzanF\SuzanF.

Note You can use either a "\" or a "/" as a delimiter for the IMAP4 account name. If you cannot connect using one delimiter, try using the other delimiter since some clients may have problems with these characters.

- If only a Windows NT domain and user account are specified as the IMAP4 account, the Microsoft Exchange Server IMAP4 computer uses a mailbox alias that is equivalent to the Windows NT user account. For example, specifying *domain_name*\SuzanF as the IMAP4 account is equivalent to specifying *domain_name*\SuzanF\SuzanF as the IMAP4 account.
- The IMAP4 password for the mailbox is the Windows NT user account password that is associated with the Microsoft Exchange Server mailbox.

Note With Windows NT Challenge/Response, it is not possible to specify the name of the Microsoft Exchange Server mailbox you want to access. By default, Microsoft Exchange Server attempts to access the mailbox associated with the Windows NT user account that the user is logged on as. For example, if you are logged on as Domain\Suzanf, with Windows NT Challenge/Response enabled, Microsoft Exchange Server attempts to access the mailbox called Suzanf.

IMAP4 E-mail Address

The IMAP4 e-mail address is the SMTP e-mail address that Internet users use to send messages. For example, the user's IMAP4 e-mail address could be SuzanF@FB.com.

IMAP4 Server Name

The IMAP4 server name is the computer name of the Microsoft Exchange Server computer that has the IMAP4 mailbox account that the IMAP4 client accesses.

SMTP Server Name

The SMTP server name is the name of the computer running the Internet Mail Service that provides SMTP service for the IMAP4 client.

Sample IMAP4 Client Configuration

The following example shows how to set up an IMAP4 client for a Microsoft Exchange Server user named Suzan Fine at a company called Ferguson & Bardell (FB).

Create a Microsoft Exchange Server mailbox for Suzan with SuzanF as the alias name and Exchange1 as the computer name. The primary Windows NT account that is given permissions on this mailbox is FB\SuzanF. The Internet Mail Service that is providing SMTP service to the IMAP4 accounts is also running on the Exchange1 computer. The domain name of the company is FB.com. The following options must be specified for the Microsoft Internet Mail IMAP4 client, which is included in Outlook Express:

Name Suzan Fine

Organization Ferguson & Bardell

E-mail address SuzanF@FB.com

Outgoing Mail (SMTP) server Exchange1

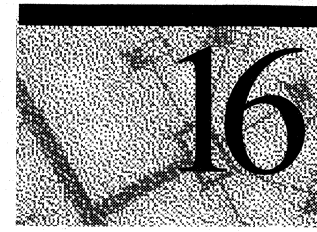
Incoming Mail (IMAP4) server Exchange1

IMAP4 account FB\SuzanF\SuzanF

Password Windows NT password for account FB\SuzanF

CHAPTER 16

LDAP



Lightweight Directory Access Protocol (LDAP) is an Internet protocol that enables users with LDAP clients to access directory information from the Microsoft Exchange Server directory. Clients with permission to use LDAP can browse, read, search, and write directory listings in the Microsoft Exchange Server directory. For example, a user can search for specific information, such as phone numbers and office locations, from any application that supports LDAP. Many LDAP clients can access a single Microsoft Exchange Server computer and perform queries for directory information such as user names and locations. With the appropriate permissions, you can modify Microsoft Exchange Server directory information with LDAP. For example, a user can use an LDAP application to modify his or her address or phone number.

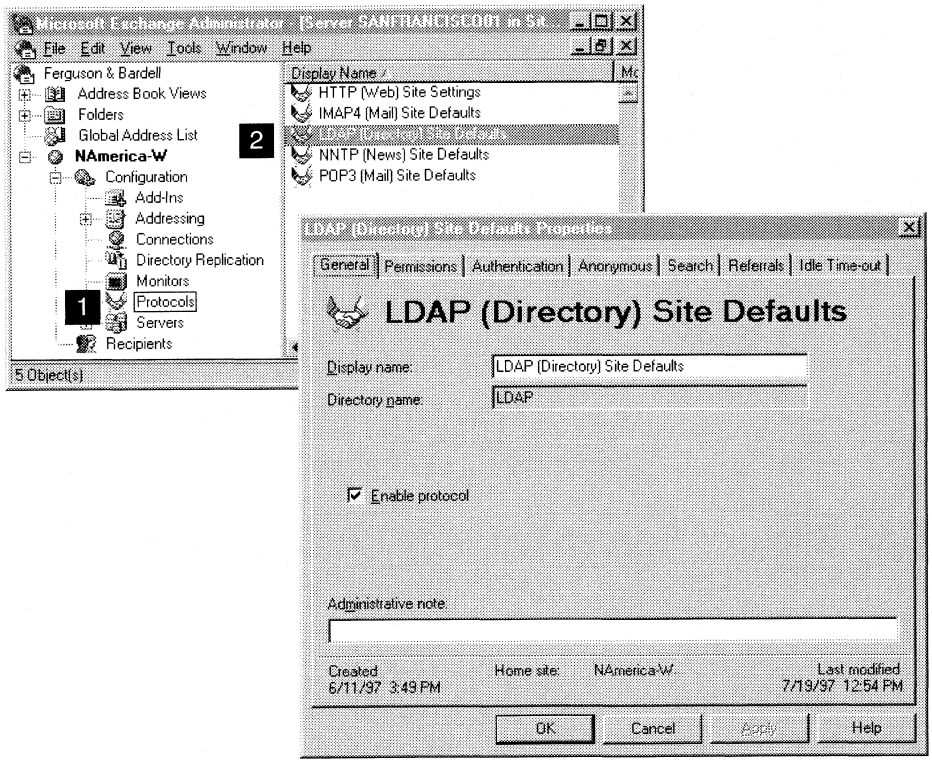
LDAP Site and Server Property Configuration

When Microsoft Exchange Server is installed, LDAP is enabled within the site by default. LDAP clients can access the directory as soon as the server is set up.

You can set properties for LDAP at either the site or server level using the Microsoft Exchange Server Administrator program. To prevent unauthorized users from accessing your organization's directory, you can configure LDAP so that users must be authenticated to connect to your server. You can also configure other LDAP properties such as anonymous connections.

Getting to the Site and Server property pages

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **LDAP (Directory) Site Defaults** to configure site LDAP defaults, or **LDAP (Directory) Settings** to configure a server's LDAP settings.



General Properties

Use the **General** property page to specify a display name for the LDAP object and to enable or disable LDAP on the Microsoft Exchange Server computer.

Getting to the General property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **LDAP (Directory) Site Defaults** to configure site LDAP defaults, or **LDAP (Directory) Settings** to configure a server's LDAP settings.
3. Select the **General** tab.

Defining a Display Name

Use the **General** property page to define the LDAP display name.

1. Select the **General** tab.
2. Type a display name.

Option	Description
Display name	A maximum of 256 alphanumeric characters, which can include spaces and special characters.
Directory name	A name defined automatically during installation that cannot be changed.

Using the Site Defaults

Use the **General** property page on the LDAP server object to use the default values from the LDAP site object.

Note This option is available only for LDAP properties in the server container.

1. Select the **General** tab.
2. Select or clear the **Use site defaults for all properties** check box.

Option	Description
Use site defaults for all properties	Select to use the options you have set for permissions and message format.

Enabling or Disabling LDAP

Use the **General** property page to enable or disable LDAP.

Note It can take several minutes for the change to take effect.

1. Select the **General** tab.
2. Select or clear the **Enable protocol** check box.

Permissions

You can assign specific permissions on the LDAP object. For more information on permissions, see *Microsoft Exchange Server Getting Started.*

Authentication

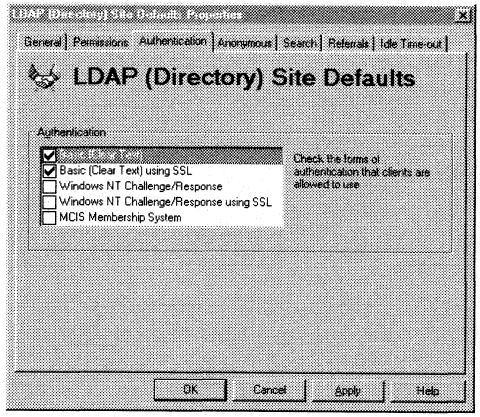
Use the **Authentication** property page to specify methods of *authentication* that LDAP clients use when connecting to Microsoft Exchange Server. Authentication is the process the LDAP server uses to determine whether to grant the user permission to connect to the system. By default, Microsoft Exchange Server allows an LDAP client to connect using any of the listed authentication methods.

One method of authentication that you can specify is Secure Sockets Layer (SSL) encryption. SSL encrypts all data sent between clients and servers. To use SSL, Microsoft Internet Information Server (IIS) must be installed on the Microsoft Exchange Server computer before Microsoft Exchange Server is installed, and the Microsoft Exchange Server service account must be granted Administrator permissions for the local computer. In addition, you must complete the following procedure.

1. In the Internet Information Server Key Manager, select the LDAP protocol icon.
2. Create a key request by choosing **Create New Key** from the **Key** menu and typing the required information.
3. Obtain a certificate from a Certificate Authority.
4. Select the key request under the LDAP protocol, and choose **Install Key Certificate** from the **Key** menu.
5. Select the default server connection, or enter the server's IP address to bind the key to any inbound connection.
6. From the **Servers** menu, choose **Commit Changes Now**, and choose **OK** to commit all the changes.

Getting to the Authentication property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **LDAP (Directory) Site Defaults** to configure site LDAP defaults, or **LDAP (Directory) Settings** to configure a server's LDAP settings.
3. Select the **Authentication** tab.



Setting Authentication Methods

Use the **Authentication** property page to specify the authentication method an LDAP client uses to access information on the Microsoft Exchange Server computer. In order for an LDAP client to log on to the Microsoft Exchange Server computer, one of the authentication methods that the client supports must be enabled on the server. Check with your client's vendor if you are unsure which authentication methods are available.

To use SSL encryption, IIS must be installed on the Microsoft Exchange Server computer.

1. Select the **Authentication** tab.
2. In the **Authentication** box, select an authentication type.

Option	Description
Basic (Clear Text)	Enable authentication through an unencrypted user name and password.
Basic (Clear Text) using SSL	Enable authentication and all client/server communication to occur through an SSL-encrypted channel on port 636. SSL is a protocol that provides secure data communication using data encryption and decryption.
Windows NT Challenge/Response	Enable authentication through Windows NT network security and an encrypted password.
Windows NT Challenge/Response using SSL	Enable authentication using Windows NT network security to occur through an SSL-encrypted channel.
MCIS Membership System	Enable authentication using Windows NT network security to occur through the Microsoft Commercial Internet Server (MCIS) Membership System.

Anonymous Connections

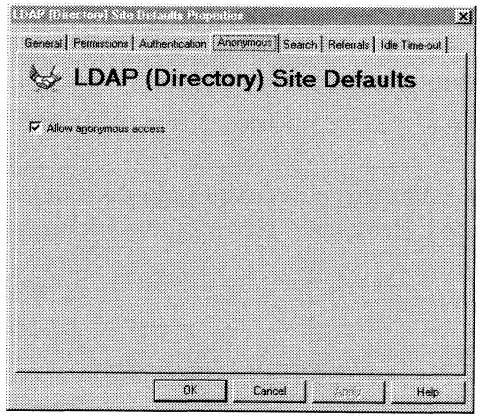
You can specify whether LDAP users can connect to Microsoft Exchange Server anonymously. If users can't connect anonymously, they can't access Microsoft Exchange Server without a valid Windows NT user account and authentication by a Windows NT Server.

You can specify which directory attributes authenticated and anonymous users can view when accessing the directory. For example, you may not want to allow anonymous users to view the manager attribute of each user in the directory. Use the **Attributes** property page on the DS Site Configuration object to set which attributes are visible to anonymous and authenticated users. Anonymous users can view a subset of attributes visible to authenticated users.

Note In order for an LDAP client to access the directory as an authenticated user, the user must provide valid Windows NT Server credentials in the following format: cn=username, cn=Windows NT domain. For example: cn=awilliams, cn=chicago. The user should also provide a password for the account. Microsoft Exchange Server also supports distinguished name representation of domain names, such as dc=domain, cn=username or cn=username, or dc=domain.

Getting to the Anonymous property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **LDAP (Directory) Site Defaults** to configure site LDAP defaults, or **LDAP (Directory) Settings** to configure a server's LDAP settings.
3. Select the **Anonymous** tab.



Setting Anonymous Access

Use the **Anonymous** property page to specify whether LDAP users can connect anonymously to Microsoft Exchange Server.

1. Select the **Anonymous** tab.
2. Select the **Allow anonymous access** check box.

Searches

LDAP allows clients to perform searches when connected to a directory. For example, if a user searches the directory for a particular user, LDAP returns the entry for that user. LDAP provides search capabilities by matching the requested information with an entry in the directory by performing substring searches. There are three types of substring searches that LDAP can perform:

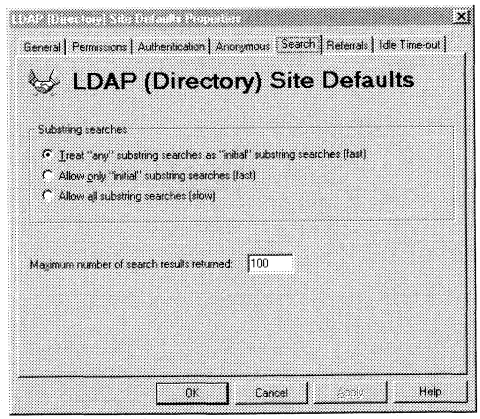
Initial substring search The directory matches the substring that the user specifies against the beginning of an attribute in the directory. For example, an initial substring search for "Sf" in a display name would return Suzan (Fine). Initial substring searches are typically faster than the other types of substring searches.

Final substring search The directory matches the substring that the user specifies against the end of an attribute in the directory. For example, an initial substring search for "ne" in a display name would return Stacey and Steve, but not Sean or Shannon. Initial substring searches are typically slower than initial substring searches.

Any substring search The directory matches the substring that the user specifies against any portion of an attribute in the directory. For example, a substring search for "r" in a display name would return Maria and Raymond. Any substring searches are the slowest substring searches.

Getting to the Searches property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **LDAP (Directory) Site Defaults** to configure site LDAP defaults, or **LDAP (Directory) Settings** to configure a server's LDAP settings.
3. Select the **Search** tab.



Specify Substring Searches

Use the **Search** property page to specify how LDAP will perform directory searches on client requests.

1. Select the **Search** tab.
2. Select an option.

Option	Description
Treat "any" substring searches as "initial" substring searches (fast)	Specifies that only initial substring searches will be performed. Final substring searches will not be performed, and any substring searches are converted to initial substring searches (which will return partial but sometimes incomplete results).
Allow only "initial" substring searches (fast)	Specifies that only initial substring searches will be performed. Final substring searches and any substring searches will not be performed.
Allow all substring searches (slow)	Specifies that all substring searches will be performed, including initial, any, or final substring searches.
Maximum number of search results returned	Specifies the maximum number of entries that will be returned for all searches. Performance decreases as this number increases. If more than the maximum number of specified results are found in an LDAP search, Microsoft Exchange Server does not return any results for the search. If no number is specified, a default of 100 is used for the number.

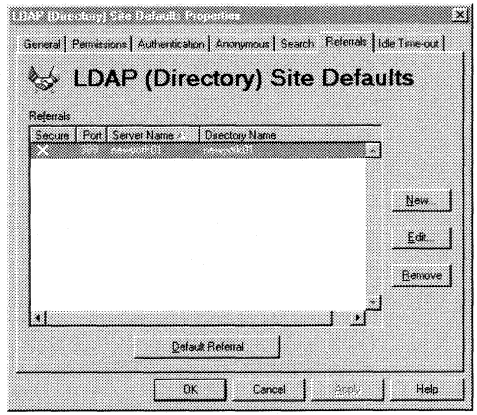
Referrals

If an LDAP client requests information that your Microsoft Exchange Server computer doesn't have, you can configure your server to refer the client to another server that can fulfill the request. For example, if a client searches on server A for the telephone number for John Baker, but John Baker is in another organization, server A tells the client to request the information from a server in John Baker's organization. You can use the **Referrals** property page to specify the server outside of your organization that an LDAP client connects to for information.

Note Clients can only be referred to servers outside the local Microsoft Exchange Server organization.

Getting to the Referrals property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **LDAP (Directory) Site Defaults** to configure site LDAP defaults, or **LDAP (Directory) Settings** to configure a server's LDAP settings.
3. Select the **Referrals** tab.



Adding a Referral

You can specify a server that is used to provide information that a client requests.

1. Select the **Referrals** tab.
2. Choose **New**.

Option	Description
Server Name	The Domain Name System (DNS) name of the server that is used for the referral, for example, server.fab.com.
Directory Name	The base directory name (specified in RFC 1779 format) that is used to generate a referral, for example, ou=exchange,o=fab,c=us.
Port	The port number used to connect to the other server.
Connect over SSL	Specifies whether the connection to the other server occurs using an SSL port.

Setting a Default Referral

You can specify a server that is used by default when directory information is not found on the Microsoft Exchange Server computer the client is connected to.

1. Select the **Referrals** tab.
2. Under **Referrals**, select the referral server.
3. Choose **Default Referral**.

Modifying a Referral

You can edit information about a referral server.

1. Select the **Referrals** tab.
2. Choose **Edit.**

Removing a Referral

If you no longer want to refer clients to a server, you can delete the server from the list of referral servers.

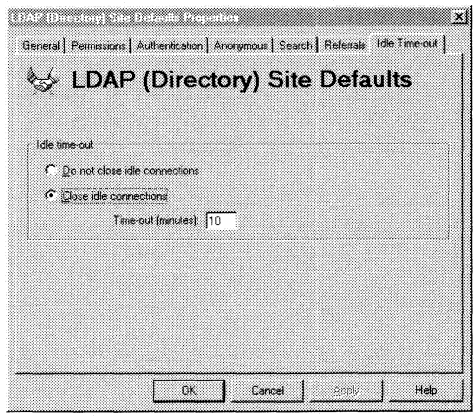
1. Select the **Referrals** tab.
2. Choose **Remove**.

Idle Time-out

Use the **Idle Time-out** property page to specify how long LDAP connections can remain idle before they are closed.

Getting to the Idle Time-out property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **LDAP (Directory) Site Defaults** to configure site LDAP defaults, or **LDAP (Directory) Settings** to configure a server's LDAP settings.
3. Select the **Idle Time-out** tab.



Setting Idle Time-out Options

Use the **Idle Time-out** property page to close LDAP connections after a specified interval of inactivity.

1. Select the **Idle Time-out** tab.
2. Select an option.

Option	Description
Do not close idle connections	Idle connections never close.
Close idle connections	Idle connections close after the time period specified in the **Time-out (minutes)** box.
Time-out (minutes)	The amount of time in minutes a connection can remain idle before being closed. The default is 10 minutes.

CHAPTER 17

NNTP



Microsoft Exchange Server enables Microsoft Outlook users to participate in online discussions across the Internet using Network News Transfer Protocol (NNTP) newsgroups. It also enables users running client applications that support NNTP to access newsgroup public folders made available on Microsoft Exchange Server computers. Newsgroup public folders are public folders that are accessible as NNTP newsgroups.

Users can read and post items, such as messages and documents, to NNTP newsgroups, which are represented in Microsoft Exchange Server as public folders. For example, scientists can exchange research information by posting messages to a newsgroup public folder for their area of interest. Other scientists around the world can then read and respond to the items in the newsgroup. Items in newsgroups can be replicated to USENET host computers in newsfeeds.

The Internet News Service is responsible for providing users with access to newsgroups. It uses NNTP commands to define the communication between hosts. NNTP is an application protocol that is used over Transport Control Protocol/Internet Protocol (TCP/IP) networks and defines a client/server command set for access to newsgroups.

Before installing the Internet News Service and setting up a newsfeed, you should become familiar with how to use and plan your newsfeed. For more information, see *Microsoft Exchange Server Concepts and Planning*.

How the Internet News Service Works

The Internet News Service is a Windows NT service that provides both uni-directional and bi-directional newsfeeds so Outlook users can send messages to and receive messages from the Internet. The Internet News Service needs to be running only on the Microsoft Exchange Server computer that is configured for newsfeeds. The Internet News Service does not need to be running on the Microsoft Exchange Server computer in order for NNTP clients to access newsgroup public folders on that server.

The Internet News Service works with the information store to provide newsgroups. It connects to other hosts on a scheduled basis to send push feeds or perform pull feeds. (For information about types of newsfeeds, see "Newsfeeds" later in this chapter.) The public information store handles all incoming connections from clients and accepts push feeds from other host computers.

The Internet News Service can use either a dedicated or a dial-up connection to communicate with host computers on the Internet. When users post items to newsgroup public folders, the Internet News Service can send the items to an Internet newsfeed provider or another organization that has servers running NNTP. It can also receive newsfeeds from these host computers so Outlook users can read items posted by other users on the Internet.

Newsgroup public folders on Microsoft Exchange Server computers can be accessed by Outlook and any third-party newsreader applications that support NNTP, such as Microsoft Internet News or FreeAgent. Third-party newsreaders can read and post items to newsgroup public folders just as they would in Outlook.

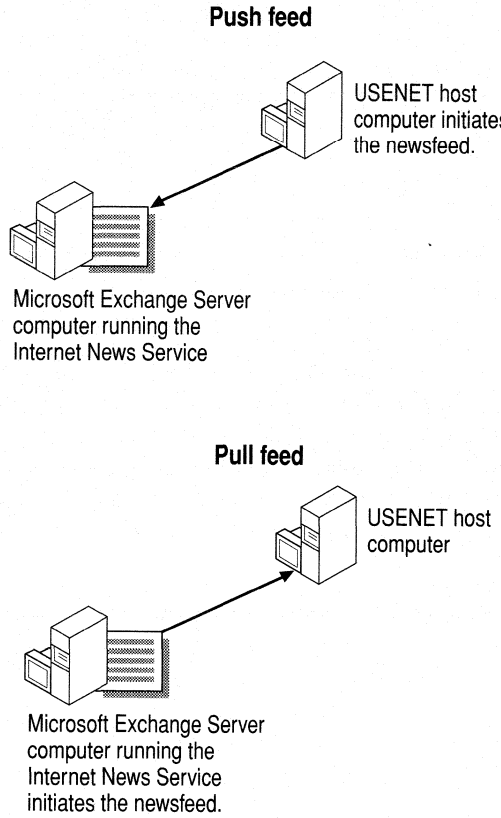
You can configure multiple newsfeeds from multiple sources on one or more Microsoft Exchange Server computers. For example, your server can receive a newsfeed from one newsfeed provider for all newsgroups in the alt hierarchy and another newsfeed from another provider for all newsgroups in the rec hierarchy. However, newsfeeds should not overlap; the same newsgroup shouldn't be fed from two different newsfeed providers. If users in two different sites want to access some of the same newsgroups, the common newsgroup public folders should be replicated from one site to another instead of using different newsfeeds for both. Feeding the same newsgroup from multiple different providers causes redundant replication of each message in the newsgroup, which increases network traffic.

Newsfeeds

You can configure the news service to support multiple newsfeeds through either *push feeds* or *pull feeds*. With a push feed, your provider's host computer initiates newsfeeds to your Microsoft Exchange Server computer. Push feeds are better than pull feeds for handling large newsfeeds. However, a push feed requires more interaction between you and your newsfeed provider because your provider controls which newsgroups you receive.

With a pull feed, your Microsoft Exchange Server initiates connections and delivers messages to host computers in your provider's site. Pull feeds also check for new messages and retrieve them. Pull feeds work well for small newsfeeds and over dial-up connections.

The following illustration shows the difference between push and pull feeds.



You can configure inbound and outbound newsfeeds as follows:

Inbound newsfeeds

- You can pull messages from your provider's host computer.
- You can accept messages that your host pushes to your Microsoft Exchange Server computer.

Outbound newsfeeds

- You can push (or send) messages posted to newsgroup public folders to your provider's host computer.
- If a host computer needs to pull messages from your Microsoft Exchange Server computer, you need to configure only NNTP client support on your computer. The host computer can then pull messages and act as though it is an NNTP newsreader.

Newsgroup Public Folders

You can designate any public folder as a newsgroup public folder that can be accessible to NNTP clients and send and receive items in a newsfeed. Outlook users can access these newsgroups just as they would any other public folder. However, now users can exchange information with people around the world and within their organization.

When you set up the Internet News Service, it creates a public folder for Internet newsgroups called Internet News. You can move or rename the Internet News public folder, but you can't delete it. You can also designate other public folders to contain newsgroup public folders.

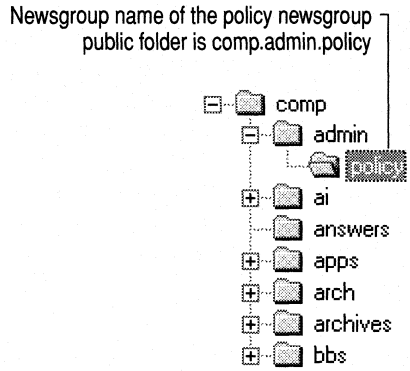
A newsgroup public folder is like any other Microsoft Exchange Server public folder. The administrator can set permissions on public folders to control who can read and post items to the newsgroup. Newsgroup public folders can also be replicated within an organization using Microsoft Exchange Server public folder replication. Any public folder that is replicated to another server retains its newsgroup properties and can be included in newsfeeds if a news service is running on that server. However, other news services cannot feed items into or from the folder.

To replicate newsgroup public folders that are included in newsfeeds, the Microsoft Exchange Server computer that is running the Internet News Service and is configured for newsfeeds must have local replicas of newsgroup public folders. When new items are posted to a replica of a newsgroup public folder, the change is replicated to the server running the Internet News Service. This server is then responsible for uploading the changes to the newsfeed provider's host computer.

Naming Newsgroup Public Folders

To enable NNTP clients to access newsgroup public folders, newsgroup public folders are assigned names that are based on their location within the newsgroup hierarchy. A hierarchy is any top-level newsgroup public folder in the tree. Public folders can't be newsgroups unless their parent folders are newsgroup hierarchies.

A newsgroup public folder inherits a portion of its name from its parent folder. The full newsgroup name of the folder is a combination of the public folder's name and the name of its parent folders, each separated by a period. For example, in the following illustration, if a newsgroup public folder called policy is in the comp.admin hierarchy, the newsgroup name of the policy newsgroup public folder is comp.admin.policy.



Note The name of a public folder cannot contain any periods because the name will conflict with the newsgroup name for the public folder. For example, a newsgroup public folder cannot be named new.ads. If an unsupported character such as a period is used, Microsoft Exchange Server replaces it with a dash.

Using Moderated Newsgroups

Some newsgroups are moderated, which means that all items posted to the folder are first mailed to a designated moderator who decides whether to accept or reject the posting. Items sent to moderated newsgroup public folders do not appear in the public folder until the moderator has accepted them. If a newsgroup is moderated, the Internet News Service automatically forwards the posted item to a specified address without modifying the heading. You can designate a moderator for a newsgroup public folder using Outlook.

Using the Internet News Service

You can use the Administrator program to manage newsgroup public folders, process NNTP control messages, and catch up to current newsfeeds if your server falls behind the current newsfeeds sent from your provider.

Managing Newsgroup Public Folders

The public folder hierarchy structure gives you flexibility in managing your newsgroup public folders. For example, you can make public folders in an existing public folder tree into newsgroups by designating the parent folder as a *newsgroup hierarchy*. All public folders underneath the parent folder also become newsgroup public folders. For more information, see "Setting Up Newsgroup Hierarchies" later in this chapter.

Because newsgroup public folder names depend on the newsgroup public folder's location within the hierarchy, newsgroup public folders cannot be moved once they have been created. However, you can move hierarchies underneath other hierarchies. If you move a hierarchy and its subfolders underneath another hierarchy, the folders in the relocated hierarchy retain their newsgroup names. They do not inherit the newsgroup name of the hierarchy they are underneath. For example, if the comp hierarchy is moved underneath the activities hierarchy, the names of newsgroup public folders in the comp hierarchy do not change.

Understanding Control Messages

NNTP host computers use *control messages* to communicate with each other. Control messages are commands that are used to create and remove newsgroups or cancel messages that have already been posted. For example, if a new newsgroup has been created, the host providing the newsfeed sends a control message to hosts receiving the newsfeed, indicating that a new newsgroup has been created. The Internet News Service then uses this information to determine whether a new newsgroup public folder should be added to the public folder hierarchy.

Microsoft Exchange Server uses three types of control messages.

Control message	Description
NEWGROUP	Broadcasts that a new group has been created.
RMGROUP	Broadcasts that a group has been removed.
Cancel	Broadcasts a request to delete a single item posted to a newsgroup.

When Microsoft Exchange Server receives NEWGROUP and RMGROUP control messages, it queues them until you decide whether to accept the messages. If you don't trust a particular USENET host, you can delete the control messages from the host without accepting the changes. If you accept a NEWGROUP control message, the Internet News Service creates a public folder for the new newsgroups. If you accept an RMGROUP control message, the Internet News Service deletes the public folder for the deleted newsgroup.

Cancel control messages are processed transparently when an item in a newsgroup is deleted. The Internet News Service accepts Cancel control messages only after it has verified that the user deleting the item is in the organization's global address list and that the control message originated from that organization. Microsoft Exchange Server also generates its own Cancel control messages when an item is deleted from a newsgroup public folder.

Catching Up to Current Newsfeeds

Because the volume of items transmitted daily in newsfeeds is considerable, USENET hosts must be able to keep up with the constant flow of data. If, for some reason, a host cannot process new items posted to newsgroups quickly enough, it can fall behind. The longer items are backed up waiting for the host to process them, the harder it is for the host to catch up.

The Internet News Service allows you to mark all items posted to newsgroups as delivered so hosts receiving the newsfeed can catch up to the most current newsfeed. Marking all messages as delivered enables hosts to flush their queues of newsgroup items waiting to be sent to other hosts. This is equivalent to deleting the items posted to newsgroups before they are delivered.

The Internet News Service enables Microsoft Exchange Server computers to catch up regardless of whether they are configured for push or pull feeds. For example, if your Microsoft Exchange Server computer is configured for push feeds and the host computer that receives your newsfeeds didn't process your feeds for several days, you can flush the queue of newsgroup postings waiting to be sent to the host. This enables the other host to ignore any old postings and process only the most recent postings.

When it performs a pull feed, Microsoft Exchange Server retrieves only messages that were posted since the last time Microsoft Exchange Server connected to the host. Microsoft Exchange Server also saves the time of that connection. The next time it connects to the host, it retrieves messages posted only since the saved time.

Setting all messages as delivered on a Microsoft Exchange Server computer configured for pull feeds not only flushes queued messages, it also resets the baseline time for future connections. This is useful if your server falls behind in processing newsfeeds received from other hosts. Instead of requesting information about items posted during the last several hours when it connects to other hosts, the Internet News Service requests information about items posted since the current time. Although no items are actually sent during this initial connection, the next time the Internet News Service connects to that host, it uses the previous time as the base for the request. For example, the first time the Internet News Service connects to a host, it requests all postings since the current time, for example 5 P.M. No postings are actually sent until several hours later when the Internet News Service connects to the host again and requests all postings since 5 P.M.

Contacting Your Newsfeed Provider

Before you configure your newsfeed, you must contact an Internet newsfeed provider and subscribe to a USENET newsfeed. Your newsfeed provider will ask you for the following information:

- The Fully Qualified Domain Name (FDQN) or Internet protocol (IP) address of the Microsoft Exchange Server computer that is running the Internet News Service. For example, your server's FDQN might be myserver.mycompany.com.
- Whether you plan to use a push feed or pull feeds for inbound messages and outbound messages. In general, you should use push feeds if you plan to receive large newsfeeds over a local area network (LAN) connection. You should use pull feeds if you plan to receive smaller newsfeeds, and you'll be connecting to your newsfeed provider's host computer using a dial-up connection.
- (Optional) The inbound host account and password if you want to make your system more secure. Your newsfeed provider's host computer can use this information to log on to your Microsoft Exchange Server computer.

When you contact your newsfeed provider, you should ask the following questions:

- What is the host computer's FDQN or IP address? Note that there can be multiple host computers.
- How should you access your newsfeed provider's *active file*? An active file is a file that contains a list of all the newsgroups you can subscribe to through your newsfeed provider. Will your newsfeed provider send it to you (typically through e-mail or File Transfer Protocol) or should you download it directly from the host computer?
- Does your newsfeed provider require the use of secure connections? If so, your newsfeed provider must give you a host account and password, which your Microsoft Exchange Server computer will use to log on to your provider's host computer.

Internet News Service and Newsfeeds

To set up the Internet News Service and newsfeeds, you must run the Newsfeed Configuration Wizard. After you have set up the Internet News Service and newsfeeds, you can customize properties on these objects.

For more information about configuring NNTP properties, see Chapter 13, "Internet Protocols."

Typical Configuration Scenarios

You have a variety of options for setting up the Internet News Service. The following are guidelines for configuring and using the Internet News Service in different scenarios.

Scenario 1

Following are the tasks you must complete using the Newsfeed Configuration Wizard if you want to receive a push newsfeed from your newsfeed provider.

- Configure the Internet News Service to push outbound newsfeeds, and accept inbound push newsfeeds.

Note To configure an inbound and outbound newsfeed, configure one bi-directional newsfeed. Problems can occur if you configure separate inbound and outbound feeds.

- Download or import the active file from your newsfeed provider, and create newsgroups.
- Select which public folders you want to push outbound to the newsfeed provider, or specify which public folders will accept the push feed from the newsfeed provider.

Scenario 2

Following are the tasks you must complete using the Newsfeed Configuration Wizard if you want to pull newsgroups from a newsfeed provider.

- Download or import the active file from your newsfeed provider.
- Specify which newsgroups you want to pull. If the newsgroup public folders have not been created, the Internet News Service creates them.
- Select which public folders you want to push outbound to the newsfeed provider, or specify which public folders will accept the push feed from the newsfeed provider.

Scenario 3

Following are the tasks you must complete using the Newsfeed Configuration Wizard if you want to set up a push feed to send to another company.

- Configure the Internet News Service to push outbound newsfeeds, and accept inbound push newsfeeds.
- Select which public folders you want to push outbound to the newsfeed provider, or specify which public folders will accept the push feed from the newsfeed provider.

Configuring an NNTP Newsfeed

The Newsfeed Configuration Wizard makes it easy for you to create one or more newsfeeds on a Microsoft Exchange Server computer. The display name for any newsfeeds you create is based on the name of the newsfeed provider and your server's name.

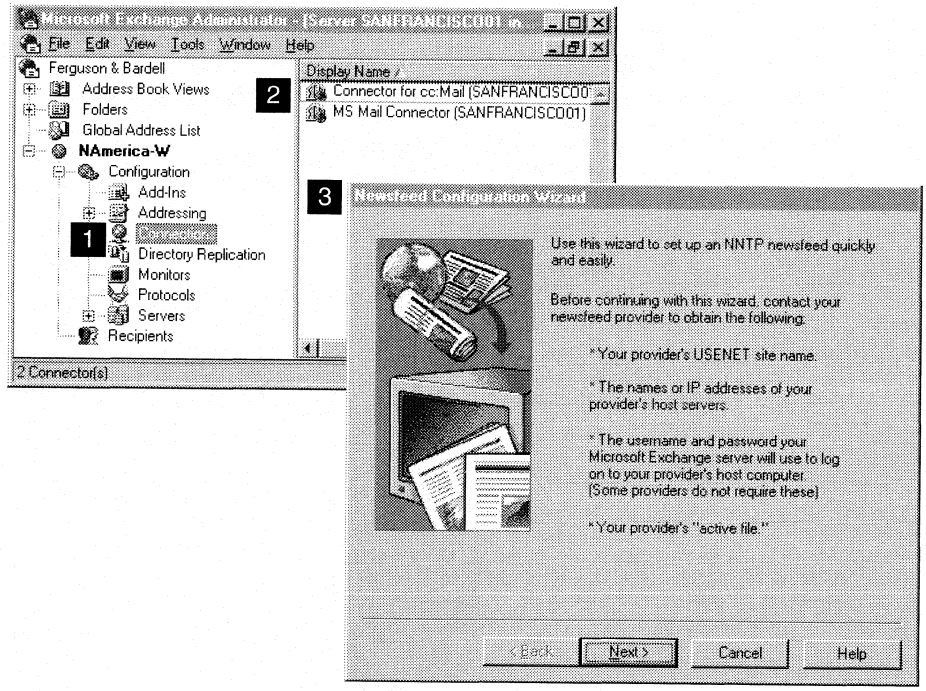
When you run the Newsfeed Configuration Wizard, you must provide the following information:

- The USENET site name of the newsfeed provider that is supplying the newsfeed. This is the value used in the path header for newsgroup messages. It is typically the FDQN of the host computer that is sending the newsfeed.
- The mailbox name of the administrator who can add and remove newsgroup public folders.

- The name and location of the active file if it will not be downloaded from your newsfeed provider's host computer.

Getting to the Newsfeed Configuration Wizard

1. In the Administrator window, choose a site, and then choose **Connections**.
2. From the **File** menu, choose **New Other**.
3. Choose **Newsfeed**.



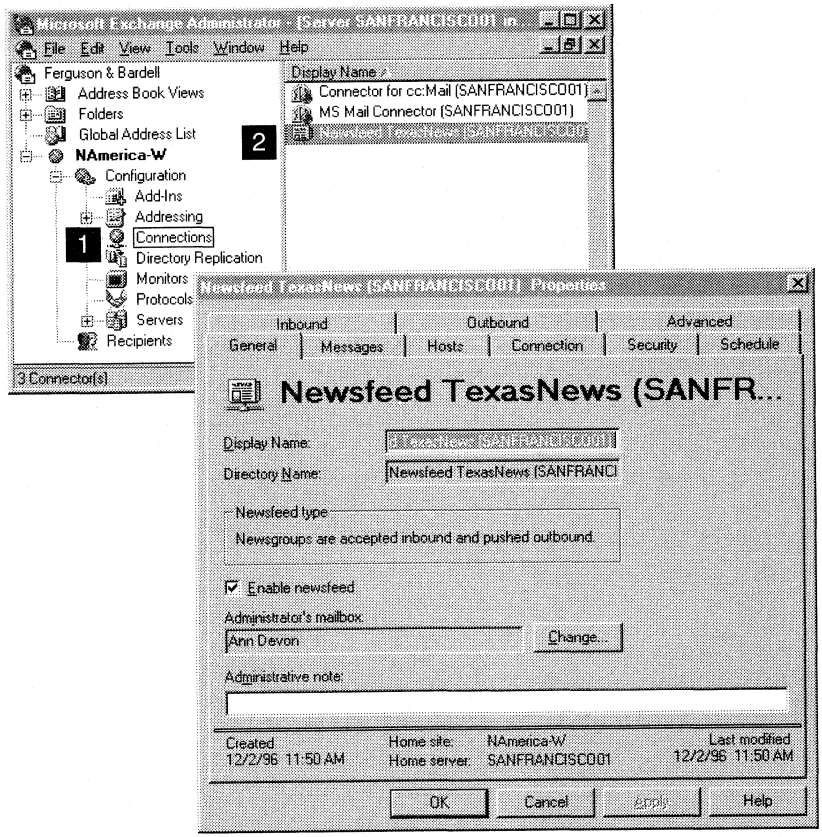
For information about options in the wizard, see Help.

Configuring Newsfeed Properties

Once you have created a newsfeed, you can set additional properties. For example, you can configure different newsgroups in your newsfeed.

Getting to the Newsfeed property pages

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.



General Properties

Use the **General** property page to enable the selected newsfeed, specify a display name for the newsfeed, and view the directory name.

Getting to the General property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **General** tab.

Defining a Display Name

Use the **General** property page to define the newsfeed display name.

1. Select the **General** tab.
2. Type a display name.

Option	Description
Display Name	A maximum of 256 alphanumeric characters, which can include spaces and special characters.
Directory Name	A name defined during installation that cannot be changed.

Enabling a Newsfeed

Use the **General** property page to enable the selected newsfeed.

1. Select the **General** tab.
2. Select the **Enable newsfeed** check box to enable the selected newsfeed to send or receive newsgroup items.

Assigning an Administrator's Mailbox

Use the **General** property page to assign an administrator's mailbox. The owner of the mailbox is the administrator who can add and remove newsgroup public folders.

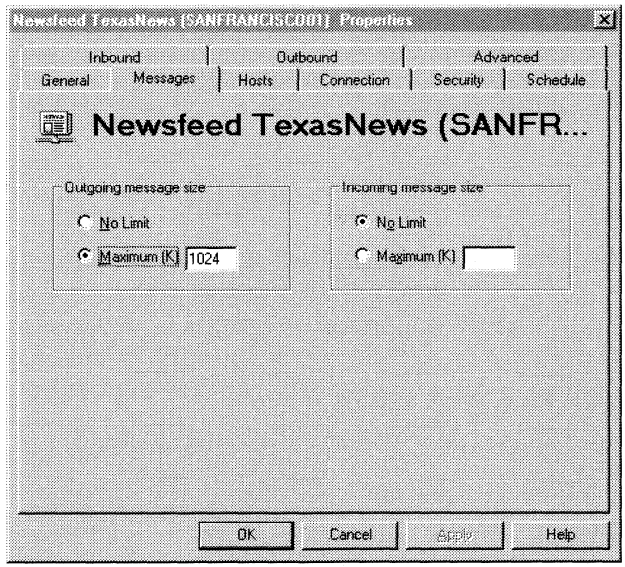
1. Select the **General** tab.
2. Choose **Change**, and then select the mailbox of the user who will administer the newsgroup public folders.

Message Size Limits

Use the **Messages** property page to specify the maximum incoming and outgoing message size in your newsfeed.

Getting to the Messages property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **Messages** tab.



Setting a Message Size Limit

You can set a limit on the size of messages that can be sent to or from this newsfeed server.

1. Select the **Messages** tab.
2. Under **Outgoing message size** or **Incoming message size**, select an option.

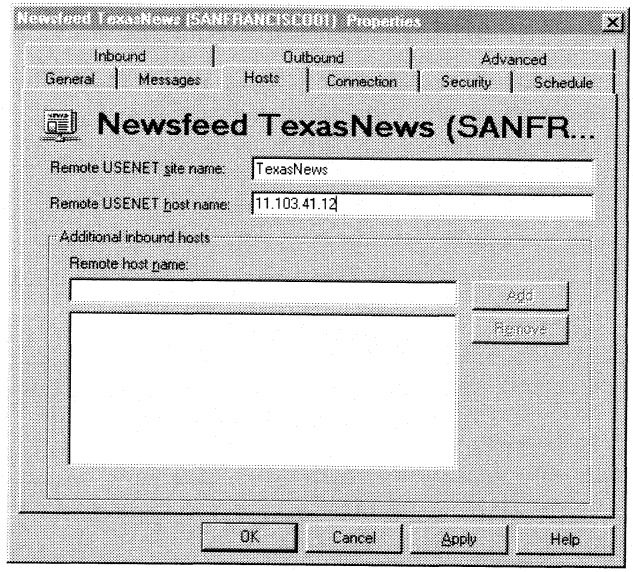
Option	Description
No Limit	There is no size limit for the message.
Maximum (K)	Select and type a number representing the largest amount of space each message can occupy.

Hosts

Hosts are the NNTP computers that your newsfeed provider supplies. Typically, you receive newsfeeds from an inbound host computer and send newsgroup postings to an outbound host. The inbound and outbound host computers can be the same.

Getting to the Hosts property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.



Connecting to the Remote USENET Site

If your server initiates connections, you must connect your newsfeed to the remote USENET site by specifying its USENET site name. Your Internet News Service can either push messages outbound to the remote USENET site or accept inbound push messages from this site.

1. Select the **Hosts** tab.
2. In the **Remote USENET site name** box, type the name of the remote USENET site that is providing your newsfeed.

Specifying the Remote USENET Host

You must specify the IP address of the USENET host computer that is providing your newsfeed. For connections to computers on the Internet, the name must be the IP address or the FDQN of the host computer, such as myserver.mycompany.com.

1. Select the **Hosts** tab.
2. In the **Remote USENET host name** box, type the FDQN or IP address of the remote USENET host that is providing your newsfeed.
3. Choose **Add**.

Setting Up Additional Inbound Hosts

You can set additional host names or IP addresses to use for inbound connections to receive newsgroups. This option is necessary only for accepting push feeds from a newsfeed provider that uses multiple hosts.

1. Select the **Hosts** tab.
2. In the **Remote host name** box, type the FDQN or IP addresses of the remote USENET hosts that are providing your newsfeed.

Removing an Inbound Connection

When you no longer want to receive newsgroups from a host computer, you can remove the host from the list of hosts supported for inbound connections.

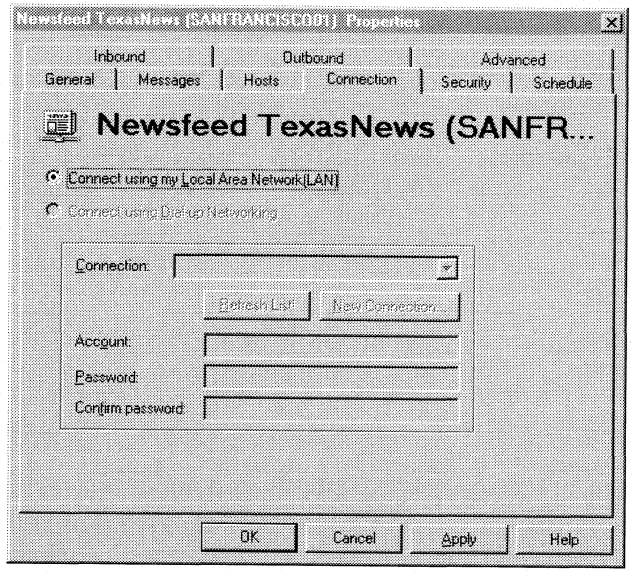
1. Select the **Hosts** tab.
2. In the **Remote host name** box, select the host name or IP address you want to remove.
3. Choose **Remove**.

Connection

Use the **Connection** property page to specify whether to use a dedicated or dial-up connection when your Microsoft Exchange Server connects to the remote USENET host.

Getting to the Connection property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **Connection** tab.



Configuring the Newsfeed to Use a LAN Connection

You can configure your Internet News Service to use a LAN connection to connect to your newsfeed provider's host computer.

1. Select the **Connection** tab.
2. Select **Connect using my Local Area Network (LAN)**.

Configuring the Newsfeed to Use a Dial-up Connection

You can configure your Internet News Service to use a dial-up connection to connect to your newsfeed provider's host computer.

Note Dial-up connections can be shared with the Internet Mail Service on the same Microsoft Exchange Server computer.

1. Select the **Connection** tab.
2. Select Connect using Dial-up Networking.
3. In the **Connection** box, select the dial-up connection you want to use.

Option	Description
Refresh List	Updates the list in the **Connection** box with the most current connections.
New Connection	Adds a new dial-up connection to the list of connections. After adding a new connection, choose **Refresh List** to display the new connection in the list.
Account	The account name for the dial-up connection. This is optional.
Password	The password for the dial-up connection. This is optional.
Confirm password	Verifies that the password is correct.

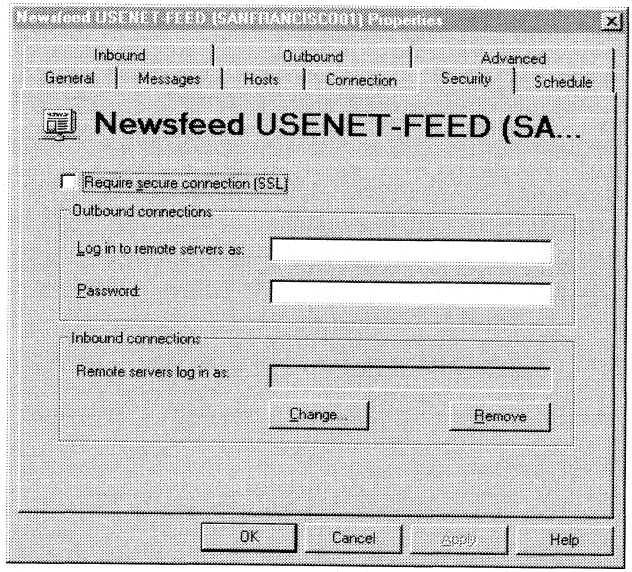
Security

By default, security is not enabled for NNTP newsfeeds. However, you can specify the account and password that your Microsoft Exchange Server computer uses to log on to remote servers and the account that the remote servers use to log on to your server. You can also set your Microsoft Exchange Server computer so that it requires Secure Sockets Layer (SSL) to be used when communicating with other servers. SSL is a protocol that encrypts all data sent between NNTP servers.

Microsoft Exchange Server provides several additional options to improve the security of connections. For more information, see "Authentication" later in this chapter.

Getting to the Security property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **Security** tab.



Requiring Secure SSL Connections

You can configure your Microsoft Exchange Server computer to require remote host computers to use SSL encryption when connecting to Microsoft Exchange Server. If Microsoft Exchange Server is configured to require SSL, SSL is used when other hosts initiate push feeds to Microsoft Exchange Server. It is also used when Microsoft Exchange Server initiates push and pull feeds to other hosts. In order for a remote host to log on to the Microsoft Exchange Server computer using SSL, SSL must be enabled on both servers.

To use SSL, Microsoft Internet Information Server (IIS) must be installed on the Microsoft Exchange Server computer before Microsoft Exchange Server is installed, and the Microsoft Exchange Server service account must be granted Administrator permissions for the local computer. In addition, you must complete the following procedure.

1. In the Internet Information Server Key Manager, choose the NNTP protocol icon.
2. Create a key request by choosing **Create New Key** from the **Key** menu, and type the required information.
3. Obtain a certificate from a Certificate Authority.
4. Under the NNTP protocol, select the key request, and then choose **Install Key Certificate** from the **Key** menu.
5. Select the default server connection or type the server's IP address to bind the key to any inbound connection.

For information about setting up SSL, see your IIS documentation.

Complete the following steps to require SSL connections for this newsfeed.

1. Select the **Security** tab.
2. Select **Require secure connection (SSL)**.

For more information about setting up SSL, see your Internet Information Server documentation.

Setting Up an Account and Password for Outbound Connections

You can set the account and password for all outbound host connections. Your Microsoft Exchange Server computer uses this account and password to connect to your newsfeed provider's host computer. The account name and password are supplied by your newsfeed provider.

Note The account name and password for outbound host connections are case-sensitive.

---

1. Select the **Security** tab.
2. In the **Log in to remote servers as** box, type the account name.

   If the remote server is running Windows NT Server, you should specify the domain and user name in this box, for example, Domain\suzanf.
3. In the **Password** box, type the password.

Setting Up a Mailbox or Custom Recipient for Inbound Connections

You can specify the Microsoft Exchange Server mailbox or custom recipient that your newsfeed provider's host computer uses to log on to your Microsoft Exchange Server computer.

Note The password for inbound host connections is case-sensitive.

1. Select the **Security** tab.
2. Under **Inbound connections**, choose **Change**.
3. Select the Microsoft Exchange Server mailbox or custom recipient that will be used to authenticate remote servers that log on to your Microsoft Exchange Server computer.

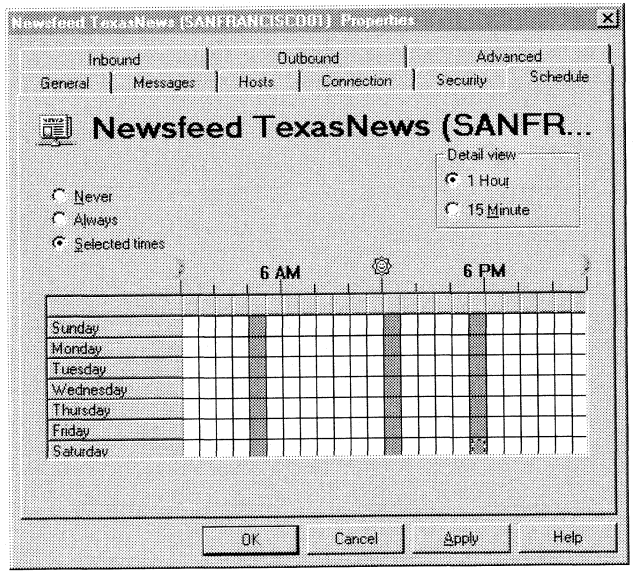
   If you do not specify a mailbox or custom recipient, no authentication is required for hosts to connect to your server.

Schedule

Use the **Schedule** property page to specify when your Microsoft Exchange Server computer will connect to the remote USENET site to send and retrieve new information.

Getting to the Schedule property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **Schedule** tab.



Setting the Connection Schedule

Depending on your organization's requirements, select time periods that best fit your users' needs to view current information.

1. Select the **Schedule** tab.
2. Select **Never**, **Always**, or **Selected times**.
3. If you chose **Selected times**, under **Detail view**, select a view for the schedule grid.

Option	Description
Never	Disables connections.
Always	Starts connections every fifteen minutes.
Selected times	Assigns specific connection times in the schedule grid. Select a time or block of time when connections should occur.
1 Hour	Displays the schedule grid in 1-hour increments.
15 Minute	Displays the schedule grid in 15-minute increments.

Inbound Pull Newsfeeds

Depending on the type of inbound newsfeed you configured with the Newsfeed Configuration Wizard, the property page for inbound pull feeds or for accepting inbound push feeds is available.

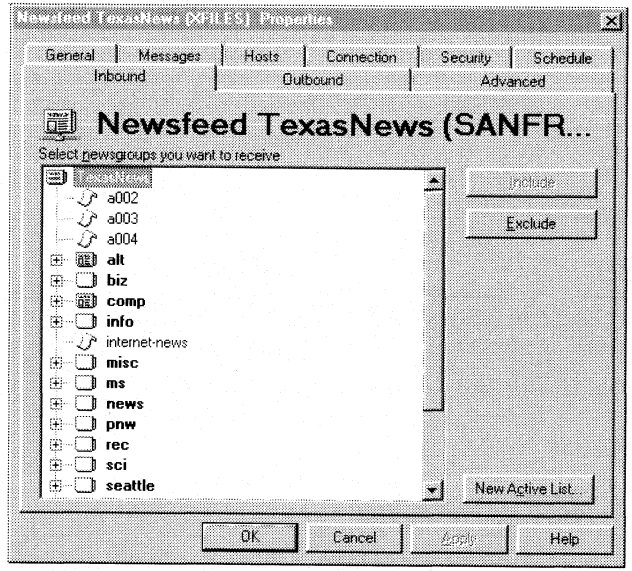
Note The list of all available newsgroups represents those that are available in the active file.

You can specify which newsgroups to include or exclude in the newsfeed. The default is to include all available newsgroups. The following table describes the symbols that are used to indicate whether you have subscribed to newsgroups.

Symbol	Description
 rec	Indicates you subscribed to the rec newsgroup.
 rec	Indicates you unsubscribed to the rec newsgroup.
 **rec**	Indicates you subscribe to all groups in the rec hierarchy, but not necessarily to the rec newsgroup.
 **rec**	Indicates you subscribe to the rec hierarchy, but not to some subgroups and not necessarily to the rec newsgroup.
 **rec**	Indicates you have unsubscribed from the rec hierarchy and all of its subgroups.
 **rec**	Indicates you have unsubscribed from the rec hierarchy and some of its subgroups.

Getting to the Inbound property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **Inbound** tab.



Adding a Newsgroup to an Inbound Pull Feed

You can add newsgroups that are pulled inbound.

1. Select the **Inbound** tab.
2. Select the newsgroup or set of newsgroups that you want to add to the newsfeed.
3. Choose **Include,** and then choose **OK**.

Removing a Newsgroup from an Inbound Pull Feed

You can remove a newsgroup or set of newsgroups from the newsfeeds that are pulled inbound.

1. Select the **Inbound** tab.
2. Select the newsgroup that you want to remove from the newsfeed.
3. Choose **Exclude,** and then choose **OK**.

Specifying a New Active File for Creating Newsgroup Public Folders in an Inbound Pull Feed

You can specify a new active file from which to create newsgroup public folders for the inbound pull newsfeed.

Note The Internet News Service must be running when an active file is downloaded from your Internet service provider.

1. Select the **Inbound** tab.
2. Choose **New Active List.**
3. Select an option.

Option	Description
Download from the newsfeed provider, via NNTP	If selected, the active file is imported from your newsfeed provider's host computer.
Import from a file	If selected, a dialog box appears prompting you to select an active file to import into your newsfeed.

Inbound Push Newsfeeds

Depending on the type of inbound newsfeed you configured with the Newsfeed Configuration Wizard, the property page for inbound pull feeds or the property page for accepting inbound push feeds is available.

Note The list of all available newsgroups represents the newsgroup public folders that are available on the Microsoft Exchange Server computer. Subscribing and unsubscribing to newsgroup public folders controls which ones accept messages from this newsfeed.

You can specify which newsgroups to include or exclude in the newsfeed. The default is to include all available newsgroups. The following table describes the symbols that are used to indicate whether you have subscribed to newsgroups.

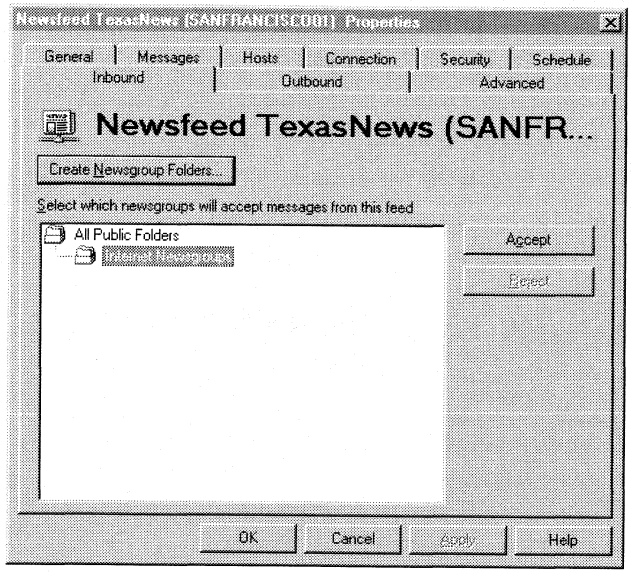
Symbols	Description
 rec	Indicates you subscribed to the rec newsgroup public folder.
 rec	Indicates you unsubscribed to the rec newsgroup public folder.
 **rec**	Indicates you subscribe to all groups in the rec hierarchy, but not necessarily to the rec newsgroup public folder.

(continued)

Symbols	Description
rec	Indicates you subscribe to the rec hierarchy, but not to some subfolders and not necessarily to the rec newsgroup.
rec	Indicates you have unsubscribed from the rec hierarchy and all of its subfolders.
rec	Indicates you have unsubscribed from the rec hierarchy and some of its subfolders.

Getting to the Inbound property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **Inbound** tab.



Configuring a Newsgroup to Accept Items in an Inbound Push Feed

Use the **Inbound** property page to specify which newsgroups will accept inbound push feeds.

1. Select the **Inbound** tab.
2. Select the newsgroup that you want to receive items in the push feed.
3. Choose **Accept**, and then choose **OK**.

Configuring a Newsgroup to Reject Items in an Inbound Push Feed

You can use the **Inbound** property page to specify which newsgroups will reject inbound push feeds.

1. Select the **Inbound** tab.
2. Select the newsgroup that you want to reject items in the push feed.
3. Choose **Reject**, and then choose **OK**.

Creating Newsgroup Public Folders

You can use the **Inbound** property page to create newsgroup public folders.

Note The symbols used to indicate whether you have subscribed to newsgroups are the same as those used for an inbound pull feed. For more information, see "Inbound Pull Newsfeeds" earlier in this chapter.

---

1. Select the **Inbound** tab.
2. Choose **Create Newsgroup Folders**.
3. Select the newsgroup that you want to create a new public folder for, and then choose **OK**.

Specifying a New Active File for an Inbound Push Feed

You can specify a new active file for the inbound push newsfeed.

Note The Internet News Service must be running when an active file is downloaded from your Internet service provider.

---

1. Select the **Inbound** tab.
2. Choose **Create Newsgroup Folders**.
3. Choose **New Active List**.
4. Select an option.

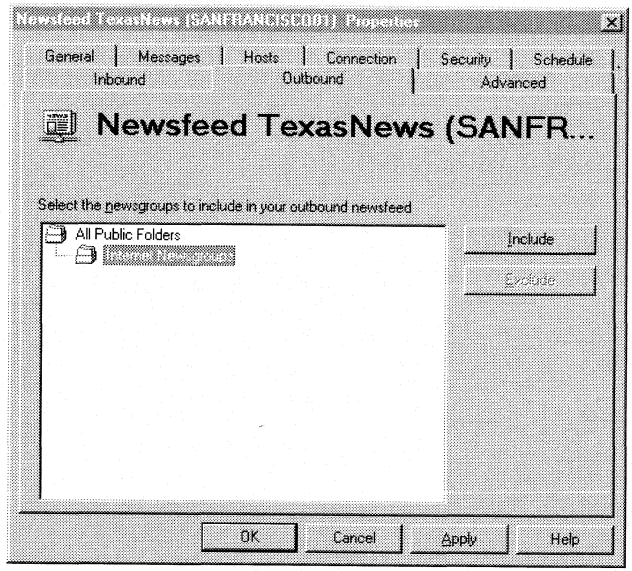
Option	Description
Download from the newsfeed provider, via NNTP	If selected, the active file is imported from your newsfeed provider's host computer.
Import from a file	If selected, a dialog box appears prompting you to select an active file to import into your newsfeed.

Outbound Newsfeeds

If your Internet News Service is configured to send outbound newsfeeds to your newsfeed provider, you can change the newsgroups that you send in the newsfeeds.

Getting to the Outbound property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **Outbound** tab.



Adding a Newsgroup to an Outbound Feed

You can add newsgroups that are pushed outbound.

1. Select the **Outbound** tab.
2. Select the public folder that contains the newsgroup you want to add to the newsfeed.
3. Choose **Include**, and then choose **OK**.

Removing a Newsgroup from an Outbound Feed

You can remove a newsgroup from the newsfeed that is pushed outbound.

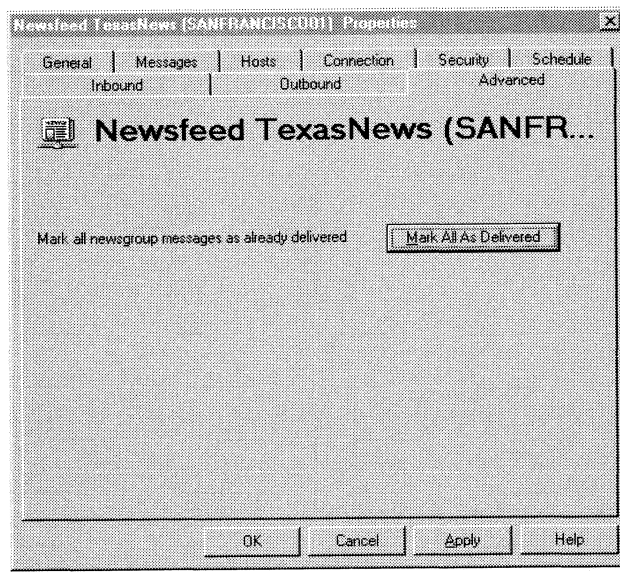
1. Select the **Outbound** tab.
2. Select the public folder that contains the newsgroup that you want to remove from the newsfeed.
3. Choose **Exclude**, and then choose **OK**.

Advanced

Use the **Advanced** property page to flush queued messages.

Getting to the Advanced property page

1. In the Administrator window, choose a site, and then choose **Connections**.
2. Double-click your newsfeed.
3. Select the **Advanced** tab.



Flushing Queued Messages

You can mark all queued newsgroup messages as delivered. This flushes the queue of messages waiting to be processed so your Microsoft Exchange Server or another host computer can catch up to the most recent newsgroup posts.

For more information about catching up to current newsfeeds, see "Catching Up to Current Newsfeeds" earlier in this chapter.

1. Select the **Advanced** tab.
2. Choose **Mark All As Delivered**.

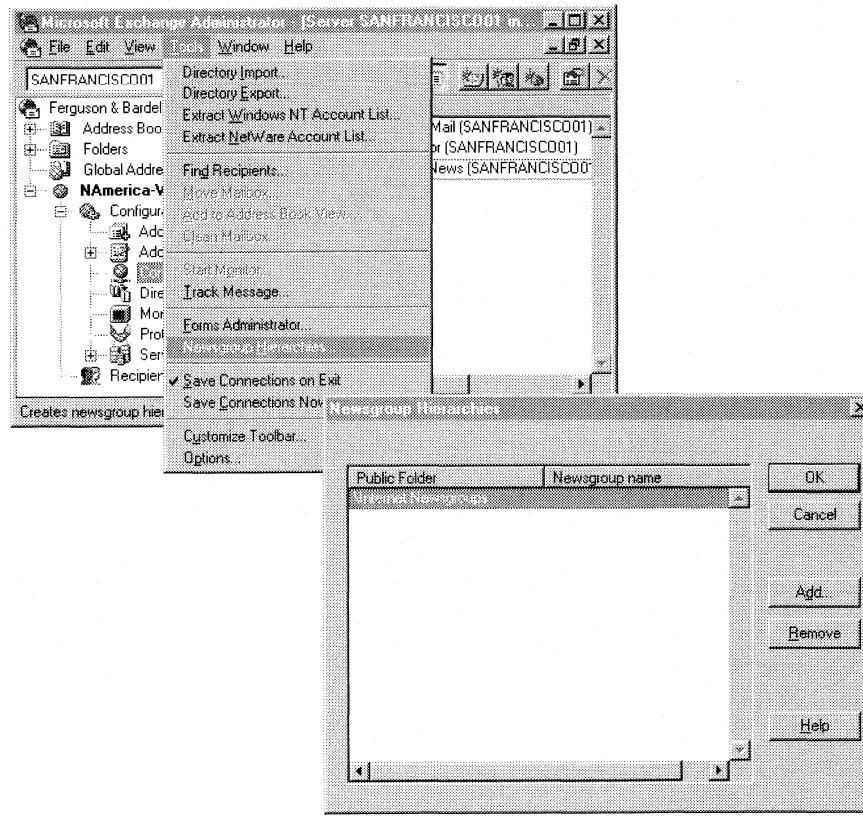
Setting Up Newsgroup Hierarchies

If you want to make an existing public folder tree into a hierarchy of newsgroup public folders, you can designate a top-level newsgroup public folder as a hierarchy parent. If the top-level newsgroup public folder doesn't already have a newsgroup name, you can specify one that is used to generate newsgroup names for all subfolders in the hierarchy. You can also remove the newsgroup properties from a public folder hierarchy.

Note Newsgroups that are included in the Internet News public folder by default, such as the comp and rec hierarchies, are not listed in the newsgroup hierarchy unless you add them to the list.

Getting to the Newsgroups Hierarchies dialog box

- From the **Tools** menu, choose **Newsgroup Hierarchies**.



Defining a Newsgroup Public Folder as a Hierarchy

1. In the **Newsgroups Hierarchies** dialog box, choose **Add**.
2. Select the public folder that you want to designate as a hierarchy parent newsgroup public folder.
3. Choose **OK**.
4. In the **Newsgroup name** box, type the name you want to assign as the newsgroup name of the public folder hierarchy.

Removing a Newsgroup Public Folder from the Hierarchy

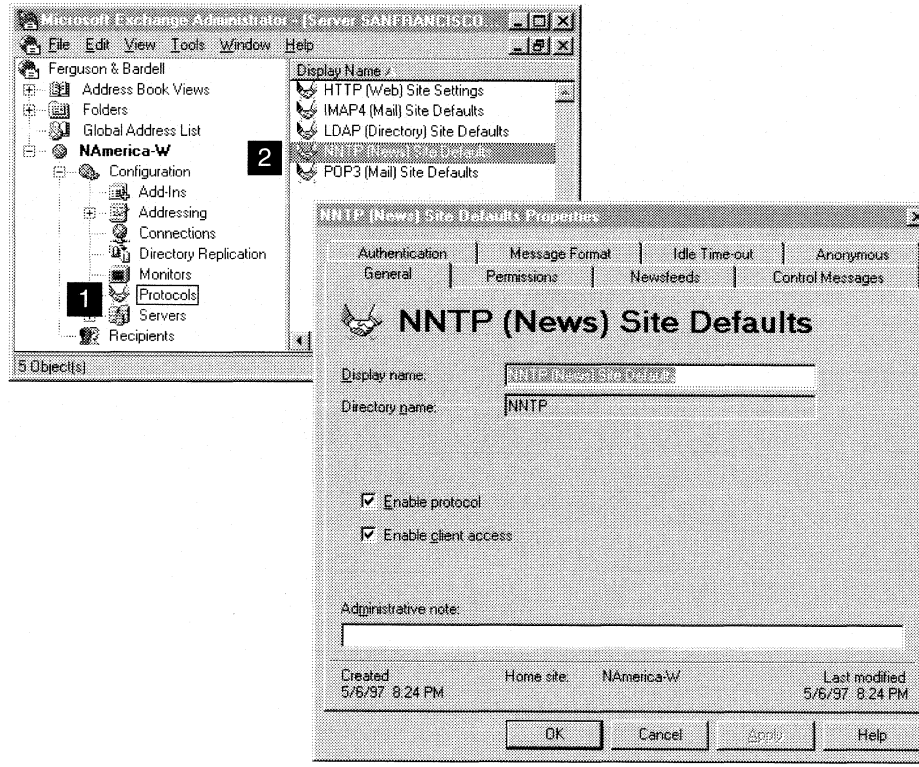
1. In the **Newsgroups Hierarchies** dialog box, select the public folder that you want to remove from the hierarchy.
2. Choose **Remove**, and then choose **OK**.

Setting Up Properties for NNTP

To send and receive USENET newsfeeds, you must configure the newsfeed and NNTP properties. You can set properties for the NNTP object that are available at the site and server levels. Site NNTP properties apply to all servers in a site; server NNTP properties apply only to a single server. With some exceptions, all properties for the NNTP object are the same for the site and the server.

Getting to the NNTP property pages

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **NNTP (News) Site Defaults** for the site, or **NNTP (News) Settings** for the server.



General Properties

Use the **General** property page to specify a display name for the newsfeed, view the directory name, and enable NNTP on your Microsoft Exchange Server computer.

Getting to the General property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **NNTP (News) Site Defaults** for the site, or **NNTP (News) Settings** for the server.
3. Select the **General** tab.

Defining a Display Name

Use the **General** property page to define the NNTP display name.

1. Select the **General** tab.
2. Type a display name.

Option	Description
Display name	A maximum of 256 alphanumeric characters, which can include spaces and special characters.
Directory name	A name defined during installation that cannot be changed.

Enabling NNTP for the Site

Use the **General** property page on the NNTP site object to enable NNTP for all servers in the site, or to enable NNTP clients to access newsgroup public folders.

1. Select the **General** tab.
2. Select **Enable protocol**.

Enabling Client Access for the Site

Use the **General** property page on the NNTP site object to enable NNTP clients to use newsgroup public folders in the site.

1. Select the **General** tab.
2. Select **Enable client access**.

Using the Site Defaults

Use the **General** property page on the NNTP server object to use the default values from the NNTP site object.

Note This option is available only for NNTP properties in the server container.

1. Select the **General** tab.
2. Select or clear the **Use site defaults for all properties** check box.

Option	Description
Use site defaults for all properties	Select to use the options you've set for permissions, newsfeeds, and message format options.

Permissions

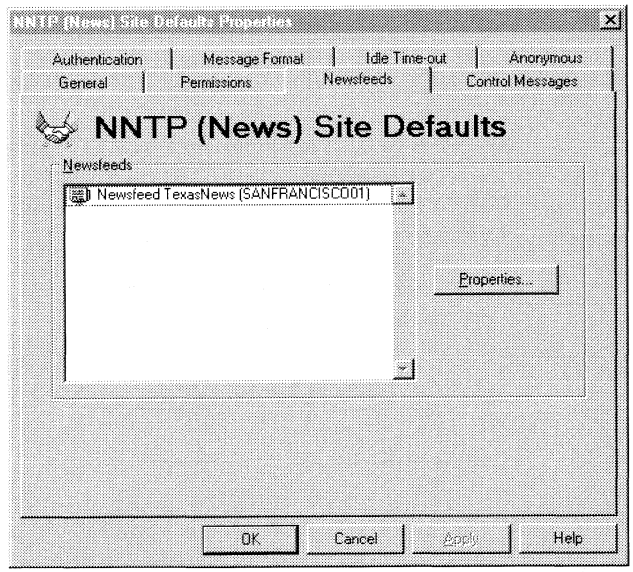
You can set permissions to control the rights that users have on the NNTP object. You delegate permission to a user (or group) by assigning the user a role, which defines how much and what type of access a user has on the object. Microsoft Exchange Server provides a number of predefined roles, but you can also create custom roles to suit your specific needs. For more information on permissions, see *Microsoft Exchange Server Getting Started.*

Newsfeed Properties

You can view the properties of a newsfeed from the NNTP site object or the NNTP server object. On the NNTP server object, you can also change the name of the USENET site and create an active file of newsgroup public folders for other hosts and clients to download.

Getting to the Newsfeeds property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **NNTP (News) Site Defaults** for the site, or **NNTP (News) Settings** for the server.
3. Select the **Newsfeeds** tab.



Viewing Newsfeed Properties

Use the **Newsfeeds** property page to view properties for newsfeeds that you have already created.

1. Select the **Newsfeeds** tab.
2. Select the newsfeed you want to view, and then choose **Properties**.

Changing the USENET Site Name

Use the **Newsfeeds** property page on the NNTP server object to change the USENET site name for servers in your site. The USENET site name is stamped on each NNTP message so servers can identify messages they receive that they have already processed.

Note This option is available only for NNTP properties in the server container.

1. Select the **Newsfeeds** tab.
2. In the **USENET site name** box, type the USENET site name.

Creating an Active File of Newsgroup Public Folders

Use the **Newsfeeds** property page on the NNTP server object to create an active file containing newsgroup public folders that other NNTP hosts and clients can download. An active file contains a list of newsgroups that hosts can subscribe to. For more information about active files, see *Microsoft Exchange Server Concepts and Planning*.

Note This option is available only for NNTP properties in the server container.

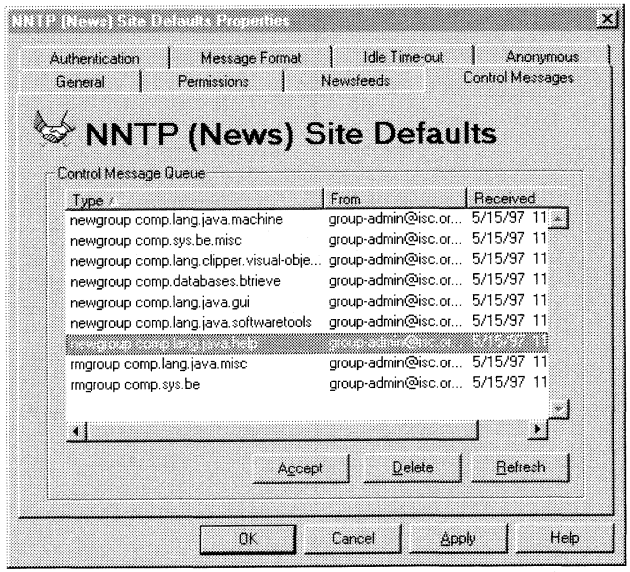
1. Select the **Newsfeeds** tab.
2. Choose **Create Active File**.
3. Specify the newsgroup public folders that you want to add to the new active file.

Control Messages Properties

When Microsoft Exchange Server receives control messages, it queues them until you decide whether to accept the messages. If you don't trust a particular USENET host, you can delete the control messages from the host without accepting their changes.

Getting to the Control Messages property page

1. In the Administrator window, choose a site, and then choose **Protocols**.
2. Double-click **NNTP (News) Site Defaults** for the site.
3. Select the **Control Messages** tab.



Processing Queued Control Messages

Use the **Control Messages** property page to process queued control messages.

1. Select the **Control Messages** tab.
2. Select the queued control message you want to process, and then choose **Accept** or **Delete**.

Option	Description
Accept	Accepts the selected control message in the queue and performs the action that it specifies.
Delete	Deletes the selected control message in the queue and does not perform the action that it specifies.
Refresh	Updates the list of queued control messages with all control messages that have been received.

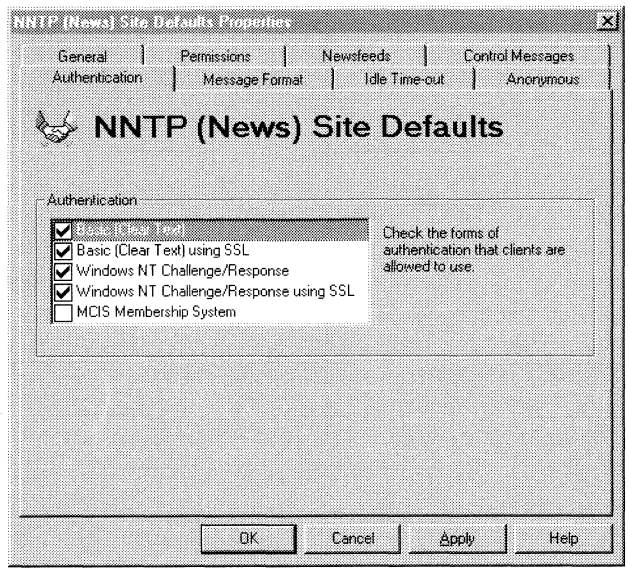
Authentication

Use the **Authentication** property page to specify authentication methods an NNTP client is allowed to use to access information on the Microsoft Exchange Server computer. Authentication is the process the NNTP server uses to determine whether to grant the user permission to connect to the system. In order for an NNTP client to log on to the Microsoft Exchange Server computer, one of the authentication methods that the client supports must be enabled on the server. Check with your client's vendor if you are unsure of which authentication methods are available.

To use SSL, IIS must be installed on the Microsoft Exchange Server computer before Microsoft Exchange Server is installed. For more information about configuring IIS, see "Requiring Secure SSL Connections" earlier in this chapter.

Getting to the Authentication property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **NNTP (News) Site Defaults** to configure site NNTP defaults, or **NNTP (News) Settings** to configure server NNTP settings.
3. Select the **Authentication** tab.



Setting Authentication Methods

Note If Windows NT Challenge/Response is enabled on the Microsoft Exchange Server computer, Microsoft Internet Mail and News version 3.0 will attempt to connect to the Microsoft Exchange Server computer using Windows NT Challenge/Response. If authentication using this method fails, Internet News will try to connect to the Microsoft Exchange Server computer using basic clear-text authentication.

1. Select the **Authentication** tab.
2. In the **Authentication** box, select an authentication type.

Option	Description
Basic (Clear Text)	Enable authentication through an unencrypted user name and password. Most NNTP clients support this method.
Basic (Clear Text) using SSL	Use SSL protocol to encrypt clear text.
Windows NT Challenge/Response	Enable authentication through Windows NT network security and an encrypted password. This method is supported by Microsoft Internet Mail and News version 3.0 and later. With Windows NT Challenge/Response, it is not possible to specify the name of the Microsoft Exchange Server mailbox you want to access. By default, Microsoft Exchange Server attempts to access the mailbox with the same name as the Windows NT user account that the user is logged on as. For example, if you are logged on as Domain\Suzanf, with Windows NT Challenge/Response enabled, Microsoft Exchange Server attempts to access the mailbox called Suzanf.
Windows NT Challenge/Response using SSL	Enable authentication using Windows NT network security to occur through an SSL-encrypted channel on port 563. This method will be supported by future versions of Microsoft Internet Mail and News.
MCIS Membership System	Enable authentication using Windows NT network security to occur through the Microsoft Commercial Internet Server (MCIS) Membership System.

Message Format Properties

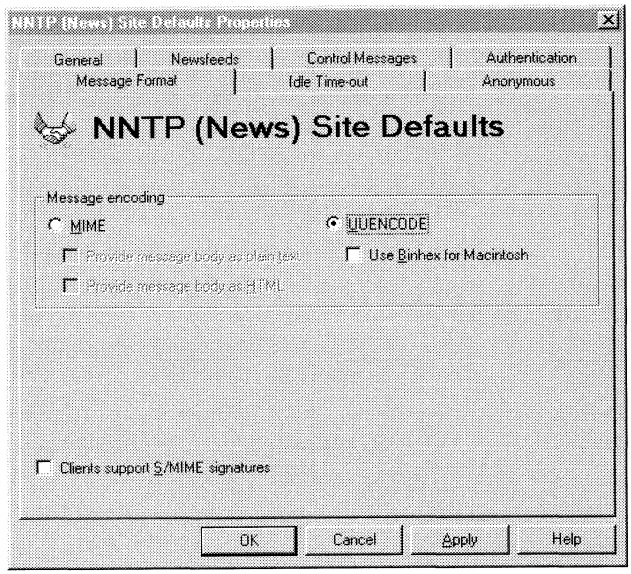
You can specify the message format for encoding newsgroup items from the NNTP site object or the NNTP server object. This applies to both incoming and outgoing messages.

The settings in the **Message Format** property page determine the format that Microsoft Exchange Server messages are converted to when they are retrieved by an NNTP client. Messages sent by an Internet user are not converted. Instead they are retrieved by the NNTP client in the format that the message was originally composed in.

Note Default character settings for NNTP are configured on a per-folder basis. For more information, see "Setting Properties on Newsgroup Public Folders" later in this chapter.

Getting to the Message Format property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **NNTP (News) Site Defaults** for the site, or **NNTP (News) Settings** for the server.
3. Select the **Message Format** tab.



Specifying Message Format Options

When a user retrieves messages using NNTP, you can specify how these messages are converted from the Microsoft Exchange Server format to various Internet mail formats.

1. Select the **Message Format** tab.
2. Under **Message encoding**, select options for message format.

Option	Description
MIME	Text and attachments are encoded using Multipurpose Internet Mail Extensions (MIME). MIME is the standard for exchanging multimedia messages on the Internet. If a MIME message is delivered to a non-MIME-aware client, the text and attachments may not be usable. This is the default.
Send message body as plain text	A plain text MIME body part is generated for the message. If **Send message body as HTML** is also selected, a MIME multipart alternative plain text MIME body part is generated.
Send message body as HTML	An HTML MIME body part is generated for the message. If **Send message body as plain text** is also selected, a MIME multipart alternative HTML MIME body part is generated. HTML is an Internet standard that enables rich-text formatting, such as bold, color, and italic, to appear in messages. Clients such as Microsoft Internet Mail and News version 3.0 can read HTML.
UUENCODE	Renders the message body as text with any attachments encoded by the uuencode method, which is commonly used in the UNIX operating system to encode 8-bit data transmitted on the Internet.
Use Binhex for Macintosh	Renders the message body as text with any attachments encoded by the BinHex method, a common method used in the Macintosh operating system to encode 8-bit data transmitted on the Internet.

Enabling Client S/MIME Signature Support

You can use the **Message Format** property page to enable support for signed S/MIME messages. This is useful for accessing newsgroups that contain signed S/MIME messages.

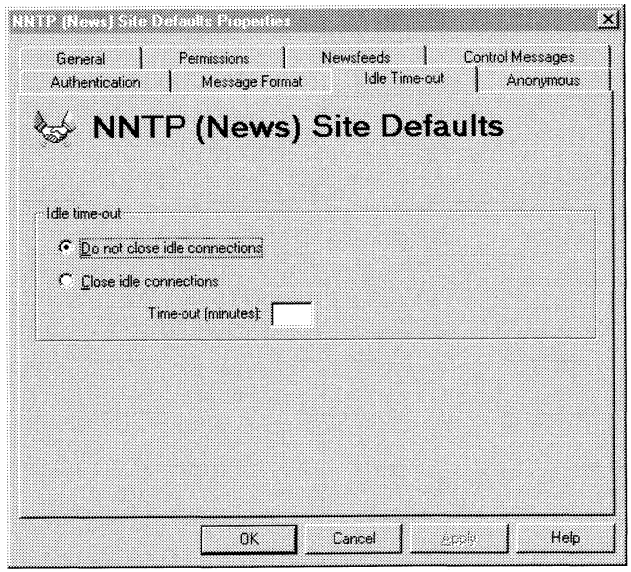
1. Select the **Message Format** tab.
2. Select Clients support S/MIME signatures.

Idle Time-out

Use the **Idle Time-out** property page to specify how long NNTP connections can remain idle before they are closed.

Getting to the Idle Time-out property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **NNTP (News) Site Defaults** to configure site NNTP defaults, or **NNTP (News) Settings** to configure a server's NNTP settings.
3. Select the **Idle Time-out** tab.



Setting Idle Time-out Connections

Use the **Idle Time-out** property page to close NNTP connections after a specified interval of inactivity.

1. Select the **Idle Time-out** tab.
2. Select an option.

Option	Description
Do not close idle connections	Idle connections never close.
Close idle connections	Idle connections close after the time period specified in the **Time-out (minutes)** box.
Time-out (minutes)	The amount of time in minutes a connection can remain idle before being closed.

Anonymous Connections

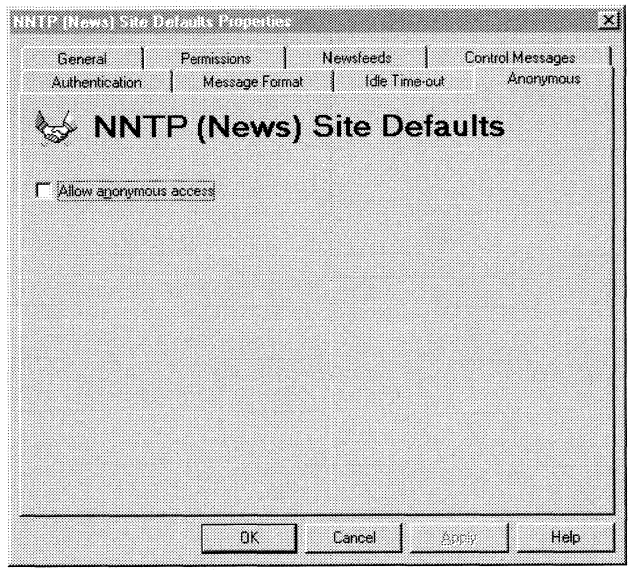
You can specify whether NNTP users can connect to Microsoft Exchange Server anonymously. NNTP users connecting to Microsoft Exchange Server anonymously don't need a Windows NT user account to access newsgroup public folders.

You can specify which newsgroup public folders that authenticated and anonymous users can view when accessing Microsoft Exchange Server. For example, you may not want to allow anonymous users to access a newsgroup public folder containing confidential information.

Note To allow anonymous access to newsgroup public folders using NNTP, the Windows NT Guest account must exist on the Microsoft Exchange Server computer, although the account does not have to be enabled. This account is used for logging anonymous access with the license manager.

Getting to the Anonymous property page

1. In the Administrator window, choose a site or server, and then choose **Protocols**.
2. Double-click **NNTP (News) Site Defaults** to configure site NNTP defaults, or **NNTP (News) Settings** to configure a server's NNTP settings.
3. Select the **Anonymous** tab.



Setting Anonymous Access

Use the **Anonymous** property page to specify whether NNTP users can connect anonymously to Microsoft Exchange Server.

Note In order for users to connect anonymously to Microsoft Exchange Server public folders, you must select the **Allow anonymous access** check box on the **Anonymous** property page. You must also grant anonymous users permissions on the public folder by using the Administrator program or Outlook.

---

1. Select the **Anonymous** tab.
2. Select the **Allow anonymous access** check box.

Diagnostics Logging

You can control how logging information for NNTP is written to the Windows NT Event Log. You can specify the types of events that are logged for NNTP and the level of logging information for each event. Viewing the event log for NNTP is useful when troubleshooting problems occur.

Note Diagnostics logging is available only for NNTP properties in the server container.

For more information about diagnostics logging, see *Microsoft Exchange Server Maintenance and Troubleshooting*.

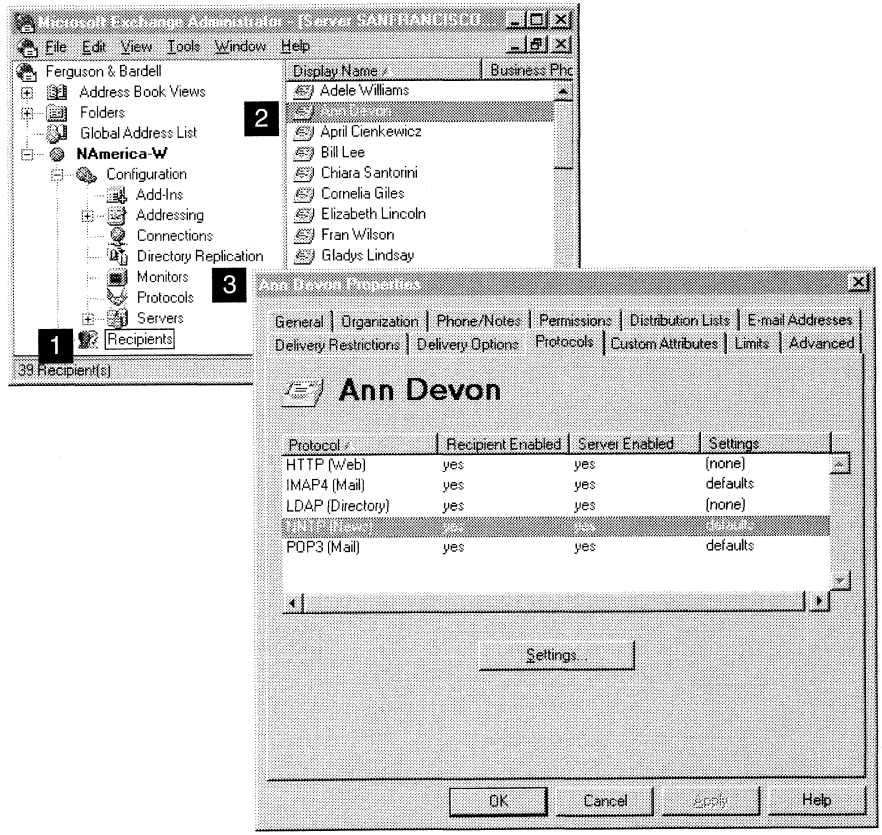
NNTP Mailbox and Custom Recipient Configuration

You can specify whether an NNTP client can use a mailbox or a custom recipient to be authenticated to connect to Microsoft Exchange Server. Disabling NNTP access on a mailbox or custom recipient means that an NNTP client cannot connect to the server using that mailbox or custom recipient's credentials. To provide authenticated access to a user who has a mailbox in your Microsoft Exchange Server organization, NNTP must be enabled at the mailbox and at the server. To provide authenticated access to a user without a mailbox, create a custom recipient for the user with an associated Windows NT account. The NNTP client must provide this account information when connecting to Microsoft Exchange Server.

Note If you disable the NNTP protocol on the server object, NNTP support is also disabled for individual mailboxes. For NNTP to be enabled on a mailbox, it must be enabled on the server and mailbox.

Getting to the Protocols property page

1. In the Administrator window, choose **Recipients**.
2. Double-click the mailbox or custom recipient you want to configure.
3. Select the **Protocols** tab.



Enabling NNTP for a Mailbox or Custom Recipient

Use the **Protocols** property page to enable NNTP for individual mailboxes or custom recipients.

1. Select the **Protocols** tab.
2. Select **NNTP (News)**, and then choose **Settings**.
3. Select the **Enable NNTP for this recipient** check box.

Specifying NNTP Settings for Message Encoding

If NNTP is enabled on a mailbox or custom recipient, you can use default settings for the message format. Alternatively, you can customize the settings for individual mailboxes or custom recipients. You can specify how text and attachments are encoded and the character set that your recipient uses.

The settings in the **Message Format** property page determine the format that Microsoft Exchange Server messages are converted to when they are retrieved by an NNTP client. Messages sent by an Internet user are not converted. Instead they are retrieved by the NNTP client in the format that the message was originally composed in.

1. Select the **Protocols** tab.
2. Select **NNTP (Mail)**, and then choose **Settings**.
3. Select options for message content defaults and message encoding. To use message format defaults that you set at the server level, select the **Use protocol defaults** check box.

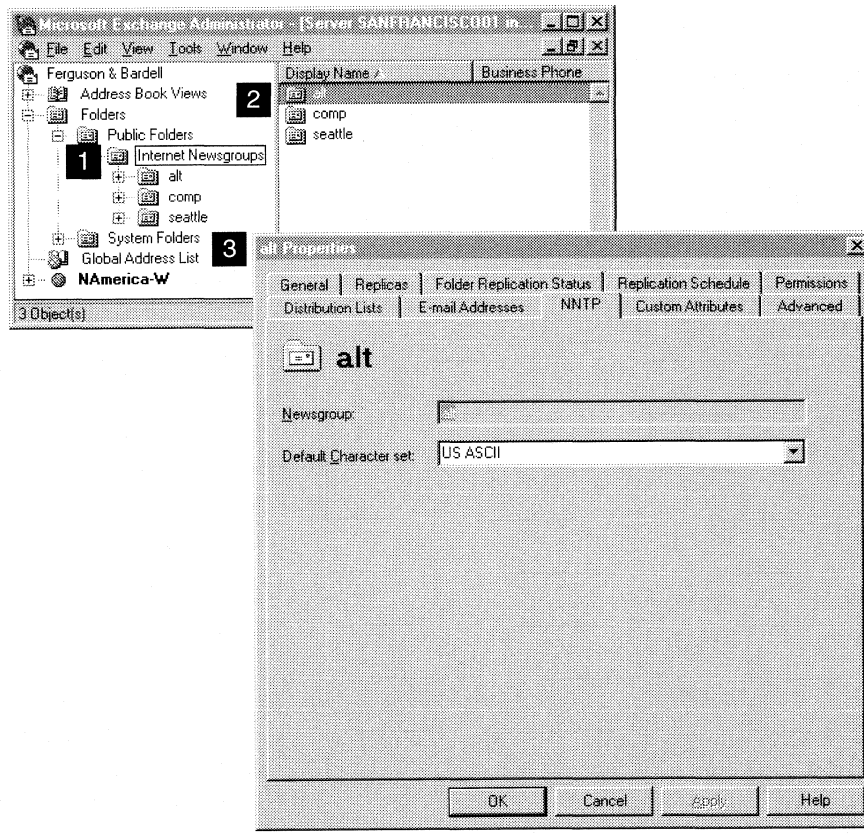
For information about these options, see "Message Format Properties" earlier in this chapter.

Setting Properties on Newsgroup Public Folders

Once a newsgroup public folder has been created, you can view or change its NNTP properties using the Microsoft Exchange Server Administrator program.

Getting to the NNTP property page

1. In the Administrator window, choose **Public Folders**.
2. Double-click the newsgroup public folder you want to configure.
3. Select the **NNTP** tab.



Changing the Default Character Sets

Use the **NNTP** property page on the newsgroup public folder to specify a different default character set for MIME and non-MIME messages.

Microsoft Exchange Server allows you to specify the *character set* you want to use for Internet messages. A character set is a method for encoding characters in a language's writing system to numeric values. There are many character sets for representing text in different languages. For some languages, there are multiple incompatible character sets in use. In order to read the text of a message, your e-mail or newsreader client must be able to decode the character set in which the text has been encoded.

MIME clients include information in the message that identifies the character set, so they are truly capable of multilingual support. When Microsoft Exchange Server receives a MIME message from a client or a newsfeed, the message is saved into the information store using the character set specified in the message. It remains in this character set when an NNTP client retrieves it or it is sent out in a newsfeed.

Because non-MIME messages do not have character set information in them, the sending and receiving software must be configured to use the same character set. For NNTP, this configuration is done on a per-folder basis because typically the messages within newsgroups use the same character set. Microsoft Exchange Server uses the default character set for all non-MIME messages. For example, you would use ISO Latin 1 (iso-8859-1) for the French newsgroups (newsgroup hierarchies fr.*), and JIS (iso-2022-jp) for the Japanese newsgroups (newsgroup hierarchies fj.*).

Messaging Application Programming Interface (MAPI) clients such as Outlook are capable of multilingual support, but they compose messages using Microsoft Windows code pages instead of Internet character sets. In some cases, there are multiple Internet character sets available for a particular Windows code page. When a message posted by a MAPI client is retrieved in MIME format from the information store for an NNTP client or newsfeed, the **Default Character set** option determines the character set that is used if there are multiple character sets available for the code page of the message. The default character set varies according to the language installed on the server.

1. Select the **NNTP** tab.
2. In the **Default Character set** box, select the default character set to be used for items in this newsgroup public folder. The default character set specifies the character set that will be used when generating MIME and non-MIME messages that originate from Microsoft Exchange Server.

Configuring NNTP Clients

To connect to a Microsoft Exchange Server computer running NTTP, you must specify the following information on the NNTP client:

- An NNTP account name and password (unless anonymous connections are used).
- An NNTP server name.

You can also configure NNTP clients to support SSL when connecting to Microsoft Exchange Server computers that support SSL.

Because NNTP clients vary, the steps for configuring clients to connect to a Microsoft Exchange Server computer running NTTP are different for each client. For information about how to configure the Microsoft Internet News client that is included with Microsoft Internet Explorer version 3.0, see "Sample NNTP Client Configuration" later in this chapter.

NNTP Account

An NNTP account is the alias name of a Microsoft Exchange Server mailbox or custom recipient that supports NNTP. For example, the alias for Suzan Fine's mailbox is SuzanF.

Because Microsoft Exchange Server uses Windows NT user accounts for authentication, it may be necessary to specify the mailbox's Windows NT domain, user account, and alias name. Performance can be improved by including the mailbox's Windows NT domain in the NNTP account.

Keep the following in mind when you set up your NNTP client's account:

- If a Windows NT domain and user name are specified as the NNTP account, they must precede the mailbox's alias name. For example, *Windows_NT_domain\user_account_name\mailbox_alias name*.
- If only an alias name is specified as the NNTP account, the Microsoft Exchange Server computer running NNTP uses a Windows NT user name that is equivalent to the alias name. All Windows NT domains are searched to locate the first domain that contains that Windows NT user. For example, if you specify SuzanF as the NNTP account, all domains are searched to find the first domain that contains user *Windows_NT_domain*\SuzanF\SuzanF.
- If only a Windows NT domain and user account are specified as the NNTP account, the Microsoft Exchange Server computer running NNTP uses a mailbox alias that is equivalent to the Windows NT user account. For example, *domain_name*\SuzanF as the NNTP account is equivalent to *domain_name*\SuzanF\SuzanF as the NNTP account.
- The NNTP password for the mailbox is the Windows NT user account password that is associated with the Microsoft Exchange Server mailbox or custom recipient.

NNTP Server

The NNTP server name is the computer name of the Microsoft Exchange Server computer that has the NNTP newsgroups that the NNTP client accesses.

SSL Connections

Not all NNTP clients support SSL. For information about configuring NNTP clients to use SSL, see your NNTP client documentation. If you enable only SSL security on your Microsoft Exchange Server computer, only clients that support SSL can connect to it.

Sample NNTP Client Configuration

The following example shows how to set up an NNTP client for a Microsoft Exchange Server user named Suzan Fine at a company called Ferguson & Bardell (FB).

You create a Microsoft Exchange Server mailbox or custom recipient for Suzan with SuzanF as the alias name and Exchange1 as the computer name. The primary Windows NT account that is associated with this mailbox or custom recipient is FB\SuzanF. The Internet Mail Service that is providing Simple Mail Transfer Protocol (SMTP) service to the NNTP accounts is also running on the Exchange1 computer. The domain name of the company is FB.com. The following options must be specified for the Microsoft Internet News NNTP client, which is included in Microsoft Internet Explorer 3.0:

Name Suzan Fine

Organization Ferguson & Bardell

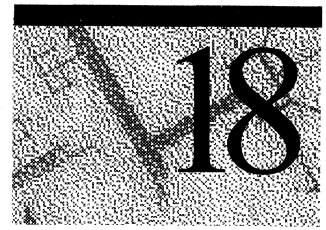
News server name Exchange1

Account name FB\SuzanF

Password Windows NT password for account FB\SuzanF

CHAPTER 18

Microsoft Outlook Web Access



With Microsoft Outlook Web Access, users can access data on a Microsoft Exchange Server computer using an Internet browser from a UNIX, Macintosh, or Microsoft Windows-based computer. It provides Web-based public access to Microsoft Exchange Server public folders and the global address list. Registered users can log on to their personal accounts to read private e-mail and send messages. Using Web-based public folder access, an organization can build private and public discussion forums on the Internet and private intranets. Users can publish information on the Internet without converting documents to Hypertext Markup Language (HTML) format.

Microsoft Outlook Web Access works with a user's Web browser, communicating through the Microsoft Internet Information Server (IIS) to provide a client interface to a Microsoft Exchange Server mailbox. Outlook Web Access extends the messaging capabilities of Microsoft Exchange Server through the Internet to the World Wide Web.

Outlook Web Access Installation

You can install Outlook Web Access (.Asp and HTML) files during Microsoft Exchange Server setup. Microsoft Exchange Server can be installed on the same Windows NT Server computer as IIS, or it can be installed on a different Windows NT Server computer that can be accessed by the server where Outlook Web Access is installed. When installing Outlook Web Access and Microsoft Exchange Server on the same computer, the WWW service in IIS must be enabled.

Active Server, a feature of IIS, acts as a liaison between a server component (Outlook Web Access) and a Web browser such as Microsoft Internet Explorer or Netscape Navigator. Active Server combines HTML, server-executed scripts, and remote procedure calls (RPCs) to generate web pages dynamically. You can customize these .Asp files for your organization. For example, you can add company information to a title, change graphics, or otherwise modify the operation of Outlook Web Access. You should back up the files before you customize them.

To download more information about customizing .Asp files for use with Microsoft Exchange Server, use your Internet browser to visit http://www.microsoft.com/msdn/sdk/ and follow the Microsoft Platform SDK link.

How Outlook Web Access Works

To access the logon page for the Microsoft Exchange Server computer, users start their Web browser and connect to the Internet, specifying the Uniform Resource Locator (URL) of their Active Server. The Web browser then displays an introductory Web page that prompts users to log on using their mailbox name. Users must type their Microsoft Exchange Server mailbox alias and press ENTER. The **Enter Network Password** dialog box appears, prompting users for their user name and password. Users must type their domain name and Windows NT user account alias in the **User name** box in the format: *domain\Windows NT user account alias*, followed by their Windows NT user account password in the **Password** box.

Note The user's Microsoft Exchange Server mailbox name and Windows NT user account alias can be different. This is because the Windows NT user management utilities and the Microsoft Exchange Server Administrator program allow separate setup of the Windows NT user account and the Microsoft Exchange Server mailbox.

After typing the complete logon information, users can access their private mailbox and public folder data. Microsoft Exchange Server Messaging Application Program Interface (MAPI) data, Active Server scripts (.Asp files), and RPC data are translated to HTML on the Active Server and transmitted to the browser using the Hypertext Transfer Protocol (HTTP).

Authentication

Users can access the Microsoft Exchange Server computer through the Internet by logging on with a secure connection as a validated user or an anonymous user. When a user logs on to a Microsoft Exchange Server computer, an authenticated and encrypted session is established between the browser and the IIS computer. To gain access to Microsoft Exchange Server, the user's Windows NT domain account password must be validated before permission is granted to use the program and its data. This information is used by IIS to log the user on to the Microsoft Exchange Server computer.

Security Levels

Basic authentication is the lowest level of security available for Internet or intranet users. Security for Outlook Web Access is configured through the Microsoft Internet Service Manager provided with IIS. When setting up basic authentication, you must also set up Log on Locally permission on the IIS computer.

If IIS and Microsoft Exchange Server are installed on the same computer, Windows NT Challenge/Response authentication can be enabled to offer a higher level of security than basic authentication. However, if IIS is installed on a different computer than Microsoft Exchange Server, Windows NT Challenge/Response authentication must be disabled.

Additional security can be established by enabling Secure Sockets Layer (SSL) on the IIS computer. SSL is used to encrypt data passed between the Web browser and IIS. This feature can be used only with Web browsers that support SSL, such as Microsoft Internet Explorer version 3.02 or Netscape Navigator version 3.01. A security certificate must be obtained to enable the use of SSL. The supplier of the security certificate provides instructions for setting up the server and the browsers. Either basic authentication or Windows NT LAN Manager (NTLM) security must be enabled on the IIS system to use SSL.

For more information about setting up SSL, see your Microsoft Internet Information Server documentation.

Validated User

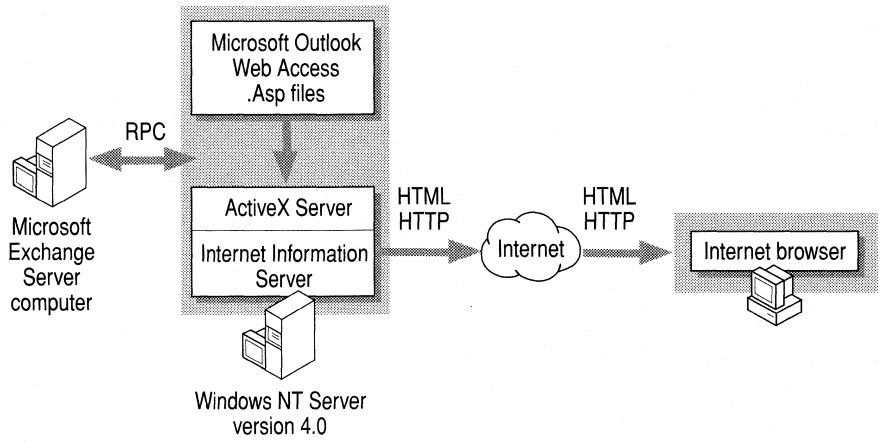
Outlook Web Access uses Windows NT authentication to grant access to mailboxes. To log on, users must enter their Windows NT user account name, their password, and their mailbox name. After validation is successfully completed, users have the same permissions they have when they log on to a computer directly connected to the network.

Anonymous User

An *anonymous user* is a non-validated Web user who is not recognized by Microsoft Exchange Server. A user can log on to a Microsoft Exchange Server computer anonymously, but is restricted to viewing and accessing only the published public folders and address lists. You can specify which folders and address lists to publish using the Microsoft Exchange Server Administrator program.

Outlook Web Access Configuration

Outlook Web Access is configured using the Microsoft Exchange Server Administrator program. The following illustration shows a possible configuration of the Microsoft Exchange Server computer and Outlook Web Access running on separate computers.

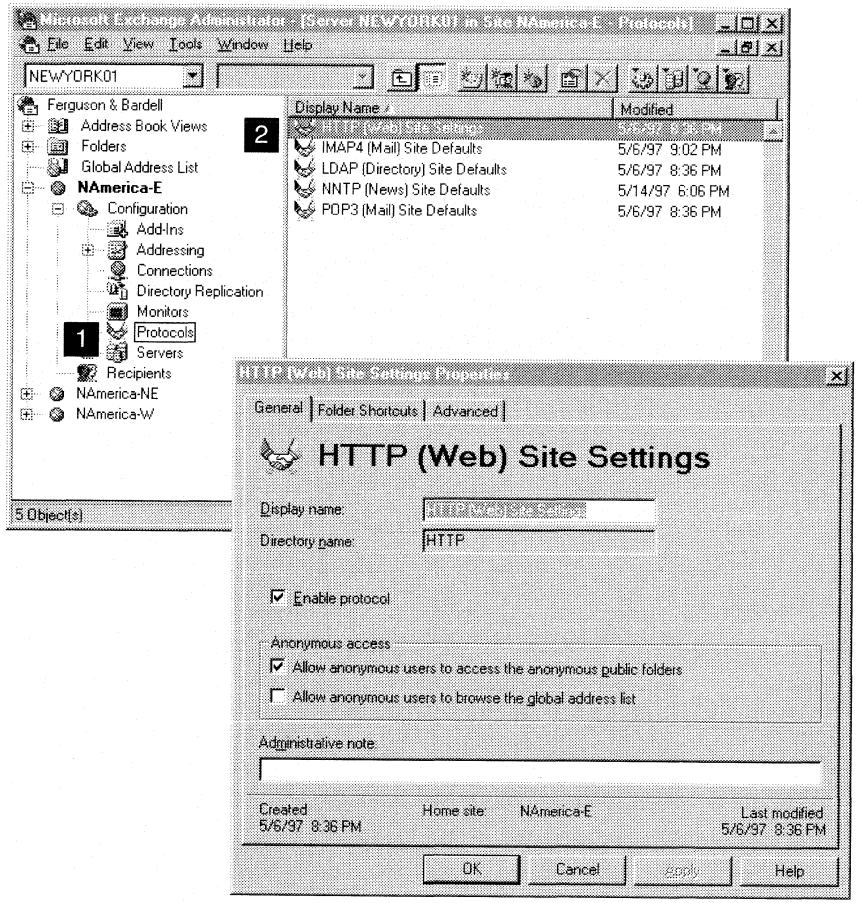


After Setup, you can use the Administrator program to define whether public folders and the global address list can be viewed by anonymous users. You can specify which public folders are available to anyone on the Internet. These are called *published public folders* and are defined using the **Folder Shortcuts** property page.

Users must have a copy of an Internet browser that supports JavaScript and frames, such as Microsoft Internet Explorer 3.0 or Netscape Navigator 3.0. Once you have configured Outlook Web Access, provide the URL to users. The format is http://*<IIS server name>*/exchange.

Getting to the HTTP (Web) Site Settings property pages

1. In the Administrator window, choose a site, and then choose **Protocols**.
2. Double-click HTTP (Web) Site Settings.



General Properties

Use the **General** property page to define the display name, view the directory name, enable the HTTP protocol, and grant anonymous users access to published public folders and the global address list.

Getting to the General property page

1. In the Administrator window, choose a site, and then choose **Protocols**.
2. Double-click **HTTP (Web) Site Settings**.
3. Select the **General** tab.

Defining the Display Name

Use the **General** property page to define the display name for the HTTP (Web) Site Settings object. The display name is HTTP (Web) Site Settings in the Administrator window.

1. Select the **General** tab.
2. Type a display name.

Option	Description
Display name	Type a maximum of 256 alphanumeric characters, which can include spaces and special characters. The default is HTTP (Web) Site Settings.
Directory name	The name is defined at installation and cannot be changed.

Enabling HTTP

You can use the **Protocols** property page to enable HTTP for individual mailboxes and custom recipients.

1. Select the **Protocols** tab.
2. Select **HTTP (Web)** and choose **Settings**.
3. Select the **Enable HTTP for this recipient** check box.

Enabling Web Browser Access

Use the **General** property page to enable users to connect to Microsoft Exchange Server with Internet browser software. This setting enables HTTP for the site. It is enabled by default.

1. Select the **General** tab.
2. Select or clear the **Enable protocol** check box to enable users to connect to Microsoft Exchange Server using an Internet browser.

Setting Anonymous Access

Use the **General** property page to specify whether anonymous users can access published public folders and browse the organization's global address list.

1. Select the **General** tab.
2. Under **Anonymous access**, select or clear one or both options.

Option	Description
Allow anonymous users to access the anonymous public folders	Select to give anonymous users access to public folders published on the Internet.
Allow anonymous users to browse the global address list	Select to give anonymous users the ability to browse the global address list published on the Internet.

Note You must also set anonymous permissions on any public folder shortcut that you want to make available to anonymous users.

Permissions

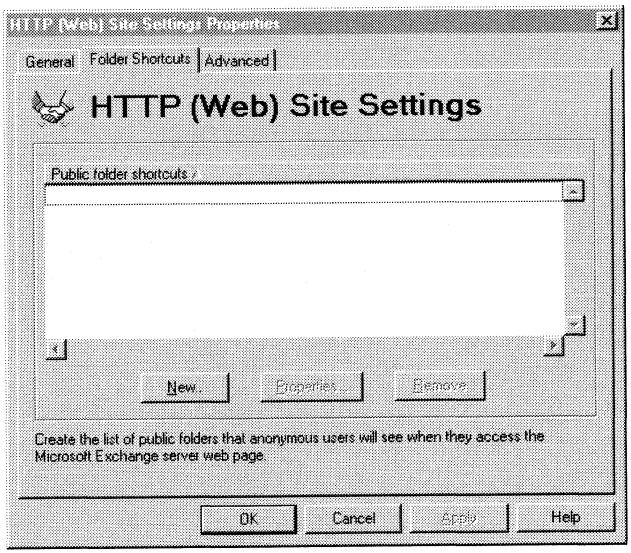
You can assign specific permissions on the HTTP object. For more information on permissions, see *Microsoft Exchange Server Getting Started.*

Published Public Folders

Folder shortcuts are links to the Microsoft Exchange Server published public folders. Use the **Folder Shortcuts** property page to define the list of public folders that anonymous users see when they access the Microsoft Exchange Server computer from the Internet.

Getting to the Folder Shortcuts property page

1. In the Administrator window, choose a site, and then choose **Protocols**.
2. Double-click **HTTP (Web) Site Settings**.
3. Select the **Folder Shortcuts** tab.



Working with Public Folder Shortcuts

Public folder shortcuts are displayed to anonymous users logging on to the Microsoft Exchange Server computer from the Internet. Use the **Folder Shortcuts** property page to select a public folder or set of public folders that you want to create shortcuts to, view details of a folder, or remove a folder.

1. Select the **Folder Shortcuts** tab.
2. Choose an option.

Option	Description
New	Displays a list of all public folders. When you select a public folder, a shortcut is automatically created and appears in the **Public folder shortcuts** box.
Properties	Displays the properties for the selected public folder.
Remove	Removes the selected public folder from the **Public folder shortcuts** box.

Setting Public Folder Anonymous Permissions

Published public folders must have at least Read permission granted to Anonymous. This is set in the **Permissions** property page of the specified folder.

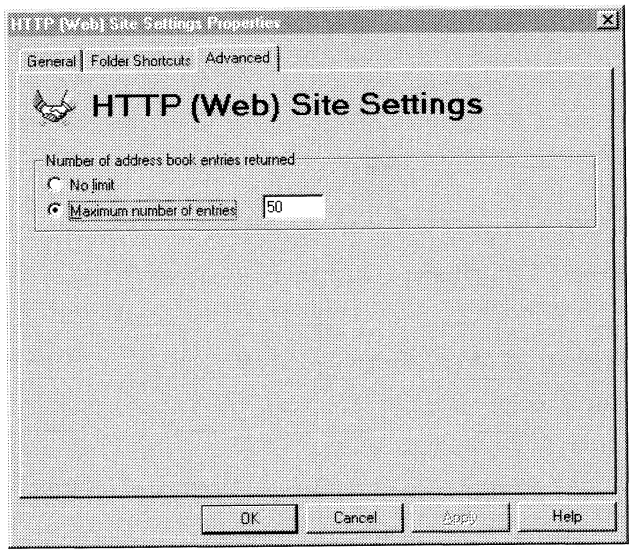
1. Select the **Folder Shortcuts** tab.
2. Select the public folder shortcut you created, and then choose **Properties**.
3. Choose **Client Permissions**.
4. In the box at the top of the **Client Permissions** dialog box, select **Anonymous**, and change its role and capabilities to the appropriate level of access. If you want to publish all subfolders of this folder for anonymous access, select the **Propagate these properties to all subfolders** check box.
5. Choose **OK**.

Advanced Properties

Use the **Advanced** property page to set the number of Address Book entries returned to all users. The default limits users to 50 entries.

Getting to the Advanced property page

1. In the Administrator window, choose a site, and then choose **Protocols**.
2. Double-click **HTTP (Web) Site Settings**.
3. Select the **Advanced** tab.



Setting the Number of Address Book Entries Returned

You can limit the number of Address Book entries that are returned to the user. If a request returns a greater number than the default value, a message informs the user to refine the search.

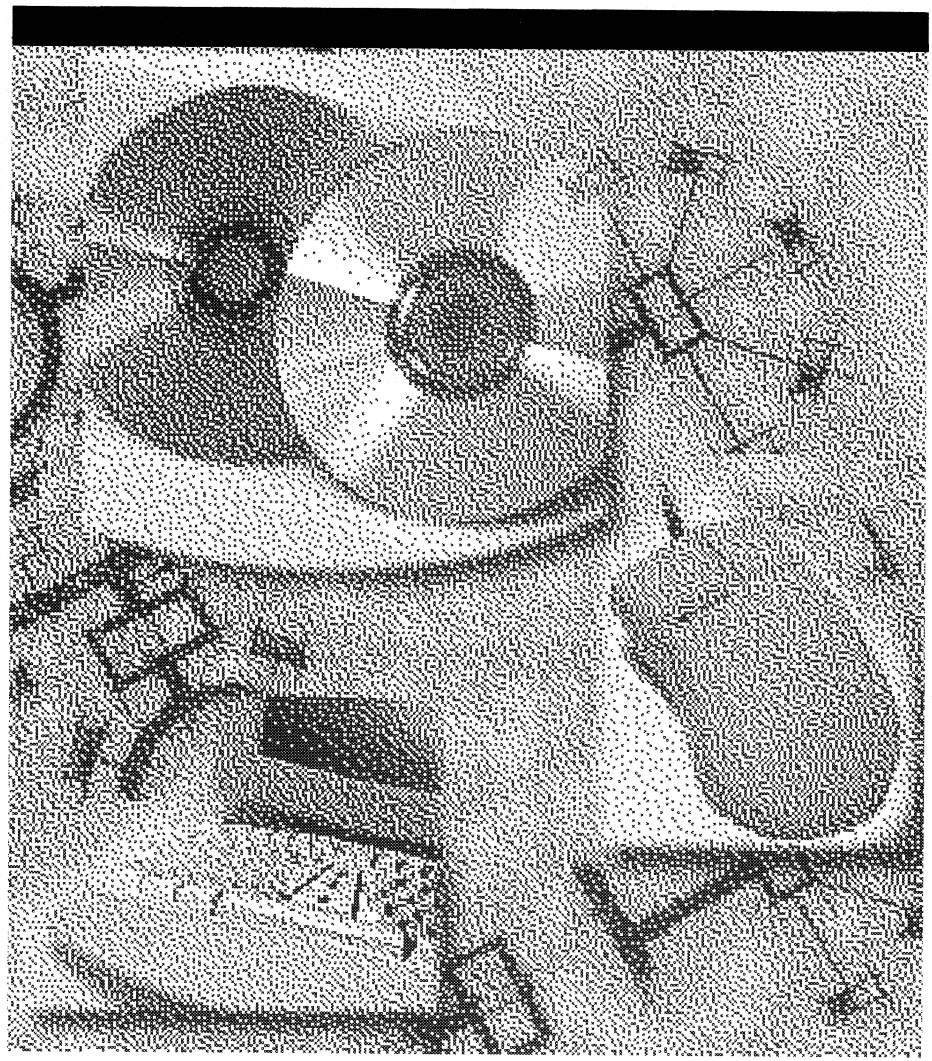
Note If you do not set a limit, the entire Address Book is displayed. This is not desirable for large directories.

1. Select the **Advanced** tab.
2. Select an option.

Option	Description
No limit	Select to display an unlimited number of Address Book entries to the user.
Maximum number of entries	Select to limit the number of Address Book entries returned to the user, and then type a number. The default is 50.

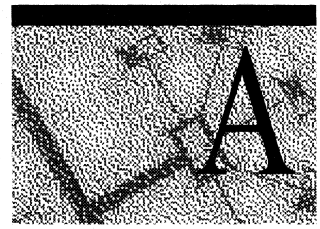
PART 4

Appendixes



APPENDIX A

Setting Up Windows NT Server for RAS Connectivity



This appendix describes how to configure Microsoft Windows NT Server version 4.0 and Microsoft Exchange Server to run the Dynamic RAS Connector using Transport Control Protocol/Internet Protocol (TCP/IP).

Note To avoid problems with name resolution, Microsoft Exchange Server computers using the Dynamic RAS Connector should not have local area network (LAN) connectivity to each other. If a LAN connection has already been established, restart the servers to clear any cached connectivity information.

You should also ensure that Windows NT Server and Microsoft Exchange Server have been updated to the latest Service Pack levels.

RAS Server Configuration

To use the Dynamic RAS Connector to establish Remote Access Service (RAS) connectivity between two Microsoft Exchange Server computers, both servers must have TCP/IP installed and must be correctly configured. To install TCP/IP and configure the server, you need to:

- Configure the modem and port.
- Enable TCP/IP for both incoming and outgoing connections.
- Create a pool of TCP/IP addresses for RAS.

Each of these steps is described in more detail in the following sections.

Configuring the Modem and Port

Use the following procedure to configure the modem and port.

1. In Control Panel, double-click the Network icon.
2. Select the **Services** tab.
3. Select **Remote Access Service**, and then choose **Properties**. If **Remote Access Service** does not appear, choose **Add** to install it.
4. Verify the **Port** and **Device** settings, and then choose **Configure**.
5. If you want bidirectional connectivity, under **Port Usage**, select **Dial out and Receive calls**.

Enabling TCP/IP

Use the following procedure to enable TCP/IP.

1. In Control Panel, double-click the Network icon.
2. Select the **Services** tab.
3. Select **Remote Access Service**, and then choose **Properties**.
4. Choose **Network**.
5. Under **Dial out Protocols**, select **TCP/IP**.
6. Under **Allow remote clients running**, select **TCP/IP**.

Creating a Pool of TCP/IP Addresses for RAS

To ensure RAS connectivity, you need to create an address pool with at least two TCP/IP addresses. If you are using multiple modem lines, the pool must contain at least one more address than the number of ports. For example, if a four-port Digiboard is being used, there must be at least five addresses in the pool. The local server uses the first address, and the others are assigned to the servers that dial in.

The IP addresses you select for your address pool do not need to correlate with other internal or external IP address schemes. Addresses from the pool will only be used by the two computers at each end of the RAS connection.

For example, the pools for each of three Microsoft Exchange Server computers connected using a Dynamic RAS Connector may appear as follows.

Server	Domain	IP Address
Seattle	WASHINGTON	207.68.142.142
Portland	OREGON	207.68.151.151
Dallas	TEXAS	204.95.110.110

Server	Modems	RAS IP Address Pool
Seattle	4 modems	131.107.10.1 to 131.107.10.5
Portland	1 modem	131.107.20.1 to 131.107.20.2
Dallas	1 modem	131.107.30.1 to 131.107.30.2

Complete the following steps to create a TCP/IP address pool.

1. In Control Panel, double-click the Network icon.
2. Select the **Services** tab.
3. Select **Remote Access Service**, and then choose **Properties**.
4. Choose **Network**, and then choose **Configure**.
5. Select **Use static address pool**, and then type the appropriate numbers in the **Begin** and **End** fields.

TCP/IP Configuration

The Microsoft Exchange Server computer should be configured to use a static IP address for its Network Interface Card (NIC).

1. In Control Panel, double-click Network.
2. Select the **Protocols** tab.
3. Select **TCP/IP Protocol**, and then choose **Properties**.
4. In the **IP Address** tab, select **Specify an IP address** and enter the appropriate information in the **IP Address** and **Subnet Mask** fields.

Lmhosts File

The Lmhosts file resolves IP addresses with domain names. When setting up for RAS connectivity, you need to add the IP address and domain of each Microsoft Exchange Server computer to the Lmhosts file on the RAS server.

If the Lmhosts file already exists, it will be located in the Winnt40\System32\Drivers\Etc directory. If this file does not exist, you need to create it. If you are not familiar with Lmhosts files, you should review the Lmhosts.sam file provided with Windows NT. This sample file is also located in the Winnt40\System32\Drivers\Etc directory.

Enabling Lmhosts Lookup Functionality

To work with the Lmhosts file, you must first enable Lmhosts lookup functionality.

1. In Control Panel, double-click Network.
2. Select the **Protocols** tab.
3. Select **TCP/IP Protocol**, and then choose **Properties**.
4. Select the **WINS Address** tab, and then select the **Enable LMHOSTS Lookup** check box.

Modifying Lmhosts Files

You must edit the Lmhosts file to include the server names and IP addresses for each Microsoft Exchange Server computer that you plan to connect using the Dynamic RAS Connector.

The file should include the server name and the IP address of the NIC from the opposing Microsoft Exchange Server computers. The LMHOSTS entry should be followed by a #PRE entry, and a #DOM:<*domain name*> entry if the server specified is a primary domain controller (PDC) or a backup domain controller (BDC) responsible for validating logons. For example, the Lmhosts file for each of three Microsoft Exchange Server computers connected through a Dynamic RAS Connector would contain the following lines:

Seattle

207.68.151.151	PORTLAND	#PRE	#DOM:OREGON
204.95.110.110	DALLAS	#PRE	#DOM:TEXAS

Portland

207.68.142.142	SEATTLE	#PRE	#DOM:WASHINGTON
204.95.110.110	DALLAS	#PRE	#DOM:TEXAS

Dallas

207.68.142.142	SEATTLE	#PRE	#DOM:WASHINGTON
207.68.151.151	PORTLAND	#PRE	#DOM:OREGON

Guidelines for Working with Lmhosts Files

When working with Lmhosts files, you should do the following:

- When you reach the bottom of the file, press ENTER several times to create blank lines before saving the file.
- Use only uppercase characters.
- Save the file without an extension (such as the default .txt extension that is automatically appended by Notepad).
- Save the Lmhosts file as a text file (but if Notepad is used to save the file, make sure that Unicode is not selected as the file type in the **Save file** dialog box).
- Verify that the name of the Lmhosts file is spelled correctly.

Verifying the Lmhosts File

You can verify that the contents of the Lmhosts file can be interpreted by Windows NT using the **Nbtstat** command.

Complete the following steps to verify the Lmhosts file.

1. At the command prompt, type **Nbtstat -R**. (Note that the *R* must be uppercase).

   This will purge the existing cache and load any entries in the Lmhosts file.
2. Type **Nbtstat -c** to view the contents of the cache.

The Microsoft Exchange Server computer names entered when generating the Lmhosts file should be displayed in the cache. If not, the Lmhosts file or Windows NT is not correctly configured.

RAS Client Configuration

When configuring the RAS client, you must create a RAS phone book entry on the Microsoft Exchange Server computer and configure that entry to use only TCP/IP.

Complete the following steps to create a RAS phone book entry.

1. From the **Start** menu, choose **Programs**, and then choose **Accessories**.
2. Choose **Dial-Up Networking**.
3. Create a phone book entry by choosing **New**, and then following the instructions in the wizard.
4. Enter a description and the phone number of the RAS server.
5. With the phone book entry open, choose **More**.
6. From the list, select **Edit entry and modem properties**.
7. Select the **Server** tab.
8. Under **Network protocols**, select **TCP/IP**. Make sure that no other protocol is selected.

Windows NT RAS Authentication

Windows NT RAS supports two authentication mechanisms. It can use the credentials of the currently logged on user to establish the connection to the remote server or use credentials that have been supplied by the user.

To choose which method to use, select or clear the **Use current user name and password** check box.

Using Credentials Defined by the Service Account

If the **Use current user name and password check box** is selected, Microsoft Exchange will use the credentials of the Microsoft Exchange service account specified during Setup. These are the credentials used by the message transfer agent (MTA), and are therefore the only default credentials available.

If the local service account has full Administrator permissions in the remote Microsoft Exchange site, this method will work. However, the Microsoft Exchange MTA requires a full-duplex communication link between the two systems. This means that the remote MTA will attempt to bind back to the local computer. To accomplish this, the credentials from the remote system must also be present and validated to access the local system.

Using Credentials Supplied by the User

If the **Use current name and password** check box is not selected, credentials must be provided when the Microsoft Exchange MTA attempts to connect to the remote server. To accomplish this, the local MTA will use the account information in the **RAS Override** property page of the Dynamic RAS Connector. The information supplied in the property page should be an authorized account in the remote system that can both log on to the remote system and access the Microsoft Exchange Server directory database with full permissions.

1. With the **Edit Phone Book Entry** dialog box open, select the **Security** tab.
2. Select the **Accept only Microsoft encrypted authentication** check box.
3. Verify that the **Use current username and password** check box is not selected.

Creating Override Accounts

You can create Windows NT accounts to be used in the **RAS Override** property page of the Dynamic RAS Connector. To configure an account, use the Windows NT User Manager for Domains.

Complete the following steps to create Windows NT accounts.

1. From the **Start** menu, choose **Programs**, choose **Administrative Tools**, and then choose **User Manager for Domains**.
2. From the **User** menu, choose **New User**.
3. Enter the same user name and password for each domain, and follow the same capitalization for each name. For example:

   Username = RASCON

   Password = RAS

In the three-server example described earlier, the following accounts could be created:

Domain	UserName	Password
WASHINGTON	RASCON	RAS
OREGON	RASCON	RAS
TEXAS	RASCON	RAS

Note Although you can choose any name for the account name and password, as mentioned earlier, the names must be identical for each domain.

After you create the Windows NT accounts, you must grant these accounts dial-in access.

Complete the following steps to grant dial-in access to Windows NT accounts.

1. In User Manager for Domains, from the **User** menu, choose **Properties**.
2. Select the account you want to grant dial-in access to.
3. Choose **Dialin**.
4. Select the **Grant dialin permission to user** check box.

After you grant the accounts dial-in access, you need to grant these accounts permission to access Microsoft Exchange Server.

Complete the following steps to provide Windows NT accounts Microsoft Exchange Server permissions.

1. In the Microsoft Exchange Server Administrator window, select a server.
2. From the **File** menu, choose **Properties**.
3. Select the **Permissions** tab. If you don't have a **Permissions** tab, you may need to log in using an account with Microsoft Exchange Server Permissions Admin or Service Account Admin roles. Or, from the **Tools** menu in the Administrator window, choose **Options**. Select the **Permissions** tab, and then select the **Show Permissions page for all objects** and **Display rights for roles on Permissions page** check boxes.
4. Under Windows NT accounts with permissions, choose Add.
5. Under **Names**, select the Windows NT account you want to add.
6. Choose **Add**, and then choose **OK**.
7. Under Roles, select Service Account Admin.

Index

\ (back slash) 412, 432
/ (slash mark) 412, 415, 432
@ (at sign) 413
% (percent symbol) 80, 81, 82, 83
* (asterisk) 80, 81, 82, 83
16 bit help files 37
32 bit help files 37
3DES encryption algorithm 64

A

A (address) records, defined 89
Accepting
  connections, Internet protocols 390
  messages
    cc:Mail Connector 223
    directory synchronization 361
    distribution lists 18
    Dynamic RAS Connector 156
    Internet Mail Service 111
    X.400 Connector 193
Access component, Microsoft Mail (PC) gateway 311
Access connection gateways
  extracting 263
  installation 264
  overview 263
Accounts
  Internet Mail Service, logon information 117
  names
    IMAP4rev1 432
    POP3 412
  NNTP 498
  outbound host connections 466
  override, RAS authentication 521
  service
    Dynamic RAS Connector 151
    Site Connector 140
Active file
  defined 455
  newsgroups
    inbound pull feeds 472
    inbound push feeds 474
    NNTP 483
Active Server, Microsoft Outlook Web Access 502
Add transactions 352
Adding
  advanced security administrators 48
  connected sites, Dynamic RAS Connector 159
  distribution list members 4, 5, 17
  Internet Mail Service
    additional 123
    routing addresses 121
  Internet protocols rules 391
  new recipient objects to container, Address Book views 32
  newsgroup public folders 459
  newsgroups
    inbound pull feeds 471
    outbound feeds 475
  RAS connections 115
  target servers, Site Connector 139
  X.400 Connector 173, 189
Additional sites, enabling 70
Address Book
  See also Address spaces; Addresses
  custom recipients 9
  described 23
  details templates
    controls 37 – 39
    described 35
    display names 36
    foreign language 40, 41
    help files 37
    modifying, overview 37
  directory synchronization
    accepting messages 361
    rejecting messages 362
  distribution lists
    display name 5
    hiding 8, 14
  downloading offline 29
  foreign language details templates 40, 41
  Microsoft Outlook Web Access 510
  one-off address templates
    described 39
    help files 40
    viewing 39
  views
    adding new recipient objects to container 32
    advanced properties 29 – 31

Address Book (*continued*)
views (*continued*)
calculating membership 34
configuration 27 – 31
creating 24 – 27
customizing hierarchy 32
deleting 34
directory name 26
display name 26, 33
exporting recipients 33
general properties 26
Group By properties 26
moving recipient objects between containers 32
overview 23 – 24
parent containers, promoting entries to 30
permissions 28
removing empty containers 31
restricting for anonymous users 33
restricting offline 28
restrictions 28
setting up large 34
showing 31
Address books, directory exchange requestor 353
Address spaces
See also Address Book; Addresses
case 81
cc:Mail Connector 218 – 220
comparing 83
costs 80
defined 79
Dynamic RAS Connector
costs 157, 158
defining 158
properties 157
general properties 80 – 84
general type 83 – 84
Internet Mail Service 109 – 110, 110
Internet type 79, 80, 81
Microsoft Mail Connector
configuration 312 – 315
foreign systems 314
overview 312
properties 250 – 253
wildcard characters 314
Microsoft Mail type 79, 80, 82
MSA type 250
prefixes 83
restrictions 84
Site Connector
costs 137
defining 137
properties 137
Address spaces (*continued*)
SMTP type 79, 80, 81
types *See specific address space types*
wildcards 80, 81, 82, 83, 314
X.400 Connector 187
X.400 type 79, 80
Addresses
See also Address Book; Address spaces
A (address) records 89
addressing templates *See* Addressing templates
cc:Mail Connector
bulletin boards 231
e-mail, generator 209, 220
e-mail, modifying 231
import container filter configuration 214
imported 211
propagating listings 207
public folders 231
CCMAIL type 219, 220
custom recipients
e-mail 11
information 11
directory exchange requestor
filters 349
manually exporting changes 352
manually importing changes 351
removing 353
removing Microsoft Exchange Server recipients 354
resynchronizing information 354
transferring information 350
types 349
updates 346, 351
viewing gateway recipient information 351
directory synchronization
delivery restrictions 359 – 362
e-mail, changing 358
e-mail, creating 358
e-mail, overview 357
e-mail, removing 359
Internet 357
Microsoft Mail (PC) 357
X.400 357
dirsync requestor
foreign types 322
import container 324
updates 327, 329
dirsync server, updates 334
disabling display names 96
IMAP4rev1 e-mail 433

Addresses (*continued*)
Internet Mail Service
connected sites 107
matching domain names 118
routing for address spaces 110
routing, adding 121
routing, editing 121
routing, removing 121
user name resolution 126
Internet protocols
access by 389
adding rules 391
IP, Internet Mail Service 89, 90
manual directory synchronization 370
Microsoft Mail (Appletalk) 261, 345, 352
Microsoft Mail (PC) 319, 325, 352
Microsoft Mail Connector regeneration 246
MSA address type 266
one-off address templates *See* One-off address templates
POP3 e-mail 413
Quarterdeck Mail 266
RAS server configuration, TCP/IP 516
remote dirsync requestor
import container 340
type 337
routing
Dynamic RAS Connector connected sites 160
X.400 Connector connected sites 190
USENET host computer, IP 462
X.400, Dynamic RAS Connector 160
Addressing templates, foreign language 40, 41
ADE (Automatic Directory Exchange) 207
Administrator
advanced security, properties
adding administrators 48
changing passwords 48
overview 47
removing administrators 48
Internet Mail Service, NDRs 92
mailbox
cc:Mail Connector 205
directory synchronization 359
dirsync server 332
Internet Mail Service 92
Microsoft Mail Connector 242, 275
NNTP newsfeeds 459
Schedule+ Free/Busy Connector 375, 377
Schedule+ Administrator program 375
AdminSch accounts, Schedule+ Free/Busy Connector 375
Advanced configuration, Internet Mail Service 125 – 130
Advanced directory synchronization functions 328
Advanced properties
Address Book views 29 – 31
X.400 Connector 194 – 197
Advanced security
administrators properties
adding administrators 48
changing passwords 48
overview 47
removing administrators 48
backing up data 72
CA permissions 60
CA property pages 45
Certificate Trust Lists
importing 56
overview 55
removing 57
revoking 57
viewing 58
configuration, overview 45
described 43
enabling additional sites 70
enrollment properties
bulk enrollment 53
certificates, compatible 54
overview 51
transmitting temporary keys 52
welcome message 52
general properties 59
KM Server
configuration 44
described 43
installation 44
starting 45
mailboxes
enabling 66
overview 65
recovering keys 69
revoking 68
temporary keys 66
viewing 69
moving KM server between sites 75
moving users between KM servers 73
passwords properties
multiple passwords policy 50
overview 49
remote sites 72
restoring data 72
site
choosing sites 62
display name 62
encryption algorithms 63 – 65

Advanced security (*continued*)
site (*continued*)
general properties 62
overview 60
permissions 63
Site Encryption Configuration property pages 45
viewing log 73
Algorithms, encryption 63 – 65
Alias names
anonymous connections, IMAP4rev1 421
cc:Mail Connector 215
custom recipients 10
directory exchange requestor 353
distribution lists 5
IMAP4rev1 432
NNTP client configuration 498
POP3 412
Schedule+ Free/Busy Connector 380
Alternate recipients 20
Anonymous
connections
directory attributes 440
IMAP4rev1 421
LDAP 440
NNTP 491
users
Microsoft Outlook Web Access 504, 507, 509
restricting Address Book views 33
ANSI characters, non-, distribution list names 7
Any substring searches 441
Appearance, Address Book details template controls 39
AppleShare 254
Appletalk
See also Microsoft Mail (Appletalk); Microsoft Mail Connector
message size limit 279
Microsoft Mail Connector diagnostics logging 294
.Asp files 502
Association parameters
Dynamic RAS Connector 154
X.400 Connector 186
Asterisk (*) 80, 81, 82, 83
Asynchronous
Dynamic RAS Connector, described 141
Microsoft Mail Connector
Connector (PC) MTAs 282
interchange properties 275 – 277
Microsoft Mail (PC) postoffices 295, 304, 307
MTA configuration 299 – 303
MTA setup 301
overview 271
setting options 298
setup 272 – 273, 295 – 297
At sign (@) 413
AT&T Easylink gateway 308
Attachments
cc:Mail Connector 227
custom recipients 14
IMAP4rev1 429
Internet Mail Service
e-mail domain 97
format 93
Macintosh files 123
maximum message size 112
rich text formatting 95
NNTP 495
POP3 403, 409
X.400 Connector, MAPI 176
Attributes
custom recipients 21 – 22
directory
anonymous user access 440
searches 441
Authentication
IMAP4rev1 418
Internet Mail Service 122
LDAP 438
Microsoft Outlook Web Access 503 – 504
NNTP
custom recipients 493
mailboxes 493
newsfeeds 485
POP3 399
Windows NT
anonymous connections 440, 491
Auto Naming, custom recipients 10
Automated directory synchronization *See* Directory synchronization
Automatic Directory Exchange (ADE) 207
Automatic replies 96

B

Back slash (\ ) 432
Backing up security data 72
Backlogs, Internet Mail Service 123
Backup utility *See* Windows NT Backup utility
Balancing load, Internet Mail Service 109
Bcc feature 269
Bi-directional newsfeeds, Internet News Service configuration 455
Binhex
attachment format 93
NNTP messages 489
POP3 messages 404

Body parts, X.400 Connector 195
Bold
  Internet Mail Service 95
  POP3 403
  X.400 Connector 176
Bridgehead server
  messaging *See* Messaging bridgehead servers
  Site Connector 136
Browsers, Web, Microsoft Outlook Web Access
  enabling access 506
  installation 502
Bulk Advanced Security tool 74
Bulletin boards, cc:Mail Connector
  distribution lists 233
  e-mail addresses 231
  names, imported 211
  overview 230
  propagating messages 231, 232
Busy times, defined 373

C

CA property pages 45
Calculation, Address Book views, membership 34
Cancel control message 453
CAs
  display name 59
  permissions 60
Case, address spaces 81
CAST-40 encryption algorithm 64
CAST-64 encryption algorithm 64
Catching up current newsfeeds 453
cc:Mail Connector
  address space 218 – 220
  administrator's mailbox 205
  attachments 227
  Automatic Directory Exchange (ADE) 207
  bulletin boards 230
  configuration 204
  connected post office 206
  connections, testing 225, 226
  delivery restrictions 223
  diagnostics logs 222
  directory synchronization 211, 216
  distribution lists 212, 233
  e-mail address generator 220
  export containers 209
  Export version 206
  foreign address name (FAN) field 212
  general properties 208
cc:Mail Connector (*continued*)
  import containers
    alias name rules 215
    directory synchronization 214
    display name rules 215
    filter configuration 214
    moving within a site 230
    overview 211
    selecting 213
  Import version 206
  installation 201
  logging events 223
  message size 209
  moving
    overview 228
    to another site 228
    within a site 229
  Netware server connections 223
  overview 201
  post office language 207
  post office options 207
  post office properties 205 – 207
  propagating messages 231, 232
  proxy names 211, 220
  public folders 230
  queues
    deleting messages 222
    overview 221
    refreshing view 222
    viewing 222
  quick start 202
  Router program 231
  setup 202
CCMAIL address type 219, 220
Certificate Server *See* Microsoft Certificate Server
Certificate Trust Lists
  importing 56
  overview 55
  removing 57
  revoking 57
  viewing 58
Certificates
  disabling mailbox security 68
  formats 54
  issuing compatible 54
Certification authorities *See* CAs
Certification Revocation Lists *See* CRLs
Challenge/Response
  IMAP4rev1 420
  Microsoft Outlook Web Access 503
  NNTP 485
  POP3 401

Changing
computer name 278
directory synchronization
e-mail addresses 358
incoming template mappings 364
outgoing template mappings 365
Character sets
IMAP4rev1 424, 429
Internet Mail Service 94, 97
newsgroup public folders 497
NNTP 495
POP3 404, 409
Characters
Internet Mail Service 95
non-ANSI, distribution list names 7
POP3, rich text formatting 403
rich text, custom recipients 14
wildcards 80, 81, 82, 83, 314
Checkpoint size, X.400 Connector 185
Clients
Internet News 498
Microsoft Mail (PC), Microsoft Mail Connector 293
Microsoft Mail 3.x, compatibility 277
NNTP
access 480
configuration 498 – 500
RAS, configuration 520
S/MIME support 98
CLNP, X.400 Connector MTA transport stack 164
Code pages
defined 207
MAPI 404, 424, 498
Color
Internet Mail Service 95
POP3 403
X.400 Connector 176
Columns, fixed-width fonts 98
Company information, custom recipients 11
Compatibility
certificates 54
Microsoft Mail 3.x client 277
Configuration
Address Book views 27 – 31
administrators properties
adding administrators 48
changing passwords 48
overview 47
removing administrators 48
advanced security, overview 45
bi-directional newsfeeds 455
CA permissions 60
Configuration (*continued*)
cc:Mail Connector
address space 219
import container filter 214
overview 204
post office options 207
Certificate Trust Lists
importing 56
overview 55
removing 57
revoking 57
viewing 58
custom recipients 9
directory exchange requestor 346
directory synchronization
incoming template mappings 363
outgoing template mappings 365
overview 355
distribution lists 5
Dynamic RAS Connector 145, 515, 520
enrollment properties
bulk enrollment 53
certificates, compatible 54
overview 51
transmitting temporary keys 52
welcome message 52
general properties, advanced security 59
IMAP4rev1
client 432 – 434
mailboxes 415, 427 – 429
sample client 434
servers 415 – 427
sites 415 – 427
Internet Mail Service
advanced 125 – 130
installation 87 – 90
POP3 410, 430
TCP/IP 88
Internet News Service
inbound newsfeeds 449, 455
Newsfeed Configuration Wizard 455
outbound newsfeeds 449
push feeds 455
scenarios 455
KM Server 44
LDAP
servers 435 – 440
sites 435 – 440
Microsoft Exchange Connection 259 – 262
Microsoft Mail (Appletalk), directory exchange requestor 344
Microsoft Mail (PC), dirsync requestor 322

Configuration (*continued*)
Microsoft Mail Connector
address space 312 – 315
administering 274
Interchange 241 – 244
interchange properties 275 – 277
MTA 282 – 289
Microsoft Mail directory server 330
Microsoft Outlook Web Access 504 – 511
NNTP
clients 498 – 500
newsfeeds 456 – 469
properties 479
passwords properties
multiple passwords policy 50
overview 49
POP3
client 411 – 414
mailboxes 397, 407 – 409
sample client 414
servers 397 – 407
sites 397 – 407
RAS client 520
remote directory requestor 343 – 355
Schedule+ Free/Busy Connector 376 – 380
Site Connector 134
X.400 Connector
foreign systems 197
MTA conformance 195
overview 171
remote global domain identifier (GDI) 197
Confirmation messages, Microsoft Mail Connector
connection changes 281
Conformance, MTA, X.400 Connector 195
Connected sites
Dynamic RAS Connector
adding or changing 159
costs 160
properties 158
removing 161
routing address 160
Internet Mail Service 107 – 108
messaging bridgehead servers 163
X.400 Connector
adding 189
costs 190
overview 189
removing 190
routing address 190
testing 198, 199
Connection times, Microsoft Exchange Connection gateway 262
Connections
anonymous
IMAP4rev1 421
LDAP 440
NNTP 491
asynchronous *See* Asynchronous
cc:Mail Connector, Netware server 223
Host computers, NNTP, removing inbound 462
Internet Mail Service
accepting messages from all hosts 103
accepting messages from secure hosts 103
accepting messages from specific hosts 104
connected sites properties 107
delivering messages by e-mail domain 102
delivering messages to single host 102
loopback detection 127
retry interval 105
scheduling 117
security 122
setting number of 100
Internet News Service 448
Internet protocols
accepting 390
adding rules 391
custom recipients 395
disabling 395
editing rules 392
mailbox configuration 395
MIME types 393 – 394
moving rules 392
overview 389
rejecting 390
removing rules 391
LAN *See* LANs
Microsoft Mail Connector *See* Microsoft Mail Connector
NNTP newsfeeds, scheduling 468
RAS phone book
adding 115
dial-up connections properties 114
viewing 114
secure, Internet 455
SSL, NNTP client configuration 499
X.25 *See* X.25
X.400 Connector
retry, overriding 186
schedule 178
Connections properties, Internet Mail Service 99 – 106
Connector (PC) MTAs
asynchronous connection
configuration 299 – 303
setup 301

Connector (PC) MTAs (*continued*)
Microsoft Mail Connector
configuration 282 – 289
options 286
postoffices, setting options 289
postoffices, specifying 288
removing 288
setup 284
X.25 connection
configuration 299 – 303
modifying 303
setup 302
Connectors
cc:Mail
address space 218 – 220
administrator's mailbox 205
attachments 227
Automatic Directory Exchange (ADE) 207
bulletin boards 230 – 232
configuration 204
connected post office 206
connections, testing 225, 226
delivery restrictions 223
diagnostics logs 222
directory synchronization 211, 216
distribution lists 212, 233
e-mail address generator 220
export containers 209
Export version 206
foreign address name (FAN) field 212
general properties 208
import containers 211 – 215
Import version 206
installation 201
message size 209
moving 228 – 230
Netware server connections 223
overview 201
post office language 207
post office options 207
post office properties 205 – 207
propagating messages 231, 232
proxy names 211
public folders 230 – 233
queues 221 – 222
quick start 202
Router program 231
setup 202
Dynamic RAS Connector
accepting messages 156
address space properties 157 – 158
configuration 145, 515
Connectors (*continued*)
Dynamic RAS Connector (*continued*)
connected sites 158 – 161
defined 133
delivery restrictions 155
described 141
general properties 147 – 148
installation 145
message size 148
MTA override properties 152 – 155
MTA transport stack 141 – 144, 147
name 147
override association parameters 154
override connection retry values 153
override RTS values 153
override transfer time-outs 154
permissions 161
phone book entry 148
RAS callback telephone number 152
RAS client configuration 520
RAS override properties 150 – 152
RAS server configuration 515 – 517
rejecting messages 156
remote server name 147
schedule properties 149 – 150
service accounts 151
setup requirements 141
TCP/IP configuration 517 – 519
Windows NT RAS authentication 520 – 522
Internet Mail Service
accepting messages from all hosts 103
accepting messages from secure hosts 103
accepting messages from specific hosts 104
accepting messages from specific senders 111
adding additional 123
adding RAS connections 115
adding routing addresses 121
address spaces 109 – 110
administrator's mailbox 92
advanced configuration 125 – 130
attachment format 93
automatic replies 96
character sets, default 94
connected sites properties 107 – 108
connections properties 99 – 106
connections, number of 100
custom routing programs 122
customizing 91
defined 133
delivering messages by e-mail domain 102
delivering messages to single host 102

Connectors (*continued*)
Internet Mail Service (*continued*)
delivery restrictions 111
diagnostics logging properties 113
dial-up connections properties 114 – 117
disabling display names 96
disabling ETRN support 131
disabling S/MIME support 98
DNS routing 101
editing routing addresses 121
e-mail domain 97
ESMTP 130 – 132
fixed-width fonts 98
general properties 112 – 113
installation 87 – 90
Internet Mail properties 92 – 98
logon information 117
loopback detection 127
Macintosh file attachments 123
mail retrieval options 115
maximum message size 112
maximum messages sent 100
message time-out values 105
message tracking 129
MIME types 123
NDRs 92
notifications 106
out-of-office replies 96
overview 87
permissions 113
queues properties 113
RAS connection time-out 116
rejecting messages from specific senders 111
removing 124
removing routing addresses 121
retry interval 105
reverse resolution 125
rich text formatting 95
routing addresses for address spaces 110
routing destinations 120
routing methods 120
routing properties 118 – 122
scheduling connections 117
security properties 122
text quoting 128
transfer modes 100
user name resolution 126
viewing RAS connections 114
VRFY 127

Connectors (*continued*)
Microsoft Mail
Appletalk, overview 235
Appletalk, requirements 236
Microsoft Mail (Appletalk) directory exchange requestor 344
Microsoft Mail Connector
access connection gateway 263 – 265
address regeneration 246
address space 312 – 315
address space properties 250 – 253
administrator's mailbox 242, 275
Appletalk, MTA, defined 235
Appletalk, MTA, diagnostics logging 254
Appletalk, MTA, message queue 248
Appletalk, MTA, postoffice names 246
Appletalk, MTA, setting up 243
asynchronous connection 295 – 298
asynchronous MTA configuration 299 – 303
client compatibility 277
computer name 278
configuration 274 – 279
connections properties 247
delivery messages 242, 275
diagnostics logging 253
gateways 308 – 311
general properties 249, 277 – 279
installing Microsoft Exchange Connection 255
installing Microsoft Exchange Connection files 257
installing Microsoft Exchange Connection gateway 257
Interchange, configuration 241 – 244
Interchange, defined 235
LANs connection 279 – 294
local postoffice properties 244
Macintosh-accessible volume 238
message size limit 250, 279
message tracking 243, 277
Microsoft Exchange Connection configuration 259 – 262
Microsoft Exchange Connection gateway connection times 262
Microsoft Exchange Connection gateway options 261
Microsoft Exchange Connection location 259
Microsoft Exchange Connection, Appletalk, defined 235
Microsoft Exchange Connection, Appletalk, requirements 237
Microsoft Exchange Connection, Appletalk, setup 254 – 265

Connectors (*continued*)
Microsoft Mail Connector (*continued*)
Microsoft Mail (Appletalk) message queue 248
Microsoft Mail (Appletalk) permissions 240
Microsoft Mail (PC) Gateways 308 – 311
Microsoft Mail (PC) postoffice configuration 304
Microsoft Mail (PC) postoffice, testing connection 304
Microsoft Mail (PC) postoffices indirect connections 305 – 308
passwords 245
PC, overview 271 – 272
postoffice, defined 235
postoffice, Macintosh-accessible volume 238
primary language 276
quick start 238, 273
routing 252
setup 237, 272 – 273
testing connections 268
X.25 connection 295 – 298
X.25 MTA configuration 299 – 303
Microsoft Mail for Appletalk Networks Connection Gateway 265
paths *See* Address spaces
RAS Connector *See* Dynamic RAS Connector
restrictions, address spaces 84
Schedule+ Free/Busy Connector
administrator's mailbox 377
AdminSch accounts 375
alias name 380
configuration 376 – 380
display name 380
distribution list, assigning 377
distribution list, exporting 378
exporting updates 378
general properties 379
installation 374 – 375
logging level 379
overview 373
Schdist.exe 375
Schedule+ Administrator program 375
Schedule+ program files 375
setup 374
unresolved messages 381
update frequency 378
Site Connector
address spaces 137 – 138
bridgehead server 136
configuration 134
defined 133
general properties 135 – 136

Connectors (*continued*)
Site Connector (*continued*)
installation 134
name 136
override properties 140
routing costs 136
setup requirements 133
target servers properties 138 – 139
Windows NT Server trust relationships 140
X.400 Connector
accepting messages from specific senders 193
adding 173
address space properties 187
address type 349
advanced properties 194 – 197
association parameters, overriding 186
body parts 195
configuration 171
connected sites 189 – 190
connected sites, testing 199
connection retry, overriding 186
connection schedule 178
connector name 174
defined 133
delivery restrictions 192
directory name 174
display name 174
foreign sites, testing 198
foreign systems configuration 197
general properties 173 – 176
installation requirements 163
link options 196
local MTA name, overriding 184
local MTA password, overriding 184
message size 196
message text word-wrap 175
MTA conformance, configuration 195
MTA transport stack 164 – 170
override properties 183 – 187
overview 163, 171
permissions 197
rejecting messages from specific senders 193
remote global domain identifier (GDI) 197
remote MTA name 174
remote MTA password 174
remote transport stack 175
removing 200
resetting override values 187
rich text 176
RTS values, overriding 185
schedule properties 177

Connectors (*continued*)
X.400 Connector (*continued*)
stack properties 178 – 182
TCP/IP connection 179
TP4 connection 182
transfer timeouts, overriding 187
X.25 connection 180
Connectors property page, X.400 Connector, MTA transport stack 169
Containers
Address Book views
adding new recipient objects to 32
customizing hierarchy 32
moving recipient objects between 32
parent, promoting entries to 30
removing 32
removing empty 31
cc:Mail Connector
export 209
import 211 – 215
dirsync requestor
export, properties 325 – 326
import, creating 320
import, properties 324 – 325
export *See* Export containers; *specific container types*
import *See* Import containers; *specific container types*
remote dirsync requestor
export, properties 341
import, properties 339
Content, message *See* Messages
Control messages
deleting 453
NNTP 452, 484
Controls, Address Book details templates
changing order 39
creating new 38
editing 38
overview 37
removing 38
reverting to original settings 39
testing appearance 39
Conventions, described xxvii
Costs
Dynamic RAS Connector
address spaces 157, 158
connected sites 160
scheduling 150
Internet Mail Service, routing 109
Microsoft Mail Connector, routing 252
Costs (*continued*)
Site Connector
address spaces 137
routing 136
target servers 139
X.400 Connector
address spaces 188
connected sites 190
Creating
Address Book details templates
controls 38
help files 37
Address Book views 24 – 27
address spaces, Dynamic RAS Connector 158
custom recipients 9
distribution lists 3
e-mail addresses 11, 16, 358
Internet Mail Service connected sites 107
LAN connection 280
MIME types 394
Credentials
RAS authentication
service account 520
user 521
CRLs
importing 56
removing certificates 57
revoking certificates 57
revoking security 68
.Csv file headers 33
Custom
Address Book view hierarchy 32
attributes, recipients 21 – 22
enrollment welcome message 52
recipients
address information 11
advanced properties 12 – 14
attachments 14
cc:Mail Connector e-mail address generator 220
cc:Mail Connector, export containers 209
cc:Mail Connector, import containers 211
company information 11
creating 9
described 9
directory synchronization, trust levels 12
distribution list membership 16
e-mail addresses 11
General property page 9
hiding from Address Book 14
Internet protocols 395

Custom (*continued*)
recipients (*continued*)
message size limit 13
Microsoft NetMeeting 13
Microsoft Outlook Web Access, HTTP, enabling 506
NNTP 493 – 495
NNTP client configuration 498
NNTP newsfeeds 467
organization information 14
phone numbers 15
rich text in messages 14
user name information 10
roles, Internet protocols 389
routing programs 122

D

Data encryption
See also Encryption
described 43
Data Encryption Standard (DES) encryption algorithm 64
Dedicated connections, Internet News Service 448
Deleting
See also Removing
Address Book views 34
cc:Mail Connector, messages from queues 222
containers 32
control messages 453
distribution lists
members 4, 6, 17
owners 6
empty containers, Address Book views 31
Microsoft Mail Connector
connections 282
MTA 288
MTA transport stack 200
newsgroups 453
public folders 453
X.400 Connector 200
Delimiters 412, 432
Delivered messages, newsfeed 453
Delivery
messages
Microsoft Mail Connector 242, 275
options 19 – 21
restrictions
cc:Mail Connector 223
directory synchronization 359 – 362
Dynamic RAS Connector 155
Internet Mail Service 111
recipients 17
X.400 Connector 192
DES encryption algorithm 64
Desktop, directory exchange requestor, locking 350
Destinations, routing, Internet Mail Service 120
Details templates, Address Book
controls
changing order 39
creating new 38
editing 38
overview 37
removing 38
reverting to original settings 39
testing appearance 39
described 35
display names 36
foreign language
installation 41
overview 40
help files 37
modifying 37
Diagnostics logging
cc:Mail Connector 222
Internet Mail Service 113
Microsoft Mail Connector 253, 294
NNTP 493
X.400 Connector, connections 199
Dial-up connections
Internet Mail Service 114 – 117
Internet News Service 448, 464
Digital signatures
Certificate Trust Lists 55
described 43
mailbox security 66
revoking security 68
Directory
import, cc:Mail Connector 215
Internet Mail Service, message archival 113
LDAP
anonymous user access 440
Microsoft Exchange Server 435
searches 441
Macintosh-accessible volume 238
names
Address Book views 26
CAs 59
Dynamic RAS Connector 147
IMAP4rev1 417
Internet protocols 388
LDAP 437
Microsoft Outlook Web Access 506
NNTP 480
NNTP newsfeeds 459

Directory (*continued*)
names (*continued*)
POP3 399
Site Connector 136
Site Encryption Configuration object 62
X.400 Connector 174
replication
Dynamic RAS Connector 158
Internet Mail Service, connected sites properties 107
Internet Mail Service, routing addresses for address spaces 110
requestor, remote, configuration 343 – 355
server, Microsoft Mail *See* Microsoft Mail directory server
Directory exchange requestor
configuration 343
dirsync server 345
log 354
Microsoft Mail (Appletalk)
address filters 349
configuration 346
foreign systems 355
making startup item 351
manually exporting address changes 352
manually exporting world lists 352
manually importing address changes 351
overview 345
removing addresses 353
removing recipients from world lists 354
resynchronizing address information 354
selecting gateway 348
setup 344
starting 350
viewing gateway recipient information 351
update messages 345
Directory synchronization
See also Dirsync requestor; Dirsync server
accepting messages 361
advanced functions 328
cc:Mail Connector
ADE 207
bulletin boards 231
connections, testing 226
export containers 209
import containers 211, 214
moving connector 228 – 230
public folders 231
schedule 216
configuration 355
custom recipients, trust levels 12
defined 317
delivery restrictions 359 – 362
Directory synchronization (*continued*)
diagnostics logging 366
directory exchange requestor
foreign systems 355
resynchronizing address information 354
distribution lists, trust levels 8
e-mail addresses
changing 358
creating 358
overview 357
removing 359
export containers 341
general properties 356
import containers 339
incoming templates
changing mappings 364
mappings configuration 363
overview 362, 364
removing mappings 364
manual
importing master list 369 – 370
remote directory synchronization requestor 370
restarting Microsoft Exchange Directory Synchronization Service 370
Resync.glb file 369, 370
starting 368
Windows NT registry 369
messages, scheduling 330, 334
Microsoft Mail
overview 317
recipient information templates 355
outgoing templates
changing mappings 365
mappings configuration 365
removing mappings 366
rejecting messages 362
starting 366, 368
stopping 367
Dirsync requestor
See also Directory synchronization; Dirsync server
defined 317
import container properties 339
Microsoft Exchange Server 319
Microsoft Mail (PC)
address updates 327, 329
advanced directory synchronization functions 328
creating 320
export container properties 325 – 326
foreign address types 322
general properties 322
import container properties 324 – 325
import container, creating 320

Dirsync requestor (*continued*)
Microsoft Mail (PC) (*continued*)
installation 319 – 330
requirements 320
schedule properties 329
settings properties 327
Microsoft Mail, defined 317
remote
address type 337
creating 335
dirsync server, setting up 331
export container properties 341
general properties 336
importing directory synchronization master list manually 369 – 370
installation 335 – 343
mailbox 337
permissions properties 343
requirements 335
Dirsync server
See also Directory synchronization; Dirsync requestor
creating 331
defined 317
directory exchange requestor 345
directory synchronization, delivery restriction system messages 359
general properties 332
installation 331 – 334
mailbox 332
Microsoft Mail (PC)
directory synchronization requestor 343
mailbox 322
Microsoft Mail, defined 317
overview 331
remote dirsync requestor, import containers 339
requirements 331
schedule properties 334
Disabling
IMAP4rev1 418
Internet Mail Service
automatic replies 96
display names 96
ESMTP support 132
ETRN support 131
out-of-office replies 96
reverse resolution 126
S/MIME support 98
text quoting 128
user name resolution 126
VRFY 128
Internet protocols 395
LDAP 438
Disabling (*continued*)
mailbox security 68
POP3 399
POP3 rich text formatting 403
Dispatch, Microsoft Mail 319
Display names
Address Book details templates 36
Address Book views 26, 33
CAs 59
cc:Mail Connector 215
custom recipients 10
dirsync server 332
distribution lists 5, 7
Dynamic RAS Connector 147
IMAP4rev1 417
Internet Mail Service, disabling 96
Internet protocols 388
KM Server 62
LDAP 437
Microsoft Mail (PC), dirsync requestor 322
Microsoft Outlook Web Access 506
NNTP 480
NNTP newsfeeds 459
POP3 399
remote dirsync requestor 336
Schedule+ Free/Busy Connector 380
Site Connector 136
Site Encryption Configuration object 62
X.400 Connector 174
Distribution lists
Address Book
display name 5
hiding from 8, 14
advanced properties 6 – 8
cc:Mail Connector
administrator's mailbox 205
bulletin boards 233
e-mail address generator 220
export containers 209
public folders 233
recipients, many 212
configuration 5
creating new 3
defined 3
described 16
directory synchronization, trust levels 8
display names 7
expansion server, specifying 5
General property page 4

Distribution lists (*continued*)
members
adding 4, 5, 17
deleting 17
modifying 4
removing 6, 17
messages
accepting and rejecting 18
delivery restrictions 17
size limit 7
name, modifying 4
non-delivery reports 6
out-of-office messages 8
owners
adding 6
deleting 6
modifying 4
reports 8
Schedule+ Free/Busy Connector
assigning 377
exporting 378
setting options 8
X.400 Connector, delivery restrictions 193
DNS
A (address) records 89
Internet Mail Service
adding to DNS 89
routing 101
routing costs 109
MX (mail exchanger) records 89
TCP/IP, Internet Mail Service, installation 88
terms 89
updating Hosts file 90
DNs (distinguished name), Internet Mail Service routing address 107
Documentation, described xxv – xxvii
Domain Name System *See* DNS
Domains
balancing load 109
e-mail
attachment format 93
delivering messages 102
Internet Mail Service 97
maximum message size 112
message content 97
Internet Mail Service
adding to routing 118
matching names 118
name
Internet Mail Service, installation 88
updating Hosts file 90
Domains (*continued*)
outbound messages, routing with DNS 101
Windows NT
IMAP4rev1 432
POP3 412
Downloading
Address Books 28
offline Address Books 29
DS Site Configuration 22
Dynamic RAS Connector
accepting messages 156
address spaces
costs 157, 158
defining 158
properties 157
X.400 157
configuration 145
connected sites
adding or changing 159
costs 160
properties 158
removing 161
routing address 160
defined 133
delivery restrictions 155
described 141
general properties 147 – 148
installation 145
LAN connections 515
message size 148
Microsoft Exchange Server, configuration 515
MTA override properties 152 – 155
MTA transport stack
connectors, defined 144
general properties 143
installation 141
MTA callback telephone number 143
name 143
permissions 144
specifying 147
name 147
override
connection retry values 153
RTS values 153
override
association parameters 154
transfer time-outs 154
permissions 161
phone book entry 148
RAS client configuration 520

Dynamic RAS Connector (*continued*)
RAS MTA transport stack, RAS callback telephone number 152
RAS override properties 150 – 152
RAS server configuration
enabling TCP/IP 516
modem configuration 516
overview 515
port configuration 516
TCP/IP address pool 516
rejecting messages 156
remote server name 147
schedule properties 149 – 150
service accounts 151
setup requirements 141
TCP/IP configuration
Lmhosts files 518 – 519
overview 515, 517
Windows NT RAS authentication
override accounts 521
overview 520
service account credentials 520
user credentials 521
Windows NT Server, configuration 515
X.400 address 160

E

Editing
Address Book details template controls 38
enrollment welcome message 52
Internet Mail Service addresses 121
Internet protocols rules 392
Lmhosts files 518
Microsoft Mail Connector address spaces 253
EHLO command 130
Eicon port adapter 164
E-mail
addresses
custom recipients 11
recipients 16
cc:Mail Connector
address generator 209, 220
addresses, modifying 231
attachments 227
bulletin boards 231
connections, testing 225, 226
public folders 231
directory synchronization
addresses, changing 358
addresses, creating 358
addresses, overview 357
addresses, removing 359
E-mail (*continued*)
disabling display names 96
domain
attachment format 93
delivering messages 102
Internet Mail Service 97
maximum message size 112
message content 97
IMAP4rev1 address 433
message encoding 497
POP3 address 413
prefixes 83
transmitting temporary keys 52
Embedded objects
cc:Mail Connector 227
defined 227
Microsoft Mail 3.x viewing and saving 277
Empty containers, removing, Address Book views 31
Enabling
anonymous connections 421
IMAP4rev1 418
LDAP 438
Microsoft Outlook Web Access
HTTP 506
Web browser access 506
NNTP
client access 480
newsfeeds 459
site 480
POP3 399, 403
RAS server configuration, TCP/IP 516
Encoding
cc:Mail Connector, post office 207
Internet Mail Service, e-mail domain 97
messages
IMAP4rev1 429
NNTP 495
POP3 409
Encryption
algorithms 63 – 65
data, described 43
IMAP4rev1 419
Internet Mail Service 122
Internet protocols, SSL 389
LDAP 438
Microsoft Outlook Web Access 503
NNTP
clients 498, 499
newsfeeds 464 – 466
SSL 485
POP3 400

Enrollment properties
bulk enrollment 53
certificates, compatible 54
overview 51
transmitting temporary keys 52
welcome message 52
Error messages
See also Troubleshooting
directory exchange requestor 350
ESMTP, Internet Mail Service 130 – 132
ETRN
Internet Mail Service 131
mail retrieval options 115
Eudora Light 413
Event Log
See also Logs
directory synchronization 366
IMAP4rev1 427
Microsoft Mail Connector 294
NNTP 493
POP3 407
Event Viewer *See* Windows NT Event Viewer
Exchange Client *See* Microsoft Exchange Client
Exchange Connector for Lotus cc:Mail *See* Connectors, cc:Mail
Exchange policy module 44
Exchange requestor, directory *See* Directory exchange requestor
Exchange Server *See* Microsoft Exchange Server
Expansion server, distribution lists 5
Export
containers 209, 325, 326, 341
version, cc:Mail Connector 206
Exporting
directory exchange requestor
address changes manually 352
world lists manually 352
directory synchronization, master list 369
recipients, Address Book views 33
Schedule+ Free/Busy Connector
distribution list 378
updates 378
Extensions, file, MIME types 393
Extracting access connection gateway 263

F

FAN fields 212
Fax gateway 308
Feeds
news *See* Newsfeeds
pull *See* Pull feeds
push *See* Push feeds
Files
.Asp 502
active, new
inbound pull feeds 472
inbound push feeds 474
NNTP 483
extensions, MIME types 393
Lmhosts
editing 518
lookup functionality 518
overview 518
verifying 519
working with 519
Macintosh
attachments 123
sharing 240, 254
Microsoft Exchange Connection, installation 257
Schedule+ Free/Busy Connector program 375
text, manually exporting world lists 352
Filters
address, directory exchange requestor 349
import container, cc:Mail Connector 214
Final substring searches 441
Flushing queued messages, outbound feeds 476
Folders, IMAP4rev1 432
Folders, public
anonymous connections 421
cc:Mail Connector
distribution lists 233
e-mail address generator 220
e-mail addresses 231
export containers 209
overview 230
propagating messages 231, 232
Microsoft Outlook Web Access, published 508 – 509
newsgroups
adding 459
character sets 497
control messages 452
creating folders 474
defined 447
deleting 453
hierarchies 477 – 478
hierarchy 451, 452
Internet News 450
managing 452
moderated 451
naming 451
new active file 472
NNTP 483

Folders, public (*continued*)
newsgroups (*continued*)
overview 450
properties 496
removing 459
replication 450
properties 3
Fonts, fixed-width 98
Foreign
address name (FAN) field 212
address types 322
language details templates, Address Book 40, 41
mail addresses, directory exchange requestor 349
Foreign systems
directory exchange requestor 355
Microsoft Mail Connector, gateways 308 – 311
remote directory requestor, configuration 343 – 355
X.400 Connector
configuration 197
override properties 183
overview 163
TCP/IP connection 179
testing 198
TP4 connection 182
X.25 connection 180
Formats
attachment 93
cc:Mail Connector e-mail address generator 220
certificates 54
message
Internet protocols 395
security 65
Forwarding, cc:Mail Connector
bulletin boards 230
history 207
public folders 230
FQDN
Internet Mail Service, routing address 107
TCP/IP, Internet Mail Service, installation 88
USENET host computer 462
Free times, defined 373
Fully qualified domain name *See* FQDN

G

Gateway Services for NetWare 223, 280
Gateways
directory exchange requestor
selecting 348
viewing recipient information 351
Gateways (*continued*)
Microsoft Exchange Connection
access connection 263 – 265
connection times 262
installation 257
options 261
Microsoft Mail Connector
list of 308
Microsoft Exchange Connection, Appletalk, defined 235
Microsoft Mail (PC), installation 309
overview 271, 308
postoffices 308 – 311
Microsoft Mail for Appletalk Networks Connection 265
Microsoft Mail, attachment format 93
GDI, X.400 Connector 197
General address space type 83 – 84
General properties
Address Book views 26
address spaces 80 – 84
advanced security 59
cc:Mail Connector 208
directory synchronization 356
dirsync server 332
Dynamic RAS Connector 147 – 148
IMAP4rev1 417
Internet Mail Service 112 – 113
Internet protocols 387
LDAP 436
Microsoft Mail (PC), dirsync requestor 322
Microsoft Mail Connector 249, 277 – 279
Microsoft Outlook Web Access 505 – 507
NNTP 480
NNTP newsfeeds 459
POP3 398
RAS MTA transport stack 143
remote dirsync requestor 336
Schedule+ Free/Busy Connector 379
Site Connector 135 – 136
site security 62
X.400 Connector 173 – 176
German, inbound message conversion 195
Global address list
directory exchange requestor
removing addresses 353
resynchronizing address information 354
Internet Mail Service, user name resolution 126
Microsoft Mail (PC)
changes 319
duplicates 325
Global domain identifier (GDI), X.400 Connector 197

Global updates, directory exchange requestor 346
Group By properties, Address Book views 26
Groups
  Internet protocols, permissions 389
  recipient *See* Address Book views; Distribution lists; Recipients
Guest account, Windows NT 491
GW extension 259

H

Headers, .Csv 33
HELO command 130
Help files
  Address Book details templates 37
  one-off address templates, Address Book 40
Hewlett Packard OpenMail 195
Hidden mailboxes
  dirsync server 322
  remote dirsync requestor 337
Hiding
  custom recipients, Address Book 14
  distribution lists, Address Book 8
Hierachies
  customizing Address Book view 32
  Internet News Service 448
  newsgroup 477
  newsgroup public folders 451, 452
History, forwarding, cc:Mail Connector 207
Hosts
  computers, NNTP
    See also USENET, hosts
    connecting to remote USENET site 461, 468
    connections 463
    control messages 452
    custom recipients 467
    inbound, passwords 467
    LAN connections 463
    mailboxes 467
    multiple inbound 462
    outbound, accounts 466
    outbound, passwords 466
    overview 461
    removing inbound connections 462
  file, updating 90
  Internet Mail Service
    accepting messages from all 103
    accepting messages from secure 103
    accepting messages from specific hosts 104
    delivering messages to single 102
Hosts (*continued*)
  Internet Mail Service (*continued*)
    names, installation 88
    names, reverse resolution 125
    retry interval 105
  USENET
    control messages 453
    current newsfeeds 453
    dedicated connections 463
    dial-up connections 463
HTML
  attachment format 93
  IMAP4rev1 messages 424
  NNTP messages 489
  POP3 messages 404
HTTP
  disabling 395
  Internet protocol 385
  Microsoft Outlook Web Access
    (Web) Site Settings name 506
    enabling 506
  restricting connections 389
  settings 386
Hypertext Transfer Protocol *See* HTTP

I

IA5 messages, inbound message conversion 195
IBM PROFS gateway 308
Idle time-outs
  IMAP4rev1 426
  LDAP 445
  NNTP 490
  POP3 406
IIS
  IMAP4rev1 419
  LDAP 438
  Microsoft Outlook Web Access 501, 503
  NNTP 485
  NNTP newsfeeds 465
  POP3 400
IMAP4rev1
  account names 432
  anonymous connections 421
  authentication 418
  client configuration 432 – 434
  diagnostics logging 427
  directory 417
  disabling 395, 418
  display name 417
  e-mail address 433

IMAP4rev1 (*continued*)
enabling 418
general properties 417
idle time-out 426
Internet Mail Service
configuration 430
connections, number of 100
routing 118
Internet message formats 423
Internet protocol 385
mailbox configuration 415, 427 – 429
Microsoft Internet Information Server (IIS) 419
overview 415
restricting connections 389
sample client configuration 434
server configuration 415 – 427
server name 433
site configuration 415 – 427
site defaults 417
SSL encryption 389, 419
Windows NT Challenge/Response 420
Import containers
cc:Mail Connector
alias name rules 215
directory synchronization 214
display name rules 215
filter configuration 214
moving within a site 230
overview 211
selecting 213
Microsoft Mail (PC), dirsync requestor 320, 324 – 325
remote dirsync requestor 339
Import version, cc:Mail Connector 206
Importing
Address Book details templates help files 37
Certificate Trust Lists 56
CRLs 56
directory exchange requestor address changes manually 351
directory synchronization master list, manually 369 – 370
manual directory synchronization, Resync.glb file 370
Microsoft Mail (Appletalk) world lists 352
recipients, Address Book views 33
Inbound connections
cc:Mail Connector, testing 226
host
custom recipients 467
mailboxes 467
passwords 467
Internet Mail Service, setting number of 100
Inbound messages
cc:Mail Connector
queues 221 – 222
size 209
tracking 207
character sets 94
Internet Mail Service
adding routing addresses 121
delivery restrictions 111
e-mail domain 97
matching domain names 118
maximum message size 112
MIME types 123
RAS connection time-out 116
routing destinations 120
routing methods 120
transfer modes 100
X.400 Connector, body parts 195
Inbound newsfeeds
Internet News Service, configuration 449, 455
multiple hosts 462
pull
adding newsgroups 471
included newsgroups 470
new active file 472
overview 470
removing newsgroups 471
push
included newsgroups 472
new active file 474
newsgroup public folders 474
newsgroups, accepting items 473
newsgroups, rejecting items 474
overview 472
removing connections 462
Inbox, Microsoft Exchange Server *See* Microsoft Exchange Server, Inbox
Incoming templates, directory synchronization
changing mappings 364
mappings configuration 363
overview 362
removing mappings 364
Indirect access to postoffices, Microsoft Mail Connector 280
Indirect connections, Microsoft Mail (PC) postoffices
manually creating information 307
overview 305
setup 305
testing 308
uploading routing information 305
Indirectly connected sites
costs 160
routing address 160

Information store, Internet News Service 448
Initial substring searches 441
Installation
  access connection gateways 264
  cc:Mail Connector 201
  dirsync server 331 – 334
  Dynamic RAS Connector 141, 145
  Foreign language details templates, Address Book 41
  Internet Mail Service
    adding to DNS 89
    overview 88
    requirements 87
    TCP/IP 88
    testing connection 90
    updating Hosts file 90
  KM Server 44
  Microsoft Certificate Server 44
  Microsoft Exchange Connection files 257
  Microsoft Exchange Connection gateway 257, 261
  Microsoft Mail (PC) gateway 309
  Microsoft Mail (PC) gateway access component 311
  Microsoft Mail Connector 374
  Microsoft Mail dirsync requestor 319 – 330
  Microsoft Mail for Appletalk Networks Connection Gateway 266
  Microsoft Outlook Web Access 501
  Microsoft Windows NT Server RAS software 141
  remote dirsync requestor 335 – 343
  Schedule+ Free/Busy Connector 374 – 375
  Schedule+ Free/Busy Connector Schedule+ Administrator program 375
  Site Connector 134
  X.400 Connector
    MTA transport stack 165
    requirements 163
    TCP/IP MTA transport stack 166
    TP4 MTA transport stack 168
    X.25 MTA transport stack 167
Integrated Services Digital Network (ISDN) networks RAS MTA transport stack 141
Interchange, Microsoft Mail Connector
  configuration 241 – 244
  defined 235, 271
  properties 275 – 277
Internet
  address space type 79, 80, 81
  e-mail address type 357
  IMAP4rev1 message format 423
  message encoding 497
  Microsoft Outlook Web Access 501
  NNTP message format 487, 495
  POP3 message format 402, 404
  secure connections 455
Internet Explorer *See* Microsoft Internet Explorer
Internet Mail Service
  accepting messages
    from all hosts 103
    from secure hosts 103
    from specific hosts 104
    from specific senders 111
  adding
    additional services 123
    domains to routing 118
    RAS connections 115
    routing addresses 121
  address spaces 109 – 110
  administrator's mailbox 92
  advanced configuration 125 – 130
  attachment format 93, 97
  automatic replies 96
  balancing load 109
  character sets 94, 404, 424
  connected sites
    properties 107 – 108
    routing address 107
  connections
    number of 100
    properties 99 – 106
  custom routing programs 122
  customizing 91
  defined 133
  delivering messages
    by e-mail domain 102
    to single host 102
  delivery restrictions 111
  diagnostics logging properties 113
  dial-up connections properties 114 – 117
  directory exchange requestor, address type 349
  disabling
    display names 96
    ETRN support 131
    S/MIME support 98
  DNS routing 101
  editing routing addresses 121
  e-mail domain 97
  encryption 122
  ESMTP 130 – 132
  fixed-width fonts 98
  general properties 112 – 113
  IMAP4rev1 configuration 430
  installation
    adding to DNS 89
    overview 88

Internet Mail Service (*continued*)
installation (*continued*)
requirements 87
TCP/IP 88
testing connection 90
updating Hosts file 90
Internet Mail properties 92 – 98
logon information 117
loopback detection 127
Macintosh file attachments 123
mail retrieval options 115
maximum message size 112
maximum messages sent 100
message time-out values 105
message tracking 129
Microsoft Mail Connector, foreign system access 308
MIME
attachment format 93
e-mail domain 97
types 123
NDRs 92
notifications 106
out-of-office replies 96
overview 87
permissions 113
POP3 configuration 410
queues properties 113
RAS connection time-out 116
rejecting messages from specific senders 111
removing 124
removing routing addresses 121
retry interval 105
reverse resolution 125
rich text formatting 95, 97
routing
addresses for address spaces 110
costs 109
destinations 120
methods 120
properties 118 – 122
scheduling connections 117
security properties 122
text quoting 128
transfer modes 100
user name resolution 126
Uuencode
attachment format 93
e-mail domain 97
viewing RAS connections 114
VRFY 127
Windows NT Server, administering 87
Internet Message Access Protocol Version 4 rev1 *See* IMAP4rev1
Internet News public folder 450
Internet News Service
See also NNTP
configuration scenarios 455
control messages 452
defined 447
inbound newsfeeds, configuration 449
Newsfeed Configuration Wizard 455
newsfeeds
current, catching up 453
outbound, configuration 449
overview 448
newsgroup public folders 450 – 451, 452
overview 447
pull feeds, defined 448
push feeds, defined 448
queued messages, flushing 454
USENET newsfeeds, subscribing to 454
Internet News Service/Network News Transfer Protocol *See* NNTP
Internet protocols
See also specific protocols
connections
accepting 390
adding rules 391
custom recipients 395
disabling 395
editing rules 392
mailbox configuration 395
MIME types 393 – 394
moving rules 392
overview 389
rejecting 390
removing rules 391
defined 385
list of supported 385
overview 385
servers
defaults 388
directory names 388
display names 388
general properties 387
permissions 389
properties, overview 385
sites
defaults 388
directory names 388
display names 388

Internet protocols (*continued*)
sites (*continued*)
general properties 387
permissions 389
properties, overview 385
TCP/IP, Internet Mail Service, installation 88
IP addresses
Internet Mail Service 89, 90
Internet protocols
access by 389
adding rules 391
NIC 517
RAS server 516
USENET host computer 462
ISDN networks, RAS MTA transport stack 141
Italic
Internet Mail Service 95
POP3 403
X.400 Connector 176

K

Key Management server *See* KM server
Keys
enabling additional sites 70
recovering security 69
security, bulk enrollment 53
temporary
mailbox security 66
transmitting 52
KM Server
administrators properties
adding administrators 48
changing passwords 48
overview 47
removing administrators 48
advanced security configuration overview 45
backing up data 72
CA permissions 60
Certificate Trust Lists
importing 56
overview 55
removing 57
revoking 57
viewing 58
configuration 44
described 43
enabling additional sites 70
enrollment properties
bulk enrollment 53
certificates, compatible 54
KM Server (*continued*)
enrollment properties (*continued*)
overview 51
transmitting temporary keys 52
welcome message 52
general properties 59
installation 44
mailbox security
enabling 66
overview 65
recovering keys 69
revoking 68
temporary keys 66
viewing 69
moving between sites 75
moving users between KM servers 73
passwords properties
multiple passwords policy 50
overview 49
restoring data 72
site security
choosing sites 62
display name 62
encryption algorithms 63 – 65
general properties 62
overview 60
permissions 63
starting 45
user security in remote sites 72
viewing security log 73

L

Languages
cc:Mail Connector post office 207
Microsoft Mail Connector, primary 276
multilingual message support 497
LANs
Dynamic RAS Connector 515
Internet News Service connections 463
Microsoft Exchange Connection setup 254
Microsoft Mail Connector
confirming connection changes 281
connection setup 279
Connector (PC) MTAs 282
creating connection 280
indirect access to postoffices 280
interchange properties 275 – 277
Microsoft Mail (PC) client 293
Microsoft Mail (PC) connection 279
Microsoft Mail (PC), configuration 290

LANs (*continued*)
Microsoft Mail Connector (*continued*)
Microsoft Mail (PC), modifying properties 291
MTA configuration 282 – 289
MTA options 286
MTA setup 284
overview 271
postoffices, setting options 289
postoffices, specifying 288
quick start 273
removing connections 282
removing MTA 288
setup 272 – 273
testing connection 293
Microsoft Mail Dispatch 319
X.400 Connector MTA transport stack 164
LDAP
anonymous connections 440
authentication 438
directory 437
directory access, anonymous user 440
directory searches 441
disabling 438
display name 437
enabling 438
general properties 436
idle time-out 445
Internet protocol 385
Microsoft Internet Information Server (IIS) 438
overview 435
permissions 438
restricting connections 389
server configuration 435 – 440
site configuration 435 – 440
site defaults 437
SSL encryption 389, 438
Life span, certificate 54
Lightweight Directory Access Protocol *See* LDAP
Links
cc:Mail Connector 227
defined 227
X.400 Connector 196
Lists, distribution
Address Book
display name 5
hiding from 8, 14
advanced properties 6 – 8
cc:Mail Connector
administrator's mailbox 205
bulletin boards 233
e-mail address generator 220
Lists, distribution (*continued*)
cc:Mail Connector (*continued*)
export containers 209
public folders 233
recipients, many 212
configuration 5
creating new 3
defined 3
described 16
directory synchronization trust levels 8
display names 7
expansion server, specifying 5
General property page 4
members
adding 5, 17
deleting 17
modifying 4
removing 6, 17
messages
accepting and rejecting 18
delivery restrictions 17
size limit 7
name, modifying 4
non-delivery reports 6
out-of-office messages 8
owners
adding 6
deleting 6
modifying 4
reports 8
reports, message originator 8
Schedule+ Free/Busy Connector
assigning 377
exporting 378
setting options 8
X.400 Connector, delivery restrictions 193
Lmhosts files
editing 518
lookup functionality 518
overview 518
verifying 519
working with 519
Load balancing, Internet Mail Service 109
Load, server, Address Book views 34
Local address lists, dirsync server 334
Local Area Networks *See* LANs
Local sites *See* Dynamic RAS Connector; Internet Mail Service; Site Connector; X.400 Connector
Locking, desktop, directory exchange requestor 350
Logon information, Internet Mail Service 117

Logs
See also Event Log
anonymous access 491
cc:Mail Connector 207, 222
directory exchange requestor 354
directory synchronization 366
IMAP4rev1 427
Internet Mail Service 113, 129
Microsoft Mail Connector 253, 294
NNTP 493
POP3 407
Schedule+ Free/Busy Connector 379
viewing security 73
X.400 Connector 199
Lookup functionality, Lmhosts 518
Loopback detection, Internet Mail Service 127
Loops, transfer, message 197
Lotus cc:Mail *See* cc:Mail

M

Macgate.ini file 259
Macintosh
accessible volume 238
file attachments 123
Microsoft Exchange Connection
requirements 237
setup 254 – 265
Microsoft Mail Connector (Appletalk)
MTA setup 243
requirements 236
NNTP messages 489
POP3 messages 404
Macproxy.dll file 266
Mail
See also Messages
Internet Mail Service retrieval options 115
queued, notifications 106
Mail (Appletalk) *See* Microsoft Mail (Appletalk)
Mail (PC) *See* Microsoft Mail (PC)
Mail Connector *See* Microsoft Mail Connector
Mailbox agents, creating 3
Mailboxes
Address Book views 23
cc:Mail Connector
administrator 205
e-mail address generator 220
export containers 209
directory synchronization, delivery restrictions 359
dirsync server 332
distribution lists, adding 17
Mailboxes (*continued*)
IMAP4rev1 configuration 415, 427 – 429
Internet Mail Service, administrator's 92
Internet protocols 395
messages, delivery restrictions 17
Microsoft Exchange Server, anonymous connections 421
Microsoft Mail (PC), dirsync server 322
Microsoft Mail Connector, administrator's 242, 275
Microsoft Outlook Web Access, HTTP, enabling 506
NNTP
client configuration 498
configuration 493 – 495
newsfeeds 459, 467
POP3 configuration 397, 407 – 409
properties 3
remote dirsync requestor 337
Schedule+ Free/Busy Connector
administrator 375, 377
AdminSch accounts 375
security
enabling 66
overview 65
recovering keys 69
revoking 68
temporary keys 66
viewing 69
Mailing lists, cc:Mail Connector 211
Managing newsgroup public folders 452
Manual
directory exchange requestor
exporting address changes 352
exporting world lists 352
importing address changes 351
directory synchronization
importing master list 369 – 370
remote directory synchronization requestor 370
restarting Microsoft Exchange Directory Synchronization Service 370
Resync.glb file 369, 370
starting 368
Windows NT registry 369
Microsoft Mail (PC) postoffices indirect connections routing information 307
MAPI
IMAP4rev1 messages 424
Internet Mail Service 95
multilingual message support 498
NNTP 498
POP3 messages 404
X.400 Connector 176

Mappings
incoming templates
changing 364
configuration 363
removing 364
outgoing templates
changing 365
configuration 365
removing 366
Masks, Internet protocols 391
Mass mailing 3
Master address lists, dirsync server 334
Master list
directory synchronization, importing manually 369 – 370
manual directory synchronization 370
MCI Mail Gateway 308
Meetings, online 13
Members, distribution lists
adding 5, 16, 17
deleting 17
modifying 4
removing 6, 17
Memory, Address Book views, large 34
Message transfer agent *See* MTA
Messages
See also Mail
accepting
delivery restrictions 223
directory synchronization 361
distribution lists 18
Dynamic RAS Connector 156
automatic replies 96
cc:Mail Connector
administrator's mailbox 205
attachments 227
delivery restrictions 223
forwarding 230
forwarding history 207
propagating 231, 232
queues 221 – 222
size 209
tracking 207
confirmation, Microsoft Mail Connector connection changes 281
control
deleting 453
NNTP 452, 484
delivery
Microsoft Mail Connector 242, 275
restrictions 17, 155
Messages (*continued*)
directory exchange requestor
directory update 346
dirsync 346
error 350
update 345
directory synchronization
delivery restrictions 359 – 362
requestor schedule 330, 334
system, delivery restrictions 359
system, e-mail addresses for, changing 358
system, e-mail addresses for, creating 358
system, e-mail addresses for, removing 359
dirsync server 322, 332
disabling display names 96
distribution lists 8
encrypting *See* Encryption
fixed-width fonts 98
format, security 65
IMAP4rev1
formats 429
Internet, format 423
Internet Mail Service
accepting from all hosts 103
accepting from secure hosts 103
accepting from specific hosts 104
adding routing addresses 121
archival directory 113
attachment format 93
character sets 94
delivering by e-mail domain 102
delivering to single host 102
delivery restrictions 111
disabling S/MIME support 98
disabling text quoting 128
e-mail domain 97
mail retrieval options 115
matching domain names 118
maximum sent 100
maximum size 112
MIME types 123
queued, notifications 106
queues properties 113
RAS connection time-out 116
retry interval 105
reverse resolution 125
rich text formatting 95
routing destinations 120
routing methods 120
routing with DNS 101

Messages (*continued*)
Internet Mail Service (*continued*)
time-out values 105
tracking 129
transfer modes 100
Internet News Service, redundant replication 448
Internet protocols formats 395
mass mailing 3
Microsoft Mail (Appletalk) queue 248
Microsoft Mail Connector
mixed environment 308
overview 271 – 272
routing 252
size limit 250
testing connections 268
multilingual support 497
newsfeeds, marking as delivered 453
newsgroup public folders
MIME character sets 497
non-MIME character sets 497
NNTP
formats 495
Internet, format 487
newsfeeds, size 460
USENET site name 483
outbound, costs 80
out-of-office replies 96
paths *See* address spaces
POP3
formats 409
Internet, format 402, 404
rich text 402 – 404
queued, flushing 454, 476
recipients
alternate 20
sending on behalf 21
rejecting
cc:Mail 223
directory synchronization 362
distribution lists 18
Dynamic RAS Connector 156
remote dirsync requestor, mailbox 337
routing *See* Address spaces
S/MIME 489
Schedule+, unresolved 381
sending to groups *See* Distribution lists
size
custom recipients 13
distribution lists 7
Dynamic RAS Connector 148
e-mail domain 97
Microsoft Mail Connector 279
Messages (*continued*)
tracking, Microsoft Mail Connector 243, 277
transfer
between sites *See* Dynamic RAS Connector; Internet Mail Connector; Site Connector; X.400 Connector
size limit 7
X.400 Connector
body parts 195
delivery restrictions 192
link options 196
messaging route, defined 163
MTA conformance 195
override properties 183
rich text 176
size 196
transfer loops 197
transfer timeouts, overriding 187
word-wrap 175
Messaging Application Programming Interface *See* MAPI
Messaging bridgehead servers
defined 163
X.400 Connector 190
MHS gateway 308
Microsoft Certificate Server 44, 54, 59
Microsoft Exchange Client
certificate formats 54
encryption algorithms 64
Microsoft Exchange Connection
directory exchange requestor
address filters 349
configuration 346
foreign systems 355
making startup item 351
manually exporting address changes 352
manually exporting world lists 352
manually importing address changes 351
overview 345
removing addresses 353
removing recipients from world lists 354
resynchronizing address information 354
selecting gateway 348
starting 350
viewing gateway recipient information 351
Microsoft Mail Connector
Appletalk, access connection gateway 263 – 265
Appletalk, configuration 259 – 262
Appletalk, connecting to postoffice 255
Appletalk, defined 235
Appletalk, gateway connection times 262
Appletalk, gateway options 261
Appletalk, installing files 257

Microsoft Exchange Connection (*continued*)
Microsoft Mail Connector (*continued*)
Appletalk, installing gateway 257
Appletalk, postoffice location 259
Appletalk, requirements 237
Appletalk, setup 254 – 265
Appletalk, testing connections 268
Microsoft Mail for Appletalk Networks Connection Gateway 265
Microsoft Exchange Connector for Lotus cc:Mail *See* Connectors, cc:Mail
Microsoft Exchange Directory Synchronization Service 366, 370
Microsoft Exchange Server
directory synchronization
incoming templates 362 – 364
outgoing templates 364 – 366
documentation, described xxv – xxvii
Dynamic RAS Connector, configuration 515
Inbox, POP3, overview 397
LDAP directory access 435
mailboxes, anonymous connections 421
Microsoft Mail (Appletalk), removing addresses 354
Microsoft Exchange Server dirsync requestor *See* Dirsync requestor
Microsoft Exchange Server dirsync server *See* Dirsync server
Microsoft Internet Explorer, Microsoft Outlook Web Access 502
Microsoft Internet Information Server (IIS) *See* IIS
Microsoft Internet Locator Server 13
Microsoft Mail
address space type 79, 80, 82
Appletalk *See* Microsoft Mail (Appletalk)
directory server
address updates 327
configuration 330
export containers 325
import containers 324
schedule properties 329
settings properties 327
directory synchronization
incoming templates 362 – 364
outgoing templates 364 – 366
overview 317
recipient information templates 355
dirsync requestor, defined 317
dirsync server 317
Dispatch 319
PC *See* Microsoft Mail (PC)
SMTP gateway 308
X.400 gateway 308
Microsoft Mail (Appletalk)
directory exchange requestor
address filters 349
configuration 346
foreign systems 355
making startup item 351
manually exporting address changes 352
manually exporting world lists 352
manually importing address changes 351
overview 345
removing addresses 353
removing recipients from world lists 354
resynchronizing address information 354
selecting gateway 348
setup 344
starting 350
viewing gateway recipient information 351
message size limit 279
Microsoft Mail Connector
access connection gateway 263 – 265
address space properties 250 – 253
AppleShare 254
connections properties 247
diagnostics logging 294
editing address spaces 253
installing Microsoft Exchange Connection gateway 257
Macintosh-accessible volume 238
message queue 248
message size limit 250
Microsoft Exchange Connection configuration 259 – 262
Microsoft Exchange Connection gateway connection times 262
Microsoft Exchange Connection gateway options 261
overview 235
requirements 236
routing 252
setup 237
testing connections 268
volume permissions 240
Microsoft Mail for Appletalk Networks Connection Gateway 265
remote directory requestor
configuration 343 – 355
Microsoft Mail (PC)
directory server 319
dirsync requestor
address updates 327, 329
advanced directory synchronization functions 328

Microsoft Mail (PC) (*continued*)
dirsync requestor (*continued*)
creating 320
export container properties 325 – 326
foreign address types 322
general properties 322
import container properties 324 – 325
import container, creating 320
installation 319 – 330
requirements 320
schedule properties 329
settings properties 327
dirsync server mailbox 322
e-mail address type 357
gateway
access component 311
installation 309
message size limit 279
Microsoft Mail Connector
LANs connection 279 – 294
message size limit 250
overview 271 – 272
postoffice configuration 304
postoffice, indirect connections 305 – 308
postoffice, testing connection 304
Microsoft Mail Connector (Appletalk) MTA setup 243
postoffices
address space 312 – 315
directory synchronization requestor 343
manually importing address lists 352
remote dirsync requestor 337
proxy format 349
remote directory requestor, configuration 343 – 355
Schedule+ Free/Busy Connector
installation 374
overview 373
Microsoft Mail (PC) 3.x
remote directory requestor
configuration 343 – 355
setup 343
Microsoft Mail (PC) External program 374
Microsoft Mail 3.x
attachment format 93
client compatibility 277
directory exchange requestor, directory synchronization 355
languages 276
Microsoft Mail Connector
access connection gateway 263 – 265
address regeneration 246
Microsoft Mail Connector (*continued*)
address space
configuration 312 – 315
overview 312
properties 250 – 253
administrator's mailbox 242, 275
asynchronous connection
Microsoft Mail (PC) postoffice 295
Microsoft Mail (PC) postoffices 304
Microsoft Mail (PC) postoffices indirect connections 307
MTA configuration 299 – 303
MTA setup 301
setting options 298
setup 295 – 297
computer name 278
configuration
administering 274
interchange properties 275 – 277
connections properties 247
delivery messages 242, 275
diagnostics logging 253
gateway
Microsoft Mail (PC), installation 309
overview 308
postoffices 308 – 311
general properties 249, 277 – 279
installing Microsoft Exchange Connection files 257
installing Microsoft Exchange Connection gateway 257
Interchange
configuration 241 – 244
defined 235, 271
Internet Mail Service 308
LANs
confirming connection changes 281
connection setup 279
creating connection 280
indirect access to postoffices 280
Microsoft Mail (PC) client 293
Microsoft Mail (PC) connection 279
Microsoft Mail (PC), configuration 290
Microsoft Mail (PC), modifying properties 291
MTA configuration 282 – 289
MTA options 286
MTA setup 284
postoffices, setting options 289
postoffices, specifying 288
removing connections 282
removing MTA 288
testing connection 293
list of gateways 308

Microsoft Mail Connector (*continued*)
local postoffice properties 244
Macintosh-accessible volume 238
message size limit 250, 279
message tracking 243, 277
Microsoft Exchange Connection
Appletalk, defined 235
Appletalk, requirements 237
Appletalk, setup 254 – 265
configuration 259 – 262
gateway connection times 262
gateway options 261
Microsoft Mail (Appletalk)
access connection gateway 263 – 265
address space properties 250 – 253
AppleShare 254
connections properties 247
directory exchange requestor 344
editing address spaces 253
Macintosh-accessible volume 238
message queue 248
message size limit 250
Microsoft Exchange Connection configuration 259 – 262
overview 235
requirements 236
routing 252
setup 237
testing connections 268
volume permissions 240
Microsoft Mail (PC)
message size limit 250
postoffice configuration 304
postoffices indirect connections 305 – 308
Microsoft Mail 3.x
client compatibility 277
languages 276
MTA
Appletalk, defined 235
Appletalk, diagnostics logging 254
Appletalk, message queue 248
Appletalk, postoffice names 246
Appletalk, setting up 243
defined 271
overview 271 – 272
passwords 245
postoffices
defined 235, 271
directory server configuration 330
installing Microsoft Exchange Connection 255
Macintosh-accessible volume 238
Microsoft Exchange Connection, location 259

Microsoft Mail Connector (*continued*)
primary language 276
quick start 238, 273
routing 252
Schedule+ Free/Busy Connector 374
setup 272 – 273
testing connections 268
X.25 connection
Microsoft Mail (PC) postoffice 295
Microsoft Mail (PC) postoffices 304
Microsoft Mail (PC) postoffices indirect connections 307
modifying MTA 303
MTA configuration 299 – 303
MTA setup 302
setting options 298
setup 295 – 297
X.400 Connector 308
Microsoft Mail External program 272
Microsoft Mail for Appletalk Networks Connection Gateway 265
Microsoft Mail Gateway attachment format 93
Microsoft Mail Multitasking MTA program 272
Microsoft NetMeeting 13
Microsoft Outlook
certificate formats 54
distribution lists
editing 6
modifying 4
encryption algorithms 64
moderated newsgroups 451
NNTP 447
Schedule+ Free/Busy Connector 373
Microsoft Outlook Calendar 373
Microsoft Outlook Web Access
Address Book entries 510
anonymous access 507
anonymous users 504
authentication 503 – 504
configuration 504 – 511
directory name 506
display name 506
enabling Web browser access 506
general properties 505 – 507
HTTP
(Web) Site Settings name 506
enabling 506
installation 501
Internet protocol 385
overview 501, 502
permissions 507

Microsoft Outlook Web Access (*continued*)
published public folders
overview 508
permissions 509
shortcuts 509
security levels 503
setup requirements 504
validated users 503
Windows NT Challenge/Response 503
Microsoft Windows NT
Address Book views permissions 28
Address Book views restrictions 28
alias name
IMAP4rev1 432
POP3 412
anonymous connections 440, 491
Backup utility 72
Challenge/Response
IMAP4rev1 420
Microsoft Outlook Web Access 503
NNTP 485
POP3 401
Connector (PC) MTAs 282
directory synchronization, manual 368
domain
IMAP4rev1 432
POP3 412
Event Log
cc:Mail Connector 222
directory synchronization 366
IMAP4rev1 427
Microsoft Mail Connector 253, 294
NNTP 493
passwords 421
POP3 407
Event Viewer 73
Guest account 491
Internet Mail Service
Event Log 113
permissions 113
security 122
LAN Manager (NTLM) security 503
Macintosh-accessible volume 238
Microsoft Mail Connector (Appletalk)
NTFS partition 236
requirements 236
volume permissions 240
Microsoft Mail Connector (Appletalk) MTA
defined 235
setup 243
Microsoft Mail Connector Interchange 235
Microsoft Windows NT (*continued*)
Microsoft Outlook Web Access
anonymous users 504
overview 502
validated users 503
NNTP
authentication 493
client configuration 498
permissions
Dynamic RAS Connector 161
RAS MTA transport stack 144
X.400 Connector 197
RAS authentication
override accounts 521
overview 520
service account credentials 520
user credentials 521
registry, exporting directory synchronization master list 369
TCP/IP, Internet Mail Service, installation 88
user account
IMAP4rev1 432
POP3 412
Microsoft Windows NT Server
Dynamic RAS Connector, configuration 515
Event Log, Schedule+ Free/Busy Connector 379
Gateway Services for NetWare 223
Internet Mail Service, administering 87
Microsoft Mail Connector Interchange, defined 271
Microsoft Mail Connector MTA, defined 271
Microsoft Mail Connector, administering 274
RAS functionality 141
RAS software
installation 141
phone book entry 148
trust relationships, Site Connector 140
Microsoft Windows NT Workstation, Microsoft Mail Connector, administering 274
MIME
encryption algorithms 64
IMAP4rev1 messages 424
Internet Mail Service
attachment format 93
character sets 94
e-mail domain 97
Macintosh file attachments 123
messages, converting to 98
rich text formatting 95
types 123
Internet protocols, types 393 – 394
newsgroup public folders, message character sets 497
NNTP messages 489
POP3 messages 404

Modems, RAS server
address pool 516
configuration 516
Moderated newsgroups 451
Moving
Address Book views, recipient objects between containers 32
cc:Mail Connector
import container, within a site 230
to another site 228
to new computer 228
within a site 229
Internet protocols, rules 392
KM server between sites 75
MIME types 394
users between KM servers 73
MS Mail *See* Microsoft Mail
MS Mail (Appletalk) *See* Microsoft Mail (Appletalk)
MS Mail (PC) *See* Microsoft Mail (PC)
MSA
address type 250, 266, 337
format update message 345
MS-DOS Templates property page 37
MSExchangeATMTA 254, 294
MSExchangeMSMI 254, 294
MSExchangePCMTA 254, 294
MSMAIL address type 352
MTA
Dynamic RAS Connector, override properties 152 – 155
Microsoft Mail (PC) External program, Schedule+ Free/Busy Connector 374
Microsoft Mail Connector
Appletalk, defined 235
Appletalk, diagnostics logging 254
Appletalk, message queue 248
Appletalk, postoffice names 246
Appletalk, setting up 243
configuration, asynchronous 299 – 303
configuration, X.25 299 – 303
defined 271
diagnostics logging 294
LAN configuration 282 – 289
Microsoft Mail (PC) client 293
Microsoft Mail (PC), configuration 290
Microsoft Mail (PC), modifying properties 291
modifying, X.25 303
options 286
postoffices, setting options 289
postoffices, specifying 288
removing 288
setup 284
setup, X.25 302
testing connection 293
MTA (*continued*)
Microsoft Mail Multitasking 272
RAS authentication 520
X.400 Connector
conformance 195
remote name 174
remote password 174
MTA transport stack
Dynamic RAS Connector, specifying 147
X.400 Connector
Connectors property page 169
deleting 200
Eicon port adapter 164
installation 165
installing TCP/IP 166
installing TP4 168
installing X.25 167
local name, overriding 184
local password, overriding 184
overview 164
permissions 169
selecting remote 175
stack properties 178 – 182
TCP/IP 164
TP0/X.25 164
TP4/CLNP 164
MTA transport stack, RAS
connectors, defined 144
general properties 143
installation 141
MTA callback telephone number 143
name 143
permissions 144
RAS callback telephone number 152
MTS-IN queue, cc:Mail Connector 221
MTS-OUT queue, cc:Mail Connector 221
Multicharacter wildcards 80, 81, 82
Multilingual message support 497
Multipart/signed messages, Internet Mail Service 98
Multiple
Internet Mail Services 123
newsfeeds
inbound 462
Internet News Service 448
passwords policies 49 – 50
Multipurpose Internet Mail Extensions *See* MIME
Multitasking MTA, Microsoft Mail 272
MX (mail exchanger) records
defined 89
routing costs 109

N

Names
account
IMAP4rev1 432
POP3 412
alias
distribution lists 5
IMAP4rev1 432
NNTP client configuration 498
POP3 412
Schedule+ Free/Busy Connector 380
cc:Mail Connector
alias, rules 215
bulletin board, imported 211
display, rules 215
e-mail address generator 209
user, imported 211
computer, Microsoft Mail Connector 278
custom attribute fields, recipient 22
custom recipients 10
directory
Address Book views 26
CAs 59
Dynamic RAS Connector 147
IMAP4rev1 417
Internet protocols 388
LDAP 437
Microsoft Outlook Web Access 506
NNTP 480
NNTP newsfeeds 459
POP3 399
Site Connector 136
Site Encryption Configuration object 62
display
Address Book details templates 36
Address Book views 26, 33
CAs 59
dirsync requestor 322
dirsync server 332
distribution lists 5, 7
Dynamic RAS Connector 147
IMAP4rev1 417
Internet Mail Service, disabling 96
Internet protocols 388
KM Server 62
LDAP 437
Microsoft Outlook Web Access 506
NNTP 480
NNTP newsfeeds 459
POP3 399
remote dirsync requestor 336
Names (*continued*)
display (*continued*)
Schedule+ Free/Busy Connector 380
Site Connector 136
Site Encryption Configuration object 62
distribution lists 4
domain
Internet Mail Service, installation 88
Internet Mail Service, matching 118
updating Hosts file 90
Domain Name System *See* DNS
Dynamic RAS Connector
connector 147
remote server 147
hosts
Internet Mail Service reverse resolution 125
Internet Mail Service, installation 88
IMAP4rev1 access 415
Internet Mail Service
distinguished, routing address 107
user, resolution 126
Microsoft Certificate Server 59
Microsoft Mail Connector
network 244
postoffice 244
newsgroup public folders 451
postoffice, Microsoft Mail Connector 291
RAS MTA transport stack 143
remote USENET site 461
resolution, Internet Mail Service 89
server
IMAP4rev1 433
POP3 413
SMTP 413, 434
Site Connector 136
USENET site 483
X.400 Connector
connector 174
directory 174
display 174
local MTA, overriding 184
Nbtstat command 519
NDRs
distribution lists 6
IMAP4rev1 messages 431
Internet Mail Service 92, 105, 112
POP3 messages 411
Netscape Navigator 502
Netware server
cc:Mail Connector 206, 223
connection requirements 280
Gateway Service 280

Network Interface Card IP address 517
Network traffic, Internet News Service 448
NEWGROUP control message 453
Newsfeed Configuration Wizard
  Internet News Service 455
  newsfeeds, NNTP 456
Newsfeeds
  See also Newsgroups
  current, catching up 453
  defined 447
  Internet News Service
    inbound newsfeeds, configuration 449
    outbound newsfeeds, configuration 449
    overview 447, 448
  messages, marking as delivered 453
  NNTP
    administrator mailbox 459
    authentication 485
    configuration 456 – 469
    connections 463
    control messages 484
    custom recipients 467
    dial-up connections 464
    directory name 459
    display name 459
    enabling 459
    general properties 459
    host computers 461 – 462
    inbound host connection passwords 467
    inbound pull feeds 470 – 472
    inbound push feeds 472 – 474
    LAN connections 463
    mailboxes 467
    message size 460
    new active file 483
    outbound feeds 475 – 477
    outbound host connection accounts 466
    outbound host connection passwords 466
    permissions 481
    scheduling connections 468
    security 464 – 467
    SSL encryption 464 – 466
    USENET site name 483
  USENET, subscribing to 454
Newsgroups
  See also Newsfeeds
  current newsfeeds, catching up 453
  defined 447
  hierarchies 477
Newsgroups (*continued*)
  inbound pull feeds
    adding 471
    included 470
    new active file 472
  inbound push feeds
    accepting items 473
    included 472
    new active file 474
    public folders 474
    rejecting items 474
  Internet News Service, overview 447
  outbound feeds
    adding 475
    flushing queued messages 476
    removing 476
  public folders
    adding 459
    character sets 497
    control messages 452
    creating 474
    defined 447
    deleting 453
    hierarchies 477 – 478
    hierarchy 451, 452
    Internet News 450
    managing 452
    moderated 451
    naming 451
    new active file 472
    NNTP 483
    overview 450
    properties 496
    removing 459
    replication 450
Newsreaders
  Internet News Service 448
  message encoding 497
NIC address 517
NNTP
  See also Internet News Service
  anonymous connections 491
  client access 480
  client configuration 498 – 500
  configuration 479
  control messages 452
  custom recipients configuration 493 – 495
  diagnostics logging 493
  directory name 480
  disabling 395

NNTP (*continued*)
display name 480
general properties 480
idle time-out 490
Internet message formats 487
Internet News Service
Newsfeed Configuration Wizard 455
overview 447
Internet protocol 385
mailboxes configuration 493 – 495
message encoding 495
newsfeeds
administrator mailbox 459
authentication 485
configuration 456 – 469
connections 463
control messages 484
custom recipients 467
dial-up connections 464
directory name 459
display name 459
enabling 459
general properties 459
host computers 461 – 462
inbound host connection passwords 467
inbound pull feeds 470 – 472
inbound push feeds 472 – 474
LAN connections 463
mailboxes 467
message size 460
new active file 483
Newsfeed Configuration Wizard 456
outbound feeds 475 – 477
outbound host connection accounts 466
outbound host connection passwords 466
overview 448
permissions 481
scheduling connections 468
security 464 – 467
SSL encryption 464 – 466
USENET site name 483
newsgroups
public folders 450 – 451, 452, 496
overview 447
pull feeds
catching up current newsfeeds 453
defined 448
push feeds
catching up current newsfeeds 453
defined 448
queued messages, flushing 454
restricting connections 389
NNTP (*continued*)
S/MIME messages 489
servers, properties 481
sites
defaults 481
enabling 480
properties 481
SSL encryption 389
USENET newsfeeds, subscribing to 454
Windows NT Challenge/Response 485
Non-ANSI characters
distribution list names 7
Non-delivery reports *See* NDRs
Non-MIME, newsgroup public folders, message character sets 497
Non-urgent messages 105, 106, 187
Non-validated users 504
Normal messages 105, 106, 187
Norwegian, inbound message conversion 195
Notifications
administrator, NDRs 92
Internet Mail Service 106
NTFS, Microsoft Mail Connector (Appletalk) 236
NTLM security 503

O

Objects
directory synchronization *See* Directory synchronization
dirsync requestor *See* Dirsync requestor
dirsync server *See* Dirsync server
embedded
cc:Mail Connector 227
defined 227
Microsoft Mail 3.x viewing and saving 277
IMAP4rev1 *See* IMAP4rev1
LDAP *See* LDAP
NNTP *See* NNTP
remote dirsync requestor *See* Remote dirsync requestor
OfficeVision gateway 308
Offline Address Books
downloading 29
views, restricting 28
OLE
Internet Mail Service 95
Microsoft Mail 3.x versions 277
One-off address templates, Address Book
described 39
help files 40
viewing 39
Online meetings 13
Organization information, custom recipients 14

Organizations, restrictions, address spaces 84
OSI, X.400 Connector MTA transport stack 164
Outbound connections
  cc:Mail Connector, testing 225
  hosts
    accounts 466
    passwords 466
  Internet Mail Service
    security 122
    setting number of 100
  X.400 Connector, schedule 178
Outbound feeds
  adding newsgroups 475
  flushing queued messages 476
  overview 475
  removing newsgroups 476
Outbound messages
  attachment format 93
  cc:Mail Connector
    queues 221 – 222
    size 209
    tracking 207
  character sets 94
  costs 80
  disabling display names 96
  Internet Mail Service
    adding routing addresses 121
    delivering by e-mail domain 102
    delivering to single host 102
    delivery restrictions 111
    disabling text quoting 128
    e-mail domain 97
    maximum message size 112
    queued, notifications 106
    RAS connection time-out 116
    routing with DNS 101
    transfer modes 100
  rich text formatting 95
  X.400 Connector
    body parts 195
    link options 196
    MTA conformance 195
    remote global domain identifier (GDI) 197
    rich text 176
Outbound newsfeeds, Internet News Service
  configuration 449, 455
Outgoing templates, directory synchronization
  changing mappings 365
  mappings configuration 365
  overview 364
  removing mappings 366
Outlook *See* Microsoft Outlook
Outlook Express, IMAP4rev1 420, 432
Outlook Web Access *See* Microsoft Outlook Web Access
Out-of-office replies 96
Override accounts, RAS authentication 521
Override properties
  Dynamic RAS Connector
    association parameters 154
    connection retry values 153
    MTA 152 – 155
    RAS 150 – 152
    RTS values 153
    transfer time-outs 154
  Site Connector 140
  X.400 Connector 183 – 187
Overriding user accounts 140
Owners
  distribution lists
    adding 6
    deleting 6
    modifying 4
    reports 8

P

Parent folders, newsgroup 451, 452
Partitions, Microsoft Mail Connector (Appletalk) 236
Passwords
  advanced security
    changing administrator 48
    multiple passwords policy 50
    overview 49
  anonymous connections 421
  IMAP4rev1 432
  inbound host connections 467
  Internet Mail Service
    logon information 117
    security 122
  Microsoft Mail Connector 245
  NNTP client configuration 499
  outbound host connections 466
  POP3 412
  remote dirsync requestor 336
  X.400 Connector, local MTA, overriding 184
Paths *See* address spaces
Paths, network, Uniform naming convention (UNC) 280
Percent symbol (%) 80, 81, 82, 83
Performance, Internet Mail Service, advanced
  configuration 125 – 130
Permissions
  Address Book views 28
  anonymous connections 422
  CAs 60

Permissions (*continued*)
Dynamic RAS Connector 151, 161
IMAP4rev1 418
Internet Mail Service 113
Internet protocols 389
LDAP 438
Microsoft Mail Connector, Microsoft Mail (Appletalk) 240
Microsoft Outlook Web Access 507
POP3 399
published public folders 509
RAS MTA transport stack 144
remote dirsync requestor 343
Site Connector
override properties 140
Windows NT Server trust relationships 140
Site Encryption Configuration object 63
X.400 Connector 169, 197
Phone
communication, RAS MTA transport stack 141
Dynamic RAS Connector, book entry 148
MTA callback telephone number 143
numbers, custom recipients 15
RAS callback telephone number 152
RAS, book
adding connections 115
configuring RAS client 520
dial-up connections properties 114
viewing connections 114
Plain text attachment format 93
Policy module, Exchange 44
POP3
account names 412
authentication 399
client configuration 411 – 414
diagnostics logging 407
directory 399
disabling 395, 399
display name 399
e-mail address 413
enabling 399
general properties 398
idle time-out 406
Internet Mail Service
configuration 410
connections, number of 100
routing 118
Internet message formats 402, 404
Internet protocol 385
mailbox configuration 397, 407 – 409
Microsoft Internet Information Server (IIS) 400
overview 397
POP3 (*continued*)
restricting connections 389
rich text formatting 402 – 404
sample client configuration 414
server configuration 397 – 407
server name 413
site configuration 397 – 407
site defaults 399
SSL encryption 389, 400
Windows NT Challenge/Response 401
Ports, RAS server
address pool 516
configuration 516
Post Office Protocol version 3 *See* POP3
Post offices, cc:Mail Connector
directory synchronization 212
language 207
Netware server connections 223
options 207
overview 205
selecting 206
Postmaster mailbox 242
Postoffices
Microsoft Mail (PC)
directory synchronization requestor 343
manually importing address lists 352
remote dirsync requestor 337
Microsoft Mail Connector
access connection gateways 263
address space 312 – 315
Connector (PC) MTAs 282 – 289
defined 235, 271
directory server configuration 330
external 290
gateway 308 – 311
indirect access 280
installing Microsoft Exchange Connection 255
local, properties 244
Macintosh-accessible volume 238
Microsoft Exchange Connection, location 259
Microsoft Mail (PC), configuration 290, 304
Microsoft Mail (PC), modifying properties 291
Microsoft Mail (PC), testing connection 304
overview 271
removing connections 282
setup 272 – 273
Microsoft Mail, Dispatch 319
workgroup 296
Prefix
address space 83
e-mail 83

Primary language, Microsoft Mail Connector 276
Primary MIME types 394
Program files, Schedule+ 375
Promoting entries to parent containers, Address Book views 30
Propagating address listings, cc:Mail Connector 207
Propagating messages, cc:Mail Connector 231, 232
Protocols, Internet
  See also specific protocols
  connections
    accepting 390
    adding rules 391
    custom recipients 395
    disabling 395
    editing rules 392
    mailbox configuration 395
    MIME types 393 – 394
    moving rules 392
    overview 389
    rejecting 390
    removing rules 391
  defined 385
  list of supported 385
  overview 385
  servers
    defaults 388
    directory names 388
    display names 388
    general properties 387
    permissions 389
    properties, overview 385
  sites
    defaults 388
    directory names 388
    display names 388
    general properties 387
    permissions 389
    properties, overview 385
Providers, Internet newsfeed 454
Proxy
  format, Microsoft Mail (PC) 349
  names, cc:Mail Connector 211, 220
Public folders
  anonymous connections 421
  cc:Mail Connector
    distribution lists 233
    e-mail address generator 220
    e-mail addresses 231
    export containers 209
    overview 230
    propagating messages 231, 232
Public folders (*continued*)
  distribution lists, adding 17
  messages, delivery restrictions 17
  Microsoft Outlook Web Access, published 508 – 509
  newsgroups
    adding 459
    character sets 497
    control messages 452
    creating folders 474
    defined 447
    deleting 453
    hierarchies 451, 452, 477 – 478
    Internet News 450
    managing 452
    moderated 451
    naming 451
    new active file 472
    NNTP 483
    overview 450
    properties 496
    removing 459
    replication 450
  properties 3
Public information store, Internet News Service 448
Public telephone, RAS MTA transport stack 141
Published public folders, Microsoft Outlook Web Access
  overview 508
  permissions 509
  shortcuts 509
Pull feeds
  catching up current newsfeeds 453
  defined 448
  inbound
    adding newsgroups 471
    included newsgroups 470
    new active file 472
    overview 470
    removing newsgroups 471
Push feeds
  catching up current newsfeeds 453
  defined 448
  inbound
    included newsgroups 472
    multiple hosts 462
    new active file 474
    newsgroup public folders 474
    newsgroups, accepting items 473
    newsgroups, rejecting items 474
    overview 472
  Internet News Service configuration 455

Q

Quarterdeck Mail
  Macproxy.dll file 266
  Microsoft Mail Connector 235
Queued control messages, NNTP 485
Queues
  cc:Mail Connector
    deleting messages 222
    overview 221
    refreshing view 222
    viewing 222
  gateway postoffice 310
  Internet Mail Service, properties 113
  mail, notifications 106
  messages, flushing 454, 476
  Microsoft Mail (Appletalk) message 248
Quoting, text, Internet Mail Service 128

R

RAS
  authentication
    override accounts 521
    overview 520
    service account credentials 520
    user credentials 521
  callback telephone number 152
  client configuration 520
  connection time-out 116
  Connector *See* Dynamic RAS Connector
  Internet Mail Service, disabling ETRN support 131
  MTA transport stack
    connectors, defined 144
    general properties 143
    installation 141
    MTA callback telephone number 143
    name 143
    permissions 144
    RAS callback telephone number 152
  phone book, Internet Mail Service 114, 115
  server, Dynamic RAS Connector, configuration 515 – 517
RC2-128 encryption algorithm 64
RC2-40 encryption algorithm 64
RC2-64 encryption algorithm 64
Recipients
  See also Distribution lists
  Address Book views
    adding new recipient objects to container 32
    advanced properties 29 – 31
    calculating membership 34
    configuration 27 – 31
    creating 24 – 27
Recipients (*continued*)
  Address Book views (*continued*)
    customizing hierarchy 32
    deleting 34
    directory name 26
    display name 26, 33
    exporting 33
    general properties 26
    Group By properties 26
    moving recipient objects between containers 32
    overview 23 – 24
    parent containers, promoting entries to 30
    permissions 28
    removing empty containers 31
    restricting for anonymous users 33
    restricting offline 28
    restrictions 28
    setting up large 34
    showing views 31
  address type 83
  alternate 20
  attributes, custom 21 – 22
  cc:Mail Connector, containers 210
  custom
    address information 11
    advanced properties 12 – 14
    attachments 14
    cc:Mail Connector e-mail address generator 220
    cc:Mail Connector, export containers 209
    cc:Mail Connector, import containers 211
    company information 11
    creating 9
    described 9
    directory synchronization, trust levels 12
    distribution list membership 16
    e-mail addresses 11
    General property page 9
    hiding from Address Book 14
    Internet protocols 395
    message size limit 13
    Microsoft NetMeeting 13
    Microsoft Outlook Web Access, enabling HTTP 506
    NNTP 493 – 495
    NNTP client configuration 498
    NNTP newsfeeds 467
    organization information 14
    phone numbers 15
    rich text in messages 14
    user name information 10
  delivery options 19 – 21

Recipients (*continued*)
described 3
directory exchange requestor
removing addresses 353
viewing gateway information 351
directory synchronization
accepting messages 361
rejecting messages 362
dirsync requestor
containers 324, 325, 326
trust levels 324, 326
distribution lists
adding 17
deleting 17
memberships 16
removing 17
e-mail addresses 16
mass mailing 3
messages, delivery restrictions 17
Microsoft Mail templates 355
properties, common 16 – 22
remote dirsync requestor
containers 340, 341, 342
trust levels 340, 342
Schedule+ Free/Busy Connector
AdminSch accounts 375
unresolved messages 381
Records
A (address) 89
MX (mail exchanger) 89
Recovering security keys 69
Recovery timeout, X.400 Connector, overriding 185
Redundant replication of messages, Internet News Service 448
Refreshing, cc:Mail Connector, queues view 222
REG_DWORD key, Address Book views 34
Regeneration, address 246
Reissuing security keys 69
Rejecting
connections, Internet protocols 390
messages
cc:Mail Connector 223
directory synchronization 362
distribution lists 18
Dynamic RAS Connector 156
Internet Mail Service 111
X.400 Connector 193
Relocating *See* Moving
Remote
Access Service *See* RAS
directory requestor, configuration 343 – 355
Remote (*continued*)
directory synchronization requestor
manual directory synchronization 370
ResyncConnectionRDNs 370
dirsync requestor
address type 337
creating 335
dirsync server, setting up 331
export container properties 341
general properties 336
import container properties 339
importing directory synchronization master list manually 369 – 370
installation 335 – 343
mailbox 337
permissions properties 343
requirements 335
MTA, X.400 Connector
name 174
password 174
server, Dynamic RAS Connector
MTA override properties 152 – 155
name 147
override association parameters 154
override connection retry values 153
override transfer time-outs 154
phone book entry 148
RAS override properties 150 – 152
RTS values 153
scheduling 149 – 150
sites *See* Dynamic RAS Connector; Internet Mail Service; Site Connector; X.400 Connector
USENET hosts
dedicated connections 463
dial-up connections 463
FQDN 462
IP address 462
LAN connections 463
multiple inbound 462
overview 461
removing inbound connections 462
USENET sites, connecting to 461, 468
X.400 Connector, global domain identifier (GDI) 197
Removing
See also Deleting
Address Book details template controls 38
advanced security administrators 48
cc:Mail Connector
address space 219
export containers 211
Certificate Trust Lists 57

Removing (*continued*)
connected sites, Dynamic RAS Connector 161
containers 32
directory exchange requestor
addresses 353
recipients from world lists 354
directory synchronization
e-mail addresses 359
incoming template mappings 364
outgoing template mappings 366
dirsync requestor, export containers 326
distribution lists members 6, 17
e-mail addresses 16
empty containers, Address Book views 31
inbound host connections 462
Internet Mail Service
addresses 121
service 124
Internet protocols rules 391
Microsoft Mail Connector
address spaces 253
connections 282
MTA 288
MIME types 394
newsgroup public folders 459
newsgroups
inbound pull feeds 471
outbound feeds 476
public folder from hierarchy 478
remote dirsync requestor, export containers 342
target servers, Site Connector 139
X.400 Connector
connected sites 190
connector 200
Renaming custom attribute fields, recipient 22
Replace transactions 352
Replication
directory
Dynamic RAS Connector 158
Internet Mail Service 107, 110
messages, redundant, Internet News Service 448
newsgroup public folders 450
Reports
distribution lists
message originator 8
owners 8
non-delivery *See* NDRs
Requestor, dirsync *See* Dirsync requestor
Resolution
names, Internet Mail Service 89
reverse, Internet Mail Service 125
user name, Internet Mail Service 126
Restarting Microsoft Exchange Directory Synchronization Service 370
Restoring security data 72
Restrictions
Address Book views 28, 33
address spaces 84
delivery
distribution lists 17
Dynamic RAS Connector 155
X.400 Connector 192
Resync.glb file 369, 370
ResyncConnectionRDNs 370
Resynchronizing address information 354
Retry
connection, X.400 Connector 186
interval, Internet Mail Service 105
values, Dynamic RAS Connector 153
Reverse resolution, Internet Mail Service 125
Revoking
Certificate Trust Lists 57
mailbox security 68
RFC 2060 415
RFC 821 125
RFC 822 125
Rich text
custom recipients 14
Internet Mail Service 95, 97
POP3 402 – 404
X.400 Connector 176
RMGROUP control message 453
Roles
defined 63
Internet protocols, permissions 389
Routing
address
Dynamic RAS Connector connected sites 160
X.400 connected sites 190
costs 80, 136
Internet Mail Service
adding domains 118
addresses for address spaces 110
addresses, adding 121
addresses, editing 121
addresses, removing 121
connected sites 107
costs 109
custom programs 122
destinations 120
DNS 101
matching domain names 118
methods 120
properties 118 – 122

Routing (*continued*)
messages *See* Address spaces
Microsoft Mail (PC) postoffices indirect connections
manually creating information, indirect 307
uploading information, indirect 305
Microsoft Mail Connector 252
RTS
Dynamic RAS Connector, values 153
X.400 Connector, overriding 185
Rules, Internet protocols
adding 391
editing 392
moving 392
removing 391

S

S/MIME
disabling support 98
encryption algorithms 64
SASL security 122
Saving embedded objects, Microsoft Mail 3.x 277
Schedule
distribution
Schedule+ Free/Busy Connector 375
properties
dirsync server 334
Dynamic RAS Connector 149 – 150
Microsoft Mail (PC), dirsync requestor 329
X.400 Connector 177
Schedule+ Free/Busy Connector
administrator's mailbox 375, 377
AdminSch accounts 375
alias name 380
configuration 376 – 380
display name 380
distribution list, assigning 377
distribution list, exporting 378
exporting updates 378
general properties 379
installation 374 – 375
logging level 379
Microsoft Mail (PC) External program 374
overview 373
Schdist.exe 375
Schedule+
Administrator program 375
program files 375
versions 373
setup 374
unresolved messages 381
update frequency 378
Scheduling
cc:Mail Connector directory synchronization 216
Internet Mail Service connections 117
NNTP newsfeeds connections 468
Search control restrictions, Address Book views 28
Searching
LDAP, directory 441
Microsoft Exchange Server directory 435
Secure
connections, Internet 455
hosts, Internet Mail Service, accepting messages from 103
Security
advanced
adding administrators 48
administrators properties 47 – 48
backing up data 72
CA permissions 60
CA property pages 45
Certificate Trust Lists 55 – 58
changing passwords 48
configuration overview 45
described 43
enabling additional sites 70
enrollment properties 51 – 54
general properties 59
KM Server configuration 44
KM server, described 43
KM Server, installation 44
KM server, starting 45
mailboxes 65 – 69
moving KM server between sites 75
moving users between KM servers 73
passwords properties 49 – 50
removing administrators 48
restoring data 72
site 60 – 65
Site Encryption Configuration property pages 45
user security in remote sites 72
viewing log 73
Internet Mail Service
NTFS 87
properties 122
Microsoft Outlook Web Access, levels 503
NNTP newsfeeds 464 – 467
Selecting
directory exchange requestor gateway 348
dirsync requestor
export container 326
import container 324
remote dirsync requestor
export container 342
import container 340

Senders, accepting and rejecting messages
distribution lists 18
Dynamic RAS Connector 156
Server load, Address Book views 34
Server, dirsync *See* Dirsync server
Servers
bridgehead, Site Connector 136
expansion, distribution lists 5
IMAP4rev1
configuration 415 – 427
name 433
site defaults 417
Internet protocols
defaults 388
directory names 388
display names 388
general properties 387
permissions 389
properties, overview 385
LDAP
configuration 435 – 440
site defaults 437
messaging bridgehead *See* Messaging bridgehead servers
Netware, connection requirements 280
NNTP
client configuration 499
properties 481
POP3
name 413
site defaults 399
configuration 397 – 407
RAS, configuration 515 – 517
remote Dynamic RAS Connector
MTA override properties 152 – 155
name 147
override association parameters 154
override connection retry values 153
override transfer time-outs 154
phone book entry 148
RAS override properties 150 – 152
RTS values 153
scheduling 149 – 150
SMTP, name 413, 434
target, Site Connector 138 – 139
Service accounts
credentials 520
Dynamic RAS Connector 151
Site Connector 140
Setting idle time-outs
IMAP4rev1 427
LDAP 446
NNTP 491
POP3 406
Settings properties, Microsoft Mail (PC), dirsync requestor 327
Settings, original, Address Book details template controls 39
Setup
Address Book views, large 34
cc:Mail Connector 202
Connector (PC) MTAs
asynchronous connection 301
X.25 connection 302
diagnostics logging, Microsoft Mail Connector 294
Dynamic RAS Connector requirements 141
Internet News Service 455
LAN connection 279
Microsoft Exchange Connection 254 – 265
Microsoft Mail (Appletalk), directory exchange requestor 344
Microsoft Mail (PC) 3.x, remote directory requestor 343
Microsoft Mail (PC) postoffices indirect connections 305
Microsoft Mail Connector
asynchronous connection 295 – 297
connector 272 – 273
Microsoft Mail (Appletalk) 237
MTA 284
X.25 connection 295 – 297
Microsoft Mail Connector (Appletalk) MTA 243
Schedule+ Free/Busy Connector 374
Site Connector requirements 133
Shortcuts
cc:Mail Connector 227
published public folders 509
Showing views, Address Book 31
Signatures, digital
Certificate Trust Lists 55
described 43
mailbox security 66
revoking security 68
Signed messages
Internet Mail Service, converting to unsigned MIME 98
NNTP 489
Simple display names, distribution lists 7
Simple Mail Transfer Protocol *See* SMTP
Single character wildcards 80, 81, 82
Site Connector
address spaces
costs 137
defining 137
properties 137
bridgehead server 136
configuration 134
defined 133
general properties 135 – 136

Site Connector (*continued*)
installation 134
Microsoft Windows NT Server trust relationships 140
name 136
override properties 140
routing costs 136
setup requirements 133
target servers
adding and removing 139
costs 139
properties 138
Site Encryption Configuration object
display name 62
enabling additional sites 70
permissions 63
Site Encryption Configuration property pages 45, 60
Sites
See also Dynamic RAS Connector; Internet Mail Service; Site Connector; X.400 Connector
addressing, Dynamic RAS Connector connected sites 160
advanced security 45
cc:Mail Connector
moving connector 228 – 230
proxy names 220
connected
Dynamic RAS Connector 158 – 161
Internet Mail Service 107 – 108
messaging bridgehead servers 163
X.400 Connector 189 – 190
X.400, testing 199
foreign, X.400, testing 198
IMAP4rev1
configuration 415 – 427
defaults 417
Internet Mail Service, adding additional 123
Internet protocols
defaults 388
directory names 388
display names 388
general properties 387
permissions 389
properties, overview 385
KM Server
enabling additional 70
moving between 75
LDAP
configuration 435 – 440
defaults 437
NNTP
defaults 481
enabling 480
properties 481
Sites (*continued*)
POP3
configuration 397 – 407
defaults 399
remote USENET, connecting to 461, 468
remote, user security 72
restrictions, address spaces 84
security
advanced 60
choosing sites 62
display name 62
encryption algorithms 63 – 65
general properties 62
permissions 63
USENET name 483
X.400 Connector
TCP/IP connection 179
TP4 connection 182
X.25 connection 180
Size
Address Book views 34
address, Microsoft Mail (Appletalk) 261
message
cc:Mail Connector 209
custom recipients 13
distribution lists 7
Dynamic RAS Connector 148
e-mail domain 97
Internet Mail Service 112
Microsoft Mail Connector 250, 279
NNTP newsfeeds 460
X.400 Connector 196
Slash mark (/) 412, 415
SMTP
address space type 79, 80, 81
attachment format 93
commands 125
headers 125
hosts, Internet Mail Service, routing 118
IMAP4rev1
e-mail address 433
messages 431
server name 434
Internet Mail Service
connections, number of 100
disabling ETRN support 131
ESMTP 130 – 132
loopback detection 127
overview 87
protocol log 113
reverse resolution 125

SMTP (*continued*)
Internet Mail Service (*continued*)
routing address 107
updating Hosts file 90
user name resolution 126
VRFY 127
Internet protocol 385
Microsoft Mail gateway 308
POP3
e-mail address 413
messages 411
server name 413
RFC 821 125
RFC 822 125
SNADS gateway 308
SSL encryption
IMAP4rev1 419
Internet Mail Service 122
Internet protocols 389
LDAP 438
Microsoft Outlook Web Access 503
NNTP 485, 498, 499
NNTP newsfeeds 464 – 466
POP3 400
Stack properties
X.400 Connector 178 – 182
Stack, MTA transport *See* MTA transport stack
Starting
directory exchange requestor 350
directory synchronization 366, 368
KM Server 45
Startup item, directory exchange requestor 351
Stopping, directory synchronization 367
Subdomains *See* Domains
Subnet masks, Internet protocols 391
Subscribing, USENET newsfeeds 454
Substring searches, LDAP, directory 441
Subtype MIME types 394
Swedish, inbound message conversion 195
System messages
directory synchronization
delivery restrictions 359
e-mail addresses, changing 358
e-mail addresses, creating 358
e-mail addresses, removing 359
dirsync server 322, 332
remote dirsync requestor 337

T

T1 time 330, 334
Target servers, Site Connector
adding and removing 139
costs 139
properties 138 – 139
TCP/IP
defined 385
Dynamic RAS Connector
configuration 515, 517 – 519
Internet Mail Service installation 88
RAS server configuration
address pool 516
enabling 516
X.400 Connector MTA transport stack
installation 166
overview 164
X.400 Connector, site connection 179
TeachText 354
Telephone
Dynamic RAS Connector, book entry 148
MTA callback number 143
numbers, custom recipients 15
RAS callback telephone number 152
RAS client, phone book entry 520
RAS MTA transport stack 141
Templates
address space type 80
detail *See* Details templates
directory synchronization
incoming 362 – 364
outgoing 364 – 366
foreign language details *See* Foreign language details templates
Microsoft Mail recipient information 355
one-off address *See* One-off address templates
Temporary keys
mailbox security 66
transmitting 52
Text
See also Rich text
files, directory exchange requestor, manually exporting world lists 352
quoting, Internet Mail Service 128
Timeout, X.400 Connector
recovery, overriding 185
transfer, overriding 187
Time-outs
IMAP4rev1 426
Internet Mail Service, messages 105

Time-outs (*continued*)
LDAP 445
NNTP idle 490
POP3 406
RAS connections 116
transfer, Dynamic RAS Connector 154
TP0/X.25, X.400 Connector MTA transport stack 164
TP4
X.400 Connector MTA transport stack, installation 168
X.400 Connector, site connection 182
TP4/CLNP, X.400 Connector MTA transport stack 164
Tracking messages
Internet Mail Service 129
Microsoft Mail Connector 243, 277
Transactions, add 352
Transfer
loops, message 197
modes, Internet Mail Service 100
time-outs, Dynamic RAS Connector 154
timeouts, X.400 Connector, overriding 187
Transmitting temporary keys 52
Transport Control Protocol/Internet Protocol *See* TCP/IP
Transport stack, MTA *See* MTA transport stack
Transport stack, RAS MTA
connectors, defined 144
general properties 143
installation 141
MTA callback telephone number 143
name 143
permissions 144
RAS callback telephone number 152
Troubleshooting
See also Error messages
cc:Mail Connector, diagnostics logging 222
directory synchronization, diagnostics logging 366
dirsync server, system messages 332
IMAP4rev1 427
Internet Mail Service
diagnostics logging 113
message tracking 129
Microsoft Mail Connector
diagnostics logging 253, 294
message tracking 243, 277
MTA message queue 248
NNTP 493
POP3 407
Schedule+ Free/Busy Connector, logging level 379
X.400 Connector, connections 199
Trust levels
cc:Mail Connector, export containers 210
directory synchronization
custom recipients 12
distribution lists 8
Trust levels (*continued*)
dirsync requestor, import container 324, 326
remote dirsync requestor, import container 340, 342
Trust relationships, Windows NT Server 140

U

UNC, network paths 280
Uniform naming convention (UNC), network paths 280
Unresolved Schedule+ messages 381
Update frequency, Schedule+ Free/Busy Connector 378
Updating, Hosts file 90
Uploading, Microsoft Mail (PC) postoffices indirect connections, routing information, indirect 305
Urgent messages 105, 106, 187
URLs, cc:Mail Connector 227
USENET
connection schedule 468
hosts
See also Host Computers, NNTP
control messages 453
current newsfeeds 453
dedicated connections 463
dial-up connections 463
FQDN 462
IP address 462
newsfeeds, subscribing to 454
remote sites, connecting to 461, 468
site name 483
Users
accounts
IMAP4rev1 432
POP3 412
address size, Microsoft Mail (Appletalk) 261
advanced security 45
anonymous
Microsoft Outlook Web Access 504
restricting Address Book views 33
authentication, anonymous connections 440
bulk enrollment 53
Busy times, defined 373
cc:Mail Connector, names, imported 211
credentials, RAS authentication 521
enrollment welcome message 52
Free times, defined 373
IMAP4rev1, permissions 418
Internet Mail Service, name resolution 126
Microsoft Outlook Web Access
Address Book entries returned 510
anonymous 507, 509
moving between KM servers 73

Users (*continued*)
permissions
Internet protocols 389
LDAP 438
POP3 399
security, remote site 72
transmitting temporary keys 52
validated 503
UUENCODE
Internet Mail Service
attachment format 93
e-mail domain 97
rich text formatting 95
NNTP messages 489
POP3 messages 404

V

V1 certificate format 54
V3 certificate format 54
Validated users 503
Viewing
cc:Mail Connector queues 222
Certificate Trust Lists 58
computer name 278
directory exchange requestor gateway recipient information 351
embedded objects, Microsoft Mail 3.x 277
gateway postoffice queue 310
LAN connection 280
mailbox security 69
Microsoft Mail Connector MTA message queue 248
newsfeed properties 482
one-off address templates, Address Book 39
RAS connections 114
security log 73
Views, Address Book
adding new recipient objects to container 32
advanced properties 29 – 31
calculating membership 34
configuration 27 – 31
creating 24 – 27
customizing hierarchy 32
deleting 34
directory name 26
display name 26
display names 33
exporting recipients 33
general properties 26
Group By properties 26
moving recipient objects between containers 32
overview 23 – 24
Views, Address Book (*continued*)
parent containers, promoting entries to 30
permissions 28
removing empty containers 31
restricting for anonymous users 33
restricting offline 28
restrictions 28
setting up large 34
showing 31
Volume
Macintosh-accessible 238
Microsoft Mail Connector permissions 240
VRFY 127

W

Web Access *See* Microsoft Outlook Web Access
Web browsers, Microsoft Outlook Web Access
enabling access 506
installation 502
Welcome message, enrollment 52
Wildcards, address spaces 80, 81, 82, 83, 314
Windows
16-bit e-mail clients, Address Book views, large 34
X.400 Connector, size, overriding 185
Windows NT *See* Microsoft Windows NT
Windows NT Server *See* Microsoft Windows NT Server
Wizard, Newsfeed Configuration
Internet News Service 455
newsfeeds, NNTP 456
Word-wrap
Internet Mail Service 128
X.400 Connector 175
Workgroup postoffices 296
World lists, directory exchange requestor 352, 354

X

X.25
Microsoft Mail Connector
Connector (PC) MTAs 282
interchange properties 275 – 277
Microsoft Mail (PC) postoffice 295
Microsoft Mail (PC) postoffices 304
Microsoft Mail (PC) postoffices indirect connections 307
modifying MTA 303
MTA configuration 299 – 303
MTA setup 302
overview 271
setting options 298
setup 272 – 273, 295 – 297

X.25 (*continued*)
packet assembly/disassembly (PAD), RAS MTA transport stack 141
X.400 Connector MTA transport stack
installation 167
overview 164
X.400 Connector, site connection 180
X.400
address space type 79, 80
Dynamic RAS Connector
address 160
address spaces 157
e-mail address type 357
Microsoft Mail gateway 308
X.400 Connector
accepting messages from specific senders 193
adding 173
address space properties 187
advanced properties 194 – 197
association parameters, overriding 186
body parts 195
configuration 171
connected sites
adding 189
costs 190
overview 189
removing 190
routing address 190
testing 199
connection retry, overriding 186
connection schedule 178
connector name 174
defined 133
delivery restrictions 192
directory exchange requestor, address type 349
directory name 174
display name 174
foreign sites, testing 198
foreign systems
configuration 197
overview 163
general properties 173 – 176
installation requirements 163
link options 196
local MTA name, overriding 184
local MTA password, overriding 184
message size 196
message text word-wrap 175
messaging bridgehead servers 163
Microsoft Mail Connector, foreign system access 308
X.400 Connector (*continued*)
MTA
remote name 174
remote password 174
remote transport stack 175
MTA conformance, configuration 195
MTA transport stack
Connectors property page 169
installation 165
installing TCP/IP 166
installing TP4 168
installing X.25 167
overview 164
permissions 169
override properties 183 – 187
overview 163, 171
permissions 197
rejecting messages from specific senders 193
remote global domain identifier (GDI) 197
removing 200
resetting override values 187
rich text 176
RTS values, overriding 185
schedule properties 177
stack properties 178 – 182
TCP/IP connection 179
TP4 connection 182
transfer timeouts, overriding 187
X.25 connection 180