

Administration Guide

GroupWise 2012

August 2014

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2003-2013 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see the [Novell Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the [Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	33
Part I System	35
1 GroupWise System Administration	37
2 ConsoleOne Administration Tool	39
2.1 ConsoleOne on Linux	39
2.1.1 Installing Linux ConsoleOne	40
2.1.2 Installing the GroupWise Administrator Snap-Ins to Linux ConsoleOne	40
2.1.3 Enabling File Locking on OES Linux	41
2.1.4 Starting Linux ConsoleOne	41
2.1.5 Mounting a Linux File System for a Domain or a Post Office	42
2.1.6 Changing the Linux Mount Directory	46
2.2 ConsoleOne on Windows	46
2.2.1 Installing ConsoleOne and the GroupWise Snap-Ins on Windows	46
2.2.2 Configuring Your Windows Machine for ConsoleOne	47
2.2.3 Starting ConsoleOne on Windows	47
2.2.4 Mapping a Drive for a New Domain or Post Office	47
2.3 ConsoleOne in a Multiple-Platform Environment	48
2.3.1 Using Linux ConsoleOne to Access Domains and Post Offices on Windows	48
2.3.2 Using Windows ConsoleOne to Access Domains and Post Offices on Linux	50
2.4 Remote Access to ConsoleOne on a Linux Server	56
2.4.1 Administrative Tasks Requiring File System Mounts	56
2.4.2 Remote ConsoleOne Access with a VNC Client	57
2.4.3 Remote ConsoleOne Access with a Secure Shell (SSH) Connection	58
3 GroupWise View	61
3.1 eDirectory View versus GroupWise View	61
3.2 GroupWise Object Icons	62
3.3 Customizing the GroupWise View	64
3.3.1 Changing the Column Display and Order	64
3.3.2 Changing the Column Widths	66
3.4 Searching in the GroupWise View	66
3.5 Performing Administrative Tasks from the GroupWise View	67
4 GroupWise System Operations	69
4.1 Select Domain	69
4.1.1 Selecting a Domain to Connect To	70
4.1.2 Understanding the Need for Domain Connections	71
4.1.3 Handling Cross-Platform Domain Connections	71
4.2 System Preferences	72
4.2.1 Admin Preferences	73
4.2.2 Routing Options	74
4.2.3 External Access Rights	74
4.2.4 Nickname Settings	75
4.2.5 Default Password	76

4.2.6	Admin Lockout Settings	76
4.2.7	Archive Service Settings	77
4.2.8	Linux Settings (Linux ConsoleOne Only)	78
4.3	eDirectory User Synchronization	79
4.4	Admin-Defined Fields	79
4.5	Pending Operations	80
4.6	Addressing Rules	80
4.7	Time Zones	81
4.7.1	Modifying a Time Zone Definition	81
4.7.2	Adding a Time Zone Definition	82
4.7.3	Deleting a Time Zone Definition	83
4.8	External System Synchronization	84
4.9	Software Directory Management	84
4.9.1	Creating a Software Distribution Directory	85
4.9.2	Updating a Software Distribution Directory	87
4.9.3	Deleting a Software Distribution Directory	88
4.10	Restore Area Management	89
4.11	Internet Addressing	89
4.12	Trusted Applications	90
4.12.1	Creating a Trusted Application and Key	90
4.12.2	Editing a Trusted Application	92
4.12.3	Deleting a Trusted Application	93
4.13	LDAP Servers	93
4.14	Global Signatures	94

5 GroupWise Utilities 95

5.1	Mailbox/Library Maintenance	95
5.2	System Maintenance	96
5.3	Backup/Restore Mailbox	96
5.4	Recover Deleted Account	96
5.5	Client Options	96
5.6	Expired Records	96
5.7	Email Address Lookup	96
5.8	Synchronize	97
5.9	User Move Status	97
5.10	Link Configuration	97
5.11	Document Properties Maintenance	97
5.12	New System	98
5.13	Check eDirectory Schema	98
5.14	Gateway Alias Migration	98
5.15	GW / eDirectory Association	99
5.15.1	Graft GroupWise Objects	99
5.15.2	Invalid Associations	100
5.15.3	Associate Objects	101
5.15.4	Disassociate GroupWise Attributes	102
5.15.5	Convert External Entity to User	102
5.15.6	Convert User to External Entity	103
5.16	Standalone GroupWise Utilities	103
5.16.1	GroupWise Check Utility (GWCheck)	103
5.16.2	GroupWise Backup Time Stamp Utility (GWTMSTMP)	103
5.16.3	GroupWise Database Copy Utility (DBCOPY)	104
5.16.4	GroupWise Generate CSR Utility (GWCSRGEN)	104

6	GroupWise Address Book	105
6.1	Customizing Address Book Fields	105
6.1.1	Adding eDirectory Fields to the Address Book	106
6.1.2	Adding LDAP Fields to the Address Book	107
6.1.3	Changing the Default Sort Order	108
6.1.4	Changing the Default Field Order	109
6.1.5	Removing Fields from the Address Book	109
6.1.6	Preventing the User Description Field from Displaying in the Address Book	109
6.2	Controlling Object Visibility	110
6.3	Updating Address Book Information	110
6.3.1	Synchronizing Information	111
6.3.2	Rebuilding the Post Office Database	111
6.4	Controlling Users' Frequent Contacts Address Books	111
6.5	Controlling Address Book Synchronization for Caching and Remote Client Users	112
6.6	Publishing Email Addresses to eDirectory	113
6.7	Enabling Wildcard Addressing	114
6.7.1	Setting Wildcard Addressing Levels	114
6.7.2	Wildcard Addressing Syntax	115
6.8	Adding External Users to the GroupWise Address Book	116
6.8.1	Creating a Non-GroupWise Domain to Represent the Internet	116
6.8.2	Linking to the Non-GroupWise Domain	117
6.8.3	Creating a Non-GroupWise Post Office to Represent an Internet Host	119
6.8.4	Creating External Users	120
6.8.5	Configuring External Users and Resources to Appear in GroupWise Busy Searches	121
7	Multilingual GroupWise Systems	123
7.1	GroupWise User Languages	123
7.2	GroupWise Administration and Agent Languages	124
7.3	International Character Considerations	125
7.4	MIME Encoding	125
7.5	Multi-Language Workstations	127
Part II	Domains	129
8	Creating a New Domain	131
8.1	Understanding the Purpose of Domains	131
8.2	Planning a New Domain	132
8.2.1	Determining When to Add a New Domain	133
8.2.2	Deciding Who Will Administer the New Domain	133
8.2.3	Planning Post Offices in the New Domain	134
8.2.4	Determining the Context for the Domain Object	134
8.2.5	Choosing the Domain Name	136
8.2.6	Deciding Where to Create the Domain Directory	136
8.2.7	Deciding Where to Install the Agent Software	137
8.2.8	Deciding How to Link the New Domain	137
8.2.9	Selecting the Domain Language	138
8.2.10	Selecting the Domain Time Zone	138
8.3	Setting Up the New Domain	138
8.3.1	Creating the New Domain	139
8.3.2	Configuring the MTA for the New Domain	141
8.3.3	Installing and Starting the New MTA	141
8.4	What's Next	142
8.5	New Domain Summary Sheet	142

9	Managing Domains	145
9.1	Connecting to a Domain	145
9.2	Editing Domain Properties	146
9.3	Converting a Secondary Domain to a Primary Domain	150
9.4	Replacing the Primary Domain Database with a Secondary Domain Database	151
9.5	Moving a Domain	152
9.6	Deleting a Domain	153
9.7	Changing the MTA Configuration to Meet Domain Needs	154
10	Managing the Links between Domains and Post Offices	155
10.1	Understanding Link Configuration	155
10.1.1	Domain-to-Domain Links	155
10.1.2	Domain-to-Post-Office Links	158
10.1.3	Link Protocols for Direct Links	159
10.2	Using the Link Configuration Tool	161
10.2.1	Starting the Link Configuration Tool	161
10.2.2	Editing a Domain Link	162
10.2.3	Editing Multiple Domain Links	163
10.2.4	Editing a Post Office Link	165
10.2.5	Viewing the Path of an Indirect Link between Domains	165
10.2.6	Viewing the Indirect Links Passing through a Domain	166
10.2.7	Viewing the Gateway Links Passing through a Gateway	167
10.2.8	Saving and Synchronizing Link Configuration Information	168
10.3	Interpreting Link Symbols	168
10.3.1	Link Type Symbols	168
10.3.2	Link Status Symbols	169
10.4	Modifying Links	169
Part III	Post Offices	171
11	Creating a New Post Office	173
11.1	Understanding the Purpose of Post Offices	173
11.2	Planning a New Post Office	174
11.2.1	Determining When to Add a Post Office	174
11.2.2	Selecting the Domain That the Post Office Belongs To	176
11.2.3	Determining the Context for the Post Office Object	176
11.2.4	Choosing the Post Office Name	176
11.2.5	Deciding Where to Create the Post Office Directory	177
11.2.6	Deciding Where to Install the Agent Software	178
11.2.7	Deciding How to Link the New Post Office	178
11.2.8	Selecting the Post Office Language	179
11.2.9	Selecting the Post Office Time Zone	179
11.2.10	Selecting a Software Distribution Directory	179
11.2.11	Selecting a Post Office Security Level	180
11.2.12	Deciding if You Want to Create a Library for the New Post Office	180
11.3	Setting Up the New Post Office	181
11.3.1	Creating the New Post Office	181
11.3.2	Configuring the POA for the New Post Office	185
11.3.3	Installing and Starting the New POA	186
11.3.4	Setting Up User Access to the New Post Office	186
11.4	What's Next	186
11.5	New Post Office Summary Sheet	187

12 Managing Post Offices	189
12.1 Connecting to the Domain That Owns a Post Office	189
12.2 Editing Post Office Properties	190
12.3 Managing Disk Space Usage in the Post Office	196
12.3.1 Understanding Disk Space Usage and Mailbox Size Limits	196
12.3.2 Preparing to Implement Disk Space Management	197
12.3.3 Setting Mailbox Size Limits	198
12.3.4 Enforcing Mailbox Size Limits	200
12.3.5 Restricting the Size of Messages That Users Can Send	201
12.3.6 Preventing the Post Office from Running Out of Disk Space	203
12.3.7 An Alternative to Disk Space Management in the Post Office	206
12.3.8 Forcing Caching Mode	206
12.4 Auditing Mailbox License Usage in the Post Office	207
12.5 Viewing Current Client Usage in the Post Office	209
12.6 Tracking and Restricting Client Access to the Post Office	209
12.7 Securing the Post Office with LDAP Authentication	211
12.8 Refreshing the Client View Files in the Post Office	211
12.9 Disabling a Post Office	212
12.10 Moving a Post Office	212
12.11 Deleting a Post Office	214
12.12 Changing POA Configuration to Meet Post Office Needs	215
Part IV Users	217
13 Creating GroupWise Accounts	219
13.1 Establishing a Default Password for All New GroupWise Accounts	219
13.2 Creating GroupWise Accounts for eDirectory Users	220
13.2.1 Creating a Single GroupWise Account	220
13.2.2 Creating Multiple GroupWise Accounts	222
13.3 Creating GroupWise Accounts for Non-eDirectory Users	224
13.4 Educating Your New Users	226
13.4.1 GroupWise Windows Client	226
13.4.2 GroupWise WebAccess	227
13.4.3 GroupWise WebAccess Mobile	227
14 Managing GroupWise Accounts and Users	229
14.1 Adding a User to a Distribution List	229
14.2 Allowing Users to Modify Distribution Lists	230
14.3 Adding a Global Signature to Users' Messages	231
14.3.1 Creating Global Signatures	231
14.3.2 Selecting a Default Global Signature for All Outgoing Messages	232
14.3.3 Assigning Global Signatures to GWIAs	233
14.3.4 Assigning Global Signatures to Windows Client Users	233
14.3.5 Excluding Global Signatures	234
14.4 Moving GroupWise Accounts	234
14.4.1 Live Move vs. File Transfer Move	235
14.4.2 Preparing for a User Move	235
14.4.3 Moving a GroupWise Account to Another Post Office in the Same eDirectory Tree	236
14.4.4 Moving a GroupWise Account to Another Post Office in a Different eDirectory Tree	238
14.4.5 Monitoring User Move Status	240
14.5 Renaming Users and Their GroupWise Accounts	242
14.6 Managing Mailbox Passwords	243
14.6.1 Creating or Changing a Mailbox Password	243

14.6.2	Removing a Mailbox Password	245
14.6.3	Bypassing the GroupWise Password	246
14.7	Managing User Email Addresses	247
14.7.1	Ensuring Unique Email Addresses	248
14.7.2	Changing a User's Internet Addressing Settings	249
14.7.3	Changing a User's Visibility in the Address Book	251
14.7.4	Creating a Nickname for a User	252
14.8	Checking GroupWise Account Usage	253
14.9	Disabling and Enabling GroupWise Accounts	254
14.10	Unlocking GroupWise Accounts	254
14.11	Removing GroupWise Accounts	255
14.11.1	Deleting a GroupWise Account	255
14.11.2	Expiring a GroupWise Account	257
14.11.3	Managing Expired or Expiring GroupWise Accounts	258
Part V Resources		263
15 Creating Resources		265
15.1	Understanding Resources	265
15.1.1	Resource Objects	265
15.1.2	Resource Types	265
15.1.3	Resource Mailboxes	266
15.1.4	Resource Owners	266
15.2	Planning Resources	266
15.3	Creating a New Resource	267
16 Managing Resources		269
16.1	Creating Rules for a Resource	269
16.1.1	Creating an Auto-Accept Rule	269
16.1.2	Creating an Auto-Denial Rule	270
16.2	Changing a Resource's Owner	271
16.3	Adding a Resource to a Distribution List	272
16.4	Moving a Resource	273
16.5	Renaming a Resource	273
16.6	Deleting a Resource	274
16.7	Managing Resource Email Addresses	274
16.7.1	Changing a Resource's Internet Addressing Settings	274
16.7.2	Changing a Resource's Visibility in the Address Book	275
16.7.3	Creating a Nickname for a Resource	276
Part VI Distribution Lists, Groups, and Organizational Roles		279
17 Understanding Distribution Lists, Groups, and Organizational Roles		281
17.1	Public vs. Personal Address Lists	281
17.2	Distribution Lists	281
17.3	eDirectory Groups and Organizational Roles	282
18 Creating and Managing Distribution Lists		285
18.1	Creating a New Distribution List	285
18.2	Adding Members to a Distribution List	289
18.3	Removing Members from a Distribution List	290

18.4	Moving a Distribution List	290
18.5	Renaming a Distribution List	291
18.6	Enabling Users to Modify a Distribution List	291
18.7	Controlling Access to a Distribution List	293
18.8	Deleting a Distribution List	294
18.9	Managing Email Addresses	294
18.9.1	Changing a Distribution List's Internet Addressing Settings	295
18.9.2	Changing a Distribution List's Visibility in the Address Book	296
18.9.3	Creating a Nickname for a Distribution List	297
18.10	Adding External Users to a Distribution List	299
18.10.1	Creating an External Domain	299
18.10.2	Creating an External Post Office	299
18.10.3	Creating an External User	299
19	Using eDirectory Groups as GroupWise Distribution Lists	301
19.1	Setting Up an eDirectory Group for Use in GroupWise	301
19.2	Seeing Which Members of an eDirectory Group Have GroupWise Accounts	303
19.3	Changing a Group's Visibility in the Address Book	304
19.4	Moving a Group	304
19.5	Renaming a Group	305
19.6	Removing a Group from GroupWise	305
20	Using eDirectory Organizational Roles as GroupWise Distribution Lists	307
20.1	Setting Up an Organizational Role for Use in GroupWise	307
20.2	Seeing Which Members of an Organizational Role Have GroupWise Accounts	308
20.3	Changing an Organizational Role's Visibility in the Address Book	309
20.4	Moving an Organizational Role	310
20.5	Renaming an Organizational Role	310
20.6	Removing an Organizational Role from GroupWise	311
Part VII	Libraries and Documents	313
21	Document Management Services Overview	315
21.1	Libraries	316
21.2	Document Storage Areas	317
21.3	Documents	318
21.3.1	Document Properties	318
21.3.2	Document Types	319
21.4	Integrations	321
22	Creating and Managing Libraries	323
22.1	Planning a Basic Library	324
22.1.1	Selecting the Post Office That the Library Will Belong To	324
22.1.2	Determining the Context for the Library Object	324
22.1.3	Choosing the Library Name	324
22.1.4	Deciding Where to Store Documents	325
22.2	Setting Up a Basic Library	326
22.2.1	Creating the Basic Library	326
22.3	Planning Full-Service Libraries	328
22.3.1	Deciding Which Libraries to Create	328
22.3.2	Selecting the Post Offices To Own Libraries	332

22.3.3	Determining the Contexts for Library Objects	332
22.3.4	Choosing Library Names	332
22.3.5	Deciding Where to Store Documents	333
22.3.6	Setting Document Version Options	335
22.3.7	Figuring Maximum Archive Directory Size	335
22.3.8	Designating Initial Librarians	336
22.3.9	Restricting Initial Public Library Rights	337
22.3.10	Determining Your Indexing Needs	338
22.3.11	Determining If You Need to Set Up Integrations for DMS Users	338
22.4	Setting Up a Full-Service Library	338
22.4.1	Creating the Full-Service Library	338
22.4.2	What's Next	340
22.5	Viewing a New Library in Your GroupWise System	341
22.5.1	Seeing the New Library in ConsoleOne	341
22.5.2	Seeing the New Library in the GroupWise Windows Client	342
22.6	Managing Libraries	342
22.6.1	Editing Library Properties	343
22.6.2	Managing Document Storage Areas	345
22.6.3	Managing Library Access	348
22.6.4	Adding and Training Librarians	350
22.6.5	Maintaining Library Databases	354
22.6.6	Moving a Library	354
22.6.7	Deleting a Library	354
22.7	Library Worksheets	355
22.7.1	Basic Library Worksheet	355
22.7.2	Full-Service Library Worksheet	356

23 Creating and Managing Documents 359

23.1	Adding Documents to Libraries	359
23.1.1	Creating New Documents in the GroupWise Windows Client	359
23.1.2	Importing Existing Documents into the GroupWise DMS System	360
23.1.3	Managing Groups of Documents	361
23.2	Organizing Documents in Libraries	362
23.2.1	Customizing Document Properties	362
23.2.2	Defining Related Document Properties	371
23.3	Indexing Documents in Libraries	374
23.3.1	Understanding DMS Indexing	374
23.3.2	Determining Your Indexing Needs	381
23.3.3	Implementing Indexing	383
23.4	Managing Documents in Libraries	383
23.4.1	Archiving and Deleting Documents	383
23.4.2	Backing Up and Restoring Archived Documents	383
23.4.3	Handling Orphaned Documents	385

24 Integrations 387

24.1	Setting Up Integrations during Windows Client Installation	387
24.2	Setting Up Integrations Using the gwappint.inf File	388
24.2.1	Understanding the Three Levels of Integration	389
24.2.2	Understanding the gwappint.inf File	390
24.2.3	Editing the gwappint.inf File	392
24.3	Controlling Integrations in the GroupWise Windows Client	393

Part VIII Databases	395
25 Understanding GroupWise Databases	397
25.1 Domain Databases	397
25.2 Post Office Databases	398
25.3 User Databases	398
25.4 Message Databases	398
25.5 Library Databases	399
25.6 Guardian Databases	399
26 Maintaining Domain and Post Office Databases	401
26.1 Validating Domain or Post Office Databases	401
26.2 Recovering Domain or Post Office Databases	402
26.3 Rebuilding Domain or Post Office Databases	405
26.4 Rebuilding Database Indexes	407
27 Maintaining User/Resource and Message Databases	409
27.1 Analyzing and Fixing User and Message Databases	409
27.2 Performing a Structural Rebuild of a User Database	411
27.3 Re-creating a User Database	412
28 Maintaining Library Databases and Documents	415
28.1 Analyzing and Fixing Databases for Libraries and Documents	415
28.2 Analyzing and Fixing Library and Document Information	416
29 Synchronizing Database Information	419
29.1 Synchronizing Individual Users or Resources	419
29.2 Synchronizing a Post Office	420
29.3 Synchronizing a Library	421
29.4 Synchronizing a Secondary Domain	421
29.5 Synchronizing the Primary Domain from a Secondary Domain	422
30 Managing Database Disk Space	423
30.1 Gathering Mailbox Statistics	423
30.2 Reducing the Size of User and Message Databases	425
30.3 Reclaiming Disk Space in Domain and Post Office Databases	427
30.4 Reducing the Size of Libraries and Document Storage Areas	428
30.4.1 Archiving and Deleting Documents	428
30.4.2 Deleting Activity Logs	429
31 Backing Up GroupWise Databases	431
31.1 Backing Up a Domain	431
31.2 Backing Up a Post Office	431
31.3 Backing Up a Library and Its Documents	432
31.4 Backing Up Individual Databases	432

32 Restoring GroupWise Databases from Backup	433
32.1 Restoring a Domain	433
32.2 Restoring a Post Office	433
32.3 Restoring a Library	434
32.4 Restoring an Individual Database	434
32.5 Restoring Deleted Mailbox Items	435
32.5.1 Setting Up a Restore Area	435
32.5.2 Restoring a User's Mailbox Items	437
32.5.3 Letting Client Users Restore Their Own Mailbox Items	437
32.6 Recovering Deleted GroupWise Accounts	438
33 Retaining User Messages	441
33.1 How Message Retention Works	441
33.1.1 What GroupWise Does	442
33.1.2 What the Message Retention Application Does	443
33.2 Acquiring a Message Retention Application	443
33.3 Enabling Message Retention	444
34 Stand-Alone Database Maintenance Programs	447
34.1 GroupWise Check	447
34.1.1 GWCheck Functionality	447
34.1.2 Using GWCheck on Windows	449
34.1.3 Using GWCheck on Linux	450
34.1.4 Performing Mailbox/Library Maintenance Using GWCheck	452
34.1.5 Executing GWCheck from a Windows Batch File	454
34.1.6 Executing GWCheck from a Linux Script	455
34.1.7 GWCheck Startup Switches	455
34.2 GroupWise Time Stamp Utility	457
34.2.1 GWTMSTMP Functionality	457
34.2.2 Running GWTMSTMP on Linux	458
34.2.3 Running GWTMSTMP on Windows	459
34.2.4 GWTMSTMP Startup Switches	459
34.3 GroupWise Database Copy Utility	463
34.3.1 DBCopy Functionality	463
34.3.2 Using DBCopy on Linux	464
34.3.3 Using DBCopy on Windows	465
34.3.4 DBCopy Startup Switches	465
Part IX Post Office Agent	469
35 Understanding Message Delivery and Storage in the Post Office	471
35.1 Post Office Representation in ConsoleOne	471
35.2 Post Office Directory Structure	472
35.3 Information Stored in the Post Office	472
35.3.1 Post Office Database	472
35.3.2 Message Store	473
35.3.3 Guardian Database	474
35.3.4 Agent Input/Output Queues in the Post Office	475
35.3.5 Libraries (optional)	476
35.4 Post Office Access Mode	476
35.5 Role of the Post Office Agent	477
35.5.1 Client/Server Processing	477
35.5.2 Message File Processing	478

35.5.3	Other POA Functions	478
35.6	Message Flow in the Post Office	479

36 Configuring the POA 481

36.1	Performing Basic POA Configuration	482
36.1.1	Creating a POA Object in eDirectory	482
36.1.2	Configuring the POA in ConsoleOne	484
36.1.3	Changing the Link Protocol between the Post Office and the Domain	487
36.1.4	Binding the POA to a Specific IP Address	490
36.1.5	Moving the POA to a Different Server	490
36.1.6	Adjusting the POA for a New Post Office Location	491
36.1.7	Configuring the POA for Remote Server Login (Windows Only)	492
36.1.8	Adjusting the POA Logging Level and Other Log Settings	493
36.2	Configuring User Access to the Post Office	494
36.2.1	Using Client/Server Access to the Post Office	494
36.2.2	Simplifying Client/Server Access with a GroupWise Name Server	496
36.2.3	Supporting IMAP Clients	498
36.2.4	Supporting SOAP Clients	499
36.2.5	Checking What GroupWise Clients Are in Use	502
36.2.6	Supporting Forced Mailbox Caching	503
36.2.7	Restricting Message Size between Post Offices	504
36.2.8	Supporting Calendar Publishing	505
36.3	Configuring Post Office Security	505
36.3.1	Securing Client/Server Access through an External Proxy Server	506
36.3.2	Controlling Client Redirection Inside and Outside Your Firewall	507
36.3.3	Securing the Post Office with SSL Connections to the POA	508
36.3.4	Providing LDAP Authentication for GroupWise Users	510
36.3.5	Enabling Intruder Detection	516
36.3.6	Configuring Trusted Application Support	517
36.4	Configuring Post Office Maintenance	517
36.4.1	Scheduling Database Maintenance	517
36.4.2	Scheduling Disk Space Management	520
36.4.3	Performing Nightly User Upkeep	523

37 Monitoring the POA 525

37.1	Using the POA Server Console	525
37.1.1	Monitoring the POA from the POA Server Console	525
37.1.2	Controlling the POA from the POA Server Console	529
37.2	Using the POA Web Console	539
37.2.1	Setting Up the POA Web Console	540
37.2.2	Accessing the POA Web Console	541
37.2.3	Monitoring the POA from the POA Web Console	542
37.2.4	Controlling the POA from the POA Web Console	549
37.3	Using POA Log Files	551
37.3.1	Locating POA Log Files	551
37.3.2	Configuring POA Log Settings and Switches	552
37.3.3	Viewing POA Log Files	552
37.3.4	Interpreting POA Log File Information	552
37.4	Using GroupWise Monitor	553
37.5	Using Novell Remote Manager	553
37.6	Using an SNMP Management Console	553
37.6.1	Setting Up SNMP Services for the POA	553
37.6.2	Copying and Compiling the POA MIB File	555
37.6.3	Configuring the POA for SNMP Monitoring	556
37.7	Notifying the GroupWise Administrator	557
37.8	Using the POA Error Message Documentation	557

37.9	Employing POA Troubleshooting Techniques	558
37.10	Using Platform-Specific POA Monitoring Tools	558

38 Optimizing the POA 559

38.1	Optimizing Client/Server Processing	559
38.1.1	Adjusting the Number of POA Threads for Client/Server Processing	559
38.1.2	Adjusting the Number of Connections for Client/Server Processing	561
38.1.3	Configuring a Dedicated Client/Server POA (Windows Only)	562
38.2	Optimizing Message File Processing	564
38.2.1	Adjusting the Number of POA Threads for Message File Processing	564
38.2.2	Configuring a Dedicated Message File Processing POA (Windows Only)	565
38.3	Optimizing Thread Management	566
38.4	Optimizing Database Maintenance	567
38.4.1	Adjusting the Number of POA Threads for Database Maintenance	567
38.4.2	Configuring a Dedicated Database Maintenance POA (Windows Only)	568
38.5	Optimizing Client Purge Operations	570
38.6	Optimizing Calendar Publishing	571

39 Managing Indexing of Attachment Content 573

39.1	Regulating Indexing	573
39.2	Configuring the Document Converter Agent (DCA)	575
39.3	Enabling the Document Viewer Agent (DVA) for Indexing	576
39.4	Controlling Maximum Document Conversion Size and Time	577
39.5	Configuring a Dedicated Indexing POA (Windows Only)	577
39.6	Customizing Indexing	579
39.6.1	Determining What to Index	579
39.6.2	Determining Indexing Priority	580
39.6.3	Reclaiming Disk Space	580

40 Using POA Startup Switches 581

40.1	@file_name	585
40.2	--attemptsresetinterval	585
40.3	--certfile	585
40.4	--cluster	586
40.5	--dcamaxsize	586
40.6	--dcamaxtime	586
40.7	--dvanipaddr	587
40.8	--dvanport	587
40.9	--dvanssl	587
40.10	--enforceclientversion	588
40.11	--evocontrol	588
40.12	--externalclientssl	588
40.13	--gwchkthreads	589
40.14	--gwclientreleasedate	589
40.15	--gwclientreleaseversion	589
40.16	--help	589
40.17	--home	590
40.18	--httppassword	590
40.19	--httpport	590
40.20	--httprefresh	591
40.21	--httpssl	591
40.22	--httpuser	591

40.23	--imap	591
40.24	--imapmaxthreads	592
40.25	--imapreadlimit	592
40.26	--imapreadnew	592
40.27	--imapport	593
40.28	--imapssl	593
40.29	--imapsslport	593
40.30	--incorrectloginattempts	593
40.31	--internalclientsssl	594
40.32	--intruderlockout	594
40.33	--ip	594
40.34	--keyfile	595
40.35	--keypassword	595
40.36	--language	595
40.37	--ldapdisablepwdchg	596
40.38	--ldapipaddr	596
40.39	--ldappooln	596
40.40	--ldappoolresettime	597
40.41	--ldapport	597
40.42	--ldapportpooln	597
40.43	--ldappwd	597
40.44	--ldapssl	598
40.45	--ldapsslpooln	598
40.46	--ldapsslkey	598
40.47	--ldapsslkeypooln	599
40.48	--ldaptimeout	599
40.49	--ldapuser	599
40.50	--ldapuserauthmethod	600
40.51	--lockoutresetinterval	600
40.52	--log	600
40.53	--logdays	601
40.54	--logdiskoff	601
40.55	--loglevel	601
40.56	--logmax	602
40.57	--maxappconns	602
40.58	--maxphysconns	602
40.59	--mtpinipaddr	603
40.60	--mtpinport	603
40.61	--mtpoutipaddr	603
40.62	--mtpoutport	604
40.63	--mtpsendmax	604
40.64	--mtpssl	604
40.65	--name	604
40.66	--noada	605
40.67	--nocache	605
40.68	--noconfig	605
40.69	--nodca	606
40.70	--noerrormail	606
40.71	--nogwchk	606
40.72	--nomf	606
40.73	--nomfhigh	607
40.74	--nomflow	607
40.75	--nomtp	607

40.76 --nonuu	607
40.77 --noqf	608
40.78 --nordab	608
40.79 --norecover	608
40.80 --nosnmp	608
40.81 --notcpip	609
40.82 --nuuoffset	609
40.83 --password	609
40.84 --port	609
40.85 --primingmax	610
40.86 --qfbaseoffset	610
40.87 --qfbaseoffsetinminute	610
40.88 --qfdeleteold	611
40.89 --qfinterval	611
40.90 --qfintervalinminute	611
40.91 --qflevel	611
40.92 --qfnolib	612
40.93 --qfnopreproc	612
40.94 --qfnusers	613
40.95 --qfuserfidbeg	613
40.96 --qfuserfidend	613
40.97 --rdaboffset	614
40.98 --rights	614
40.99 --show	614
40.100--soap	615
40.101--soapmaxthreads	615
40.102--soapport	615
40.103--soapsizelimit	615
40.104--soapssl	616
40.105--soapthreads	616
40.106--tcpthreads	616
40.107--threads	617
40.108--usedva	617
40.109--user	617

Part X Message Transfer Agent 619

41 Understanding Message Transfer between Domains and Post Offices 621

41.1 Domain Representation in ConsoleOne	621
41.2 Domain Directory Structure	622
41.3 Information Stored in the Domain	622
41.3.1 Domain Database	622
41.3.2 Agent Input/Output Queues in the Domain	623
41.3.3 Gateways	623
41.4 Role of the Message Transfer Agent	624
41.5 Link Configuration between Domains and Post Offices	624
41.6 Message Flow between Domains and Post Offices	624
41.6.1 Message Flow between Post Offices in the Same Domain	625
41.6.2 Message Flow between Different Domains	625

42 Configuring the MTA 627

42.1 Performing Basic MTA Configuration	627
---	-----

42.1.1	Creating an MTA Object in eDirectory	628
42.1.2	Configuring the MTA in ConsoleOne	629
42.1.3	Changing the Link Protocol between Domains	632
42.1.4	Changing the Link Protocol between a Domain and Its Post Offices	636
42.1.5	Binding the MTA to a Specific IP Address	639
42.1.6	Moving the MTA to a Different Server	640
42.1.7	Adjusting the MTA for a New Location of a Domain or Post Office	640
42.1.8	Adjusting the MTA Logging Level and Other Log Settings	641
42.2	Configuring User Access through the Domain	642
42.2.1	Restricting Message Size between Domains	642
42.2.2	Securing the Domain with SSL Connections to the MTA	643
42.2.3	Enabling Exchange Address Book Synchronization	645
42.3	Configuring Specialized Routing	645
42.3.1	Using Routing Domains	645
42.3.2	Scheduling Direct Domain Links	647
42.3.3	Using a Transfer Pull Configuration (Windows Only)	650
42.4	Configuring Domain Maintenance	652
42.4.1	Using eDirectory User Synchronization	652
42.4.2	Enabling MTA Message Logging	657

43 Monitoring the MTA 659

43.1	Using the MTA Server Console	659
43.1.1	Monitoring the MTA from the MTA Server Console	659
43.1.2	Controlling the MTA from the MTA Server Console	662
43.2	Using the MTA Web Console	669
43.2.1	Setting Up the MTA Web Console	669
43.2.2	Accessing the MTA Web Console	671
43.2.3	Monitoring the MTA from the MTA Web Console	672
43.2.4	Controlling the MTA from the MTA Web Console	675
43.3	Using MTA Log Files	677
43.3.1	Locating MTA Log Files	677
43.3.2	Configuring MTA Log Settings and Switches	677
43.3.3	Viewing MTA Log Files	678
43.3.4	Interpreting MTA Log File Information	678
43.4	Using GroupWise Monitor	678
43.5	Using Novell Remote Manager	679
43.6	Using an SNMP Management Console	679
43.6.1	Setting Up SNMP Services for the MTA	679
43.6.2	Copying and Compiling the MTA MIB File	681
43.6.3	Configuring the MTA for SNMP Monitoring	682
43.7	Notifying the Domain Administrator	682
43.8	Using the MTA Error Message Documentation	683
43.9	Employing MTA Troubleshooting Techniques	683
43.10	Using Platform-Specific MTA Monitoring Tools	683
43.11	Using MTA Message Logging	683

44 Optimizing the MTA 685

44.1	Optimizing TCP/IP Links	685
44.1.1	Adjusting the Number of MTA TCP/IP Connections	685
44.1.2	Adjusting the MTA Wait Intervals for Slow TCP/IP Connections	686
44.2	Optimizing Mapped/UNC Links	686
44.2.1	Using TCP/IP Links between Locations	686
44.2.2	Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways	686
44.2.3	Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices	688
44.3	Optimizing the Routing Queue	689

44.3.1	Adjusting the Maximum Number of Active Router Threads	690
44.3.2	Adjusting the Maximum Number of Idle Router Threads	690
44.4	Adjusting MTA Polling of Closed Locations	690

45 Using MTA Startup Switches 693

45.1	@file_name	695
45.2	--activelog	695
45.3	--certfile	695
45.4	--cluster	696
45.5	--cyhi	696
45.6	--cylo	696
45.7	--defaultroutingdomain	697
45.8	--fast0	697
45.9	--fast4	697
45.10	--help	697
45.11	--home	698
45.12	--httppassword	698
45.13	--httpport	698
45.14	--httprefresh	699
45.15	--httpssl	699
45.16	--httpuser	699
45.17	--ip	700
45.18	--keyfile	700
45.19	--keypassword	700
45.20	--language	701
45.21	--log	701
45.22	--logdays	702
45.23	--logdiskoff	702
45.24	--loglevel	702
45.25	--logmax	703
45.26	--maxidlerouters	703
45.27	--maxrouters	703
45.28	--messagelogdays	703
45.29	--messagelogmaxsize	704
45.30	--messagelogpath	704
45.31	--messagelogsettings	704
45.32	--msgtranssl	705
45.33	--noada	705
45.34	--nodns	705
45.35	--noerrormail	705
45.36	--nondssync	706
45.37	--norecover	706
45.38	--nosnmp	706
45.39	--show	706
45.40	--tcpinbound	707
45.41	--tcpport	707
45.42	--tcpwaitconnect	707
45.43	--tcpwaitdata	707
45.44	--vsnoadm	708
45.45	--work	708

Part XI Document Viewer Agent	709
46 Understanding Document Conversion	711
47 Scaling Your DVA Installation	713
47.1 DVA Configurations	713
47.1.1 Basic DVA Installation	713
47.1.2 Multiple DVAs for WebAccess	714
47.1.3 Multiple DVAs for a Post Office	714
47.1.4 Multiple Shared DVAs	715
47.2 DVA Installation on Additional Servers	715
47.2.1 Linux: Installing Additional DVAs	715
47.2.2 Windows: Installing Additional DVAs	716
48 Configuring the DVA	719
48.1 Editing the gwdva.dva File	719
48.2 Performing Basic DVA Configuration	719
48.2.1 Setting the DVA Home Directory	719
48.2.2 Changing the DVA IP Address or Port Number	720
48.2.3 Securing Document Conversion with SSL Connections	721
48.3 Enabling the DVA Document Quarantine	722
48.4 Putting DVA Configuration Changes into Effect	722
48.4.1 Linux: Stopping and Starting the DVA	722
48.4.2 Windows: Stopping and Starting the DVA	723
49 Monitoring the DVA	725
49.1 Using the DVA Server Console (Windows Only)	725
49.2 Using the DVA Web Console	725
49.2.1 Configuring the DVA Web Console	726
49.2.2 Viewing the DVA Web Console	726
49.3 Using DVA Log Files	727
49.3.1 Locating DVA Log Files	727
49.3.2 Configuring DVA Log Settings	727
49.3.3 Viewing DVA Log Files	728
49.3.4 Interpreting DVA Log File Information	728
50 Optimizing the DVA	729
50.1 Controlling Thread Usage	729
50.2 Controlling Maximum Document Conversion Size and Time Limits	730
51 Using Document Viewer Agent Startup Switches	731
51.1 --home	732
51.2 --httpmaxthread	732
51.3 --httpport	733
51.4 --httppassword	733
51.5 --https	733
51.6 --httpthread	734
51.7 --httpuser	734
51.8 --ip	734
51.9 --lang	735

51.10	--log	735
51.11	--logdays	735
51.12	--loglevel	736
51.13	--logmax	736
51.14	--maxquarantineage	736
51.15	--maxquarantinesize	737
51.16	--maxsize	737
51.17	--maxtime	737
51.18	--quarantine	738
51.19	--sslcert	738
51.20	--sslkey	738
51.21	--sslkeypassword	739
51.22	--temp	739
51.23	--template	739

Part XII Internet Agent 741

52 Configuring Internet Addressing 743

52.1	Planning Internet Addressing	743
52.1.1	GWIA Requirement	744
52.1.2	GWIA's Used for Outbound Messages	744
52.1.3	Internet Domain Names	744
52.1.4	Preferred Address Format	744
52.1.5	Allowed Address Formats	747
52.1.6	Override Options	748
52.2	Setting Up Internet Addressing	748
52.2.1	Installing the GWIA	748
52.2.2	Enabling Internet Addressing	748
52.2.3	Overriding Internet Addressing Defaults	751
52.3	Transitioning from SMTP Gateway Aliases to Internet Addressing	754
52.3.1	Planning to Migrate Gateway Aliases	754
52.3.2	Preparing to Migrate Gateway Aliases	754
52.3.3	Performing the Gateway Alias Migration	754
52.3.4	Verifying the Gateway Alias Migration	756

53 Configuring Internet Services 757

53.1	Configuring SMTP/MIME Services	757
53.1.1	Configuring Basic SMTP/MIME Settings	757
53.1.2	Using Extended SMTP (ESMTP) Options	760
53.1.3	Configuring How the GWIA Handles Email Addresses	761
53.1.4	Determining Format Options for Messages	763
53.1.5	Configuring the SMTP Timeout Settings	765
53.1.6	Determining What to Do with Undeliverable Messages	766
53.1.7	Configuring SMTP Dial-Up Services	767
53.1.8	Enabling SMTP Relaying	770
53.1.9	Using a Route Configuration File	772
53.1.10	Customizing Delivery Status Notifications	773
53.1.11	Managing MIME Messages	773
53.2	Configuring POP3/IMAP4 Services	777
53.2.1	Enabling POP3/IMAP4 Services	778
53.2.2	Configuring Post Office Links	779
53.2.3	Giving POP3 or IMAP4 Access Rights to Users	781
53.2.4	Setting Up an Email Client for POP3/IMAP4 Services	781
53.3	Configuring LDAP Services	782

53.3.1	Enabling LDAP Services	783
53.3.2	Configuring Public Access	784
53.4	Configuring Paging Services	785
53.4.1	Setting Up Paging	785
53.4.2	Using Paging	786
54	Managing Internet Access	787
54.1	Controlling User Access to the Internet	787
54.1.1	Classes of Service	787
54.1.2	Creating a Class of Service	788
54.1.3	Testing Access Control Settings	794
54.1.4	Maintaining the Access Control Database	796
54.2	Blocking Unwanted Email from the Internet	798
54.2.1	Real-Time Blacklists	798
54.2.2	Access Control Lists	800
54.2.3	Blocked.txt File	800
54.2.4	Mailbomb (Spam) Protection	801
54.2.5	Customized Spam Identification	802
54.2.6	SMTP Host Authentication	803
54.2.7	Unidentified Host Rejection	804
54.3	Tracking Internet Traffic with Accounting Data	805
54.3.1	Selecting an Accountant	805
54.3.2	Enabling Accounting	806
54.3.3	Understanding the Accounting File	807
54.3.4	Generating an Accounting Report	808
55	Configuring the GWIA	809
55.1	Changing the Link Protocol between the GWIA and the MTA	809
55.2	Configuring an Alternate GWIA for a Domain	810
55.3	Binding the GWIA to a Specific IP Address	811
55.4	Securing GWIA Connections with SSL	812
55.4.1	Defining the Certificate File	812
55.4.2	Defining Which Connections Use SSL	813
56	Monitoring the GWIA	817
56.1	Using the GWIA Server Console	817
56.1.1	Description	818
56.1.2	Status	818
56.1.3	Statistics	819
56.1.4	Logging	825
56.1.5	Menu Functions	826
56.2	Using the GWIA Web Console	827
56.2.1	Setting Up the GWIA Web Console	827
56.2.2	Monitoring the GWIA at the Web Console	828
56.3	Using Novell Remote Manager	829
56.4	Using an SNMP Management Console	829
56.4.1	Setting Up SNMP Services for the GWIA	829
56.4.2	Copying and Compiling the GWIA MIB File	831
56.4.3	Configuring the GWIA for SNMP Monitoring	832
56.5	Assigning Operators to Receive Warning and Error Messages	832
56.6	Using GWIA Log Files	833
56.6.1	Locating GWIA Log Files	834
56.6.2	Modifying Log Settings in ConsoleOne	834
56.6.3	Modifying Log Settings through Startup Switches	836
56.6.4	Modifying Log Settings through the GWIA Server Console	836

56.6.5	Viewing Log Files	837
56.7	Using GWIA Error Message Documentation	837
56.8	Employing GWIA Troubleshooting Techniques	837
56.9	Stopping the GWIA	838
56.9.1	Using the GWIA Server Console	838
56.9.2	Using a Command at the Command Line	838
56.9.3	Using a Mail Message	838
56.9.4	Using a Shutdown File	838
57	Optimizing the GWIA	839
57.1	Relocating the GWIA's Processing Directories	839
57.2	Increasing GWIA Speed	840
57.2.1	Sending and Receiving Threads	841
57.2.2	Increasing Polling Time	841
57.2.3	Decreasing the Timeout Cycles	842
58	Connecting GroupWise Systems and Domains Using the GWIA	843
58.1	Connecting GroupWise Systems	843
58.1.1	Overview	843
58.1.2	Creating an External Domain	844
58.1.3	Linking to the External Domain	845
58.1.4	Checking the Link Status of the External Domain	847
58.1.5	Sending Messages Between Systems	848
58.1.6	Exchanging Information Between Systems	848
58.2	Linking Domains	848
59	Using GWIA Startup Switches	851
59.1	How to Use Startup Switches	851
59.1.1	Changing GWIA Settings in ConsoleOne	852
59.1.2	Modifying the gwia.cfg File	852
59.1.3	Editing Guidelines	852
59.2	Alphabetical List of Switches	853
59.3	Required Switches	858
59.3.1	--dhome	858
59.3.2	--hn	859
59.3.3	--home	859
59.4	Console Switches	859
59.4.1	--color	859
59.4.2	--help	859
59.4.3	--mono	860
59.4.4	--show (Linux Only)	860
59.5	Environment Switches	860
59.5.1	--cluster	860
59.5.2	--ip	860
59.5.3	--ipa	861
59.5.4	--ipp	861
59.5.5	--nosnmp	861
59.5.6	--smtphome	861
59.5.7	--work	861
59.5.8	--hasoq	862
59.6	SMTP/MIME Switches	862
59.6.1	SMTP Enabled	862
59.6.2	iCal Enabled	863
59.6.3	Address Handling	863
59.6.4	Message Formatting and Encoding	868

59.6.5	Forwarded and Deferred Messages	871
59.6.6	Extended SMTP	872
59.6.7	Send/Receive Cycle and Threads	873
59.6.8	Dial-Up Connections	874
59.6.9	Timeouts	875
59.6.10	Relay Host	876
59.6.11	Host Authentication	877
59.6.12	Undeliverable Message Handling	878
59.6.13	Mailbomb and Spam Security	878
59.7	POP3 Switches	880
59.7.1	--noproversion	880
59.7.2	--pop3	880
59.7.3	--popintruderdetect	880
59.7.4	--popport	881
59.7.5	--popsport	881
59.7.6	--popssl	881
59.7.7	--pt	881
59.7.8	--sslpt	881
59.8	IMAP4 Switches	882
59.8.1	--imap4	882
59.8.2	--imapport	882
59.8.3	--imapreadlimit	882
59.8.4	--imapreadnew	882
59.8.5	--imapsport	883
59.8.6	--imapssl	883
59.8.7	--it	883
59.8.8	--noimapversion	883
59.8.9	--sslit	883
59.9	HTTP (Web Console) Switches	884
59.9.1	--httpport	884
59.9.2	--httpuser	884
59.9.3	--httppassword	884
59.9.4	--httprefresh	884
59.9.5	--httpssl	885
59.10	SSL Switches	885
59.10.1	--certfile	885
59.10.2	--keyfile	885
59.10.3	--keypasswd	885
59.10.4	--smtpsl	886
59.10.5	--httpssl	886
59.10.6	--popssl	886
59.10.7	--imapssl	886
59.10.8	/ldapssl	887
59.11	LDAP Switches	887
59.11.1	GroupWise Authentication Switches	887
59.11.2	LDAP Query Switches	888
59.12	Log File Switches	890
59.12.1	--log	890
59.12.2	--logdays	890
59.12.3	--loglevel	890
59.12.4	--logmax	891

Part XIII WebAccess 893

60 Accessing Your GroupWise Mailbox in a Web-Based Environment 895

60.1	Using WebAccess on a Desktop Workstation	895
60.2	Using WebAccess on a Tablet Device	896

60.3	Using the WebAccess Basic Interface on a Mobile Device	897
61	Scaling Your GroupWise WebAccess Installation	899
61.1	WebAccess Configurations	899
61.1.1	Basic WebAccess Application Installation	899
61.1.2	Multiple POAs for a WebAccess Application	900
61.1.3	Multiple DVAs for a WebAccess Application	900
61.1.4	Multiple WebAccess Applications and Web Servers for a Large WebAccess Installation	900
61.2	WebAccess Installation on Additional Web Servers	901
62	Configuring the WebAccess Application	903
62.1	Customizing the WebAccess Application	903
62.1.1	Editing the webacc.cfg File	904
62.1.2	Configuring Multiple POAs for the WebAccess Application	904
62.1.3	Configuring Multiple DVAs for the WebAccess Application	905
62.1.4	Adjusting Session Security	905
62.1.5	Accommodating Single Sign-On Products	906
62.1.6	Putting WebAccess Configuration Changes into Effect	906
62.2	Managing User Access	907
62.2.1	Setting the Timeout Interval for Inactive Sessions	907
62.2.2	Customizing Auto-Save Functionality	908
62.2.3	Preventing Users from Changing Their GroupWise Passwords in WebAccess	908
62.2.4	Helping Users Who Forget Their GroupWise Passwords	909
62.2.5	Controlling WebAccess Usage	909
62.3	Customizing User Functionality	911
62.3.1	Customizing the WebAccess User Interface with Your Company Logo	911
62.3.2	Controlling Viewable Attachment Types	912
62.3.3	Controlling Viewable Attachment Size	913
62.3.4	Customizing the Default Calendar View	913
62.3.5	Customizing the Default List Functionality	915
62.3.6	Enabling an LDAP Address Book	916
63	Monitoring the WebAccess Application	917
63.1	Using the WebAccess Application Web Console	917
63.1.1	Enabling the WebAccess Application Web Console	917
63.1.2	Using the WebAccess Application Web Console	917
63.2	Using WebAccess Application Log Files	918
63.2.1	Locating WebAccess Application Log Files	918
63.2.2	Configuring WebAccess Application Log Settings	918
63.2.3	Viewing WebAccess Application Log Files	919
63.2.4	Interpreting WebAccess Application Log File Information	919
Part XIV	Calendar Publishing Host	921
64	Configuring the Calendar Publishing Host	923
64.1	Using the Administration Web Console	923
64.1.1	Logging In to the Administration Web Console	923
64.1.2	Changing Post Office Settings	924
64.1.3	Adjusting Log Settings	924
64.1.4	Configuring LDAP Authentication	926
64.1.5	Customizing the Calendar Publishing Host Logo	927
64.1.6	Logging Out of the Administration Web Console	927

64.2	Using the calhost.cfg File	928
64.2.1	Editing the calhost.cfg File	928
64.2.2	Setting the Published Calendar Auto-Refresh Interval	928
64.2.3	Setting the Default Published Calendar View	929
64.2.4	Configuring an External POA IP Address	929
64.2.5	Changing the SSL Trusted Root Certificate	929
64.2.6	Restarting the Web Server	930
65	Monitoring Calendar Publishing	931
65.1	Viewing Calendar Publishing Status at the POA Web Console	931
65.2	Using Calendar Publishing Host Log Files	932
65.3	Using POA Log Files	932
66	Creating a Corporate Calendar Browse List	933
67	Managing Your Calendar Publishing Host	935
67.1	Adding Multiple Calendar Publishing Hosts	935
67.2	Assigning a Different Calendar Publishing Host to Users	936
67.3	Editing Calendar Publishing Host Configuration	936
67.4	Deleting a Calendar Publishing Host	937
Part XV	Monitor	939
68	Understanding the Monitor Agent Consoles	941
68.1	Monitor Agent Server Console	941
68.2	Monitor Agent Web Console	942
68.3	Monitor Web Console	942
69	Configuring the Monitor Agent	945
69.1	Selecting Agents to Monitor	946
69.1.1	Filtering the Agent List	946
69.1.2	Adding an Individual Agent	947
69.1.3	Adding All Agents on a Server	948
69.1.4	Adding All Agents on a Subnet	948
69.1.5	Removing Added Agents	949
69.2	Creating and Managing Agent Groups	949
69.2.1	Creating an Agent Group	950
69.2.2	Managing Agent Groups	951
69.2.3	Viewing Your Agent Group Hierarchy	951
69.2.4	Configuring an Agent Group	952
69.3	Configuring Monitoring Protocols	952
69.3.1	Configuring the Monitor Agent for HTTP	953
69.3.2	Configuring the Monitor Agent for SNMP	955
69.4	Configuring Polling of Monitored Agents	956
69.5	Configuring Email Notification for Agent Problems	957
69.5.1	Configuring Email Notification	957
69.5.2	Customizing Notification Thresholds	959
69.6	Configuring Audible Notification for Agent Problems	961
69.7	Configuring SNMP Trap Notification for Agent Problems	962
69.8	Configuring Authentication and Intruder Lockout for the Monitor Web Console	964
69.9	Configuring Monitor Agent Log Settings	965

69.10	Configuring Proxy Service Support for the Monitor Web Console	966
69.11	Monitoring Messenger Agents	967
69.12	Supporting the GroupWise High Availability Service on Linux	968

70 Configuring the Monitor Application 969

70.1	Editing the gwmonitor.cfg File	969
70.2	Setting the Timeout Interval for Inactive Sessions	969
70.3	Adjusting Session Security	970
70.4	Accommodating Single Sign-On Products	970
70.5	Configuring Monitor Application Log Settings	971
70.5.1	Locating Monitor Application Log Files	971
70.5.2	Configuring Monitor Application Log Settings	971
70.5.3	Viewing Monitor Application Log Files	971
70.6	Putting the Monitor Configuration Changes into Effect	972
70.6.1	Accepting the Default Time Interval	972
70.6.2	Changing the Default Time Interval	972
70.6.3	Immediately Putting the Configuration Changes into Effect	972

71 Using GroupWise Monitor 973

71.1	Using the Windows Monitor Agent Server Console	973
71.1.1	Viewing All Agents	974
71.1.2	Viewing Problem Agents	975
71.1.3	Viewing a Windows Agent Server Console	975
71.1.4	Viewing an Agent Web Console	976
71.1.5	Polling the Agents for Updated Status Information	977
71.2	Using the Monitor Web Console	977
71.3	Generating Reports	979
71.3.1	Link Trace Report	979
71.3.2	Link Configuration Report	980
71.3.3	Image Map Report	981
71.3.4	Environment Report	986
71.3.5	User Traffic Report	986
71.3.6	Link Traffic Report	987
71.3.7	Message Tracking Report	987
71.3.8	Performance Testing Report	988
71.3.9	Connected User Report	988
71.3.10	Gateway Accounting Report	988
71.3.11	Trends Report	988
71.3.12	Down Time Report	989
71.4	Measuring Agent Performance	989
71.4.1	Setting Up an External Monitor Domain	989
71.4.2	Configuring the Link for the External Monitor Domain	990
71.4.3	Configuring the Monitor Agent for Agent Performance Testing	991
71.4.4	Viewing Agent Performance Data	992
71.4.5	Viewing an Agent Performance Report	992
71.4.6	Receiving Notification of Agent Performance Problems	992
71.5	Collecting Gateway Accounting Data	992
71.5.1	Setting Up an External Monitor Domain	993
71.5.2	Configuring the Link for the External Monitor Domain	993
71.5.3	Configuring the Monitor Agent to Communicate through the External Monitor Domain	994
71.5.4	Setting Up an External Post Office and External User for the Monitor Agent	995
71.5.5	Designating a Gateway Accountant	995
71.5.6	Receiving and Forwarding the Accounting Files	996
71.5.7	Viewing the Gateway Accounting Report	997
71.6	Assigning Responsibility for Specific Agents	998

71.7	Searching for Agents	999
72	Comparing the Monitor Consoles	1001
73	Using Monitor Agent Startup Switches	1003
73.1	--hpassword	1004
73.2	--hapoll	1004
73.3	--hauser	1005
73.4	--help	1005
73.5	--home	1005
73.6	--httpagentpassword	1006
73.7	--httpagentuser	1006
73.8	--httpcertfile	1006
73.9	--httpmonpassword	1007
73.10	--httpmonuser	1007
73.11	--httpport	1007
73.12	--httpssl	1008
73.13	--ipa	1008
73.14	--ipp	1008
73.15	--lang	1009
73.16	--log	1009
73.17	--monwork	1009
73.18	--nmaddress	1010
73.19	--nmhome	1010
73.20	--nmpassword	1010
73.21	--nmuser	1011
73.22	--nosnmp	1011
73.23	--pollthreads	1011
73.24	--proxy	1011
73.25	--tcpwaitconnect	1012
Part XVI	Client	1013
74	Using GroupWise Windows Client Custom Installation Options	1015
75	Setting Up GroupWise Client Modes and Accounts	1017
75.1	GroupWise Client Modes	1017
75.1.1	Online Mode	1017
75.1.2	Caching Mode	1017
75.1.3	Remote Mode	1019
75.2	Email Accounts	1022
75.2.1	Accounts Menu	1022
75.2.2	Enabling POP3, IMAP4, and NNTP Account Access in Online Mode	1022
76	Setting Defaults for the GroupWise Client Options	1025
76.1	Client Options Summary	1025
76.2	Setting Client Options	1030
76.2.1	Modifying Environment Options	1031
76.2.2	Modifying Send Options	1050
76.2.3	Modifying Documents Options	1061

76.2.4	Modifying Security Options	1061
76.2.5	Modifying Calendar Options	1065
76.3	Resetting Client Options to Default Settings	1068
77	Distributing the GroupWise Windows Client	1069
77.1	Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client	1069
77.1.1	Preparing for AutoUpdate	1070
77.1.2	Working with the Setup Configuration File	1076
77.1.3	Enabling AutoUpdate in ConsoleOne	1082
77.1.4	Understanding the User's AutoUpdate Experience	1083
77.1.5	Using the AutoUpdate Error Log Files	1084
77.1.6	Disabling Your AutoUpdate Customizations	1084
77.2	Using ZENworks Configuration Management to Distribute the GroupWise Windows Client	1085
78	Supporting the GroupWise Client in Multiple Languages	1087
78.1	Providing the GroupWise Client Software in Multiple Languages	1087
78.2	Providing Post Office Support for Multiple Languages	1087
79	Tools for Analyzing and Correcting GroupWise Client Problems	1089
79.1	GroupWise Exception Handler for the Windows Client	1089
79.2	GroupWise Check	1089
79.2.1	Enabling GroupWise Check in the Windows Client	1090
80	Startup Options for the GroupWise Windows Client	1091
80.1	/@u-?	1091
80.2	/@u-user_ID	1092
80.3	/bl	1092
80.4	/c	1092
80.5	/cm	1092
80.6	/iabs	1092
80.7	/ipa-IP_address_or_hostname	1092
80.8	/ipp-port_number	1093
80.9	/l-xx	1093
80.10	/la-network_ID	1093
80.11	/nu	1093
80.12	/ph-path_name	1093
80.13	/pc-path_to_caching_mailbox	1093
80.14	/pr-path_to_remote_mailbox	1094
Part XVII	Security Administration	1095
81	Native GroupWise Security	1097
82	GroupWise Passwords	1099
82.1	Mailbox Passwords	1099
82.1.1	Using Post Office Security Instead of GroupWise Passwords	1099
82.1.2	Requiring GroupWise Passwords	1100
82.1.3	Managing GroupWise Passwords	1100
82.1.4	Using LDAP Passwords Instead of GroupWise Passwords	1102
82.1.5	Bypassing Mailbox Passwords to Respond to Corporate Mandates	1103

82.2	Agent Passwords	1103
82.2.1	Facilitating Access to Remote Servers	1103
82.2.2	Facilitating Access to eDirectory	1103
82.2.3	Protecting the Agent Web Consoles	1104
82.2.4	Protecting the GroupWise Monitor Web Console	1104
83 Encryption and Certificates		1105
83.1	Personal Digital Certificates, Digital Signatures, and S/MIME Encryption	1105
83.2	Server Certificates and SSL Encryption	1107
83.2.1	Purchasing a Commercially Generated Certificate	1107
83.2.2	Generating a Self-Signed Certificate	1111
83.2.3	Installing the Certificate on the Server	1114
83.2.4	Configuring the Agents to Use SSL	1115
83.3	Trusted Root Certificates and LDAP Authentication	1115
84 LDAP Directories		1119
84.1	Accessing Public LDAP Directories from GroupWise	1119
84.2	Offering the GroupWise Address Book as an LDAP Directory.	1119
84.3	Authenticating to GroupWise with Passwords Stored in an LDAP Directory	1120
84.3.1	Access Method	1120
84.3.2	LDAP User Name	1120
84.4	Accessing S/MIME Certificates in an LDAP Directory	1121
85 Message Security		1123
86 Address Book Security		1125
86.1	eDirectory Information Displayed in the Address Book	1125
86.2	Suppressing the Contents of the User Description Field	1125
86.3	Controlling GroupWise Object Visibility in the Address Book.	1126
86.4	Controlling GroupWise Object Visibility between GroupWise Systems	1126
87 GroupWise Administrator Rights		1127
87.1	Setting Up a GroupWise Administrator as an Admin Equivalent	1127
87.2	Assigning Rights Based on Administration Responsibilities.	1127
87.2.1	File System Rights	1128
87.2.2	eDirectory Rights	1128
87.2.3	Common Types of GroupWise Administrators	1132
87.3	eDirectory Object and Properties Rights	1135
87.4	Granting or Removing Object and Property Rights	1138
88 GroupWise Agent Rights		1139
89 GroupWise User Rights		1141
89.1	eDirectory Rights	1141
89.1.1	Configuring ConsoleOne to Automatically Set eDirectory Rights When Creating User Accounts	1141
89.1.2	Manually Granting eDirectory Rights	1142
89.2	File System Rights	1143
89.2.1	Granting File System Rights to the Software Distribution Directory.	1143
89.2.2	Granting File System Rights to the Mailbox Backup Directory	1144

90 Spam Protection	1145
90.1 Configuring the GWIA for Spam Protection	1145
90.2 Configuring the GroupWise Client for Spam Protection	1145
91 Virus Protection	1147
Part XVIII Security Policies	1149
92 Securing GroupWise Data	1151
92.1 Limiting Physical Access to GroupWise Servers	1151
92.2 Securing File System Access	1151
92.3 Securing Domains and Post Offices	1151
93 Securing GroupWise Agents	1153
93.1 Setting Up SSL Connections	1153
93.2 Protecting Agent Web Consoles	1153
93.3 Protecting Agent Startup and Configuration Files	1153
93.4 Protecting Agent and Application Log Files	1154
93.5 Protecting Agent Processes on Linux	1154
93.6 Protecting Trusted Applications	1154
94 Securing GroupWise System Access	1155
94.1 Using a Proxy Server with Client/Server Access	1155
94.2 Using LDAP Authentication for GroupWise Users	1155
94.3 Managing Mailbox Passwords	1155
94.4 Enabling Intruder Detection	1156
95 Secure Migrations	1157
95.1 GroupWise Server Migration Utility	1157
95.1.1 Source Server Credentials	1157
95.1.2 Destination Server root Password	1157
95.1.3 Agent Startup Files	1158
96 Undocumented Diagnostic Tools	1159
Part XIX Appendixes	1161
A GroupWise Port Numbers	1163
A.1 Opening Ports for GroupWise Agents and Applications	1163
A.1.1 Opening Ports on OES Linux	1163
A.1.2 Opening Ports on SLES	1164
A.1.3 Opening Ports on Windows	1165
A.2 Protocol Flow Diagram with Port Numbers	1166
A.3 Post Office Agent Port Numbers	1167
A.4 Message Transfer Agent Port Numbers	1169
A.5 Document Viewer Agent Port Numbers	1170
A.6 Internet Agent Port Numbers	1170
A.7 WebAccess Application Port Numbers	1172

A.8	Calendar Publishing Host Port Numbers	1172
A.9	Monitor Agent Port Number	1173
A.10	Monitor Application Port Numbers	1173
A.11	GroupWise High Availability Service Port Number (Linux Only)	1173
A.12	Port Numbers for Products Frequently Used with GroupWise	1174
A.12.1	Novell Messenger Port Number	1174
A.12.2	Novell Data Synchronizer Port Numbers	1174
A.12.3	BlackBerry Enterprise Server for Novell GroupWise Port Number	1175
B	GroupWise URLs	1177
C	Linux Commands, Directories, and Files for GroupWise Administration	1179
C.1	Linux Operating System Commands	1179
C.1.1	Basic Commands	1179
C.1.2	File and Directory Commands	1180
C.1.3	Process Commands	1180
C.1.4	Disk Usage Commands	1181
C.1.5	Package Commands	1181
C.1.6	File System Commands	1181
C.1.7	Network Commands	1182
C.1.8	Linux Core File	1182
C.2	GroupWise Directories and Files on Linux	1183
C.2.1	Component Installation Directories on Linux	1183
C.2.2	Linux Agent Software Subdirectories	1183
C.2.3	Linux Agent Startup and Configuration Files	1183
C.3	Linux GroupWise Commands	1184
D	Documentation Updates	1185
D.1	April 16, 2013 (GroupWise 2012 SP2)	1185
D.2	September 20, 2012 (GroupWise 2012 SP1)	1187
D.3	August 18, 2014 (GroupWise 2012 SP3)	1189

About This Guide

This Novell *GroupWise 2012 Administration Guide* helps you maintain all components of your GroupWise system. The guide is divided into the following sections:

- ♦ Part I, “System,” on page 35
- ♦ Part II, “Domains,” on page 129
- ♦ Part III, “Post Offices,” on page 171
- ♦ Part IV, “Users,” on page 217
- ♦ Part V, “Resources,” on page 263
- ♦ Part VI, “Distribution Lists, Groups, and Organizational Roles,” on page 279
- ♦ Part VII, “Libraries and Documents,” on page 313
- ♦ Part VIII, “Databases,” on page 395
- ♦ Part IX, “Post Office Agent,” on page 469
- ♦ Part X, “Message Transfer Agent,” on page 619
- ♦ Part XI, “Document Viewer Agent,” on page 709
- ♦ Part XII, “Internet Agent,” on page 741
- ♦ Part XIII, “WebAccess,” on page 893
- ♦ Part XIV, “Calendar Publishing Host,” on page 921
- ♦ Part XV, “Monitor,” on page 939
- ♦ Part XVI, “Client,” on page 1013
- ♦ Part XVII, “Security Administration,” on page 1095
- ♦ Part XVIII, “Security Policies,” on page 1149
- ♦ Part XIX, “Appendixes,” on page 1161

For troubleshooting assistance, see:

- ♦ *GroupWise 2012 Troubleshooting 1: Error Messages*
- ♦ *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*
- ♦ *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*
- ♦ Novell Support and Knowledgebase (<http://www.novell.com/support>)

To search the GroupWise documentation from the Novell Support Web site, click *Advanced Search*, select *Documentation* in the *Search In* drop-down list, select *GroupWise* in the *Products* drop-down list, type the search string, then click *Search*.

- ♦ GroupWise Support Forums (<http://forums.novell.com/forumdisplay.php?&f=356>)
- ♦ GroupWise Support Community (<http://www.novell.com/support/products/groupwise>)
- ♦ GroupWise Cool Solutions (<http://www.novell.com/cool solutions/gwmag/index.html>)

Audience

This guide is intended for those who administer a GroupWise system on Linux or Windows. Some background knowledge of the host operating system is assumed.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation.

Additional Documentation

For additional GroupWise documentation, see the following guides at the [Novell GroupWise 2012 documentation Web site \(http://www.novell.com/documentation/beta/groupwise2012\)](http://www.novell.com/documentation/beta/groupwise2012):

- ◆ *Installation Guide*
- ◆ *Server Migration Guide*
- ◆ *Administration Guide*
- ◆ *Multi-System Administration Guide*
- ◆ *Interoperability Guide*
- ◆ *Troubleshooting Guides*
- ◆ *GroupWise User Frequently Asked Questions (FAQ)*
- ◆ *GroupWise User Guides*
- ◆ *GroupWise User Quick Starts*

System

- ♦ Chapter 1, “GroupWise System Administration,” on page 37
- ♦ Chapter 2, “ConsoleOne Administration Tool,” on page 39
- ♦ Chapter 3, “GroupWise View,” on page 61
- ♦ Chapter 4, “GroupWise System Operations,” on page 69
- ♦ Chapter 5, “GroupWise Utilities,” on page 95
- ♦ Chapter 6, “GroupWise Address Book,” on page 105
- ♦ Chapter 7, “Multilingual GroupWise Systems,” on page 123

For additional assistance in managing your GroupWise system, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

1 GroupWise System Administration

As a GroupWise system administrator, it is your responsibility to keep your GroupWise system running smoothly for your GroupWise users. This *GroupWise 2012 Administration Guide* provides a wealth of information to help you accomplish this task. This System section provides an overview of the GroupWise administration tool, ConsoleOne, and its capabilities. It summarizes administrative tasks that affect your GroupWise system as a whole and provides links to more specialized instructions.

The following sections of the *Administration Guide* detail the eDirectory objects where GroupWise information is stored. Instructions are provided for creating and managing all GroupWise object types.

- ♦ [“Domains” on page 129](#)
- ♦ [“Post Offices” on page 171](#)
- ♦ [“Users” on page 217](#)
- ♦ [“Resources” on page 263](#)
- ♦ [“Distribution Lists, Groups, and Organizational Roles” on page 279](#)

The following sections of the *Administration Guide* detail the GroupWise software components that make your GroupWise system run. Instructions are provided for configuring, monitoring, and optimizing each software component.

- ♦ [“Post Office Agent” on page 469](#)
- ♦ [“Message Transfer Agent” on page 619](#)
- ♦ [“Document Viewer Agent” on page 709](#)
- ♦ [“Internet Agent” on page 741](#)
- ♦ [“WebAccess” on page 893](#)
- ♦ [“Monitor” on page 939](#)
- ♦ [“Calendar Publishing Host” on page 921](#)

The following additional sections of the *Administration Guide* provide supporting details and background information:

- ♦ [“Libraries and Documents” on page 313](#)
- ♦ [“Databases” on page 395](#)
- ♦ [“Client” on page 1013](#)
- ♦ [“Security Administration” on page 1095](#)
- ♦ [“Security Policies” on page 1149](#)

2 ConsoleOne Administration Tool

GroupWise is administered using ConsoleOne, a Java-based tool for managing your network and its resources. When you create your GroupWise system, GroupWise snap-ins are added to your ConsoleOne installation and GroupWise objects are created in Novell eDirectory. As you manage your GroupWise system, you use ConsoleOne to create additional GroupWise objects, modify GroupWise object properties, and so on.

IMPORTANT: Because the GroupWise snap-ins to ConsoleOne are required in order to work with GroupWise objects, you cannot use other network management tools, such as Novell iManager, to administer your GroupWise system. Also, you should not use older network management tools, such as NetWare Administrator, to administer your GroupWise system, unless your GroupWise system includes legacy gateways that require such tools to administer the corresponding Gateway objects and their properties.

Because GroupWise is a cross-platform product, you might have components of your GroupWise system located on Linux servers, Windows servers, and legacy NetWare servers. You can run ConsoleOne on Linux or Windows to manage GroupWise domains and post offices located on any of these platforms.

- ♦ [Section 2.1, “ConsoleOne on Linux,” on page 39](#)
- ♦ [Section 2.2, “ConsoleOne on Windows,” on page 46](#)
- ♦ [Section 2.3, “ConsoleOne in a Multiple-Platform Environment,” on page 48](#)
- ♦ [Section 2.4, “Remote Access to ConsoleOne on a Linux Server,” on page 56](#)

NOTE: Starting in GroupWise 2012, NetWare is not a supported platform for the GroupWise agents. However, the GroupWise Windows agents can be used to access domains and post offices located on NetWare servers. ConsoleOne can still administer GroupWise databases located on NetWare servers.

2.1 ConsoleOne on Linux

- ♦ [Section 2.1.1, “Installing Linux ConsoleOne,” on page 40](#)
- ♦ [Section 2.1.2, “Installing the GroupWise Administrator Snap-Ins to Linux ConsoleOne,” on page 40](#)
- ♦ [Section 2.1.3, “Enabling File Locking on OES Linux,” on page 41](#)
- ♦ [Section 2.1.4, “Starting Linux ConsoleOne,” on page 41](#)
- ♦ [Section 2.1.5, “Mounting a Linux File System for a Domain or a Post Office,” on page 42](#)
- ♦ [Section 2.1.6, “Changing the Linux Mount Directory,” on page 46](#)

2.1.1 Installing Linux ConsoleOne

You can install Linux ConsoleOne on any server that meets the system requirements listed in “[GroupWise Administration Requirements](#)” in “[GroupWise Product Overview](#)” in the *GroupWise 2012 Installation Guide*.

You must install the version of Linux ConsoleOne that is included in the downloaded *GroupWise 2012* software image in the `consoleone/Linux` subdirectory. Under some circumstances, an older version of ConsoleOne might already be installed.

- 1 In a terminal window, become `root` by entering `su -` and the `root` password.
- 2 Make the downloaded *GroupWise 2012* software image available on the Linux server where you want to install ConsoleOne.
- 3 Install the IBM JRE that is required for use with ConsoleOne:
 - 3a Change to the `admin` subdirectory of the software image.
 - 3b Install IBM JRE 1.5:

```
rpm -i NOVLc1Linuxjre-1.5.0-11.i586.rpm
```

- 4 Change to the `consoleone/Linux` subdirectory of the software image.
- 5 Check to see if an older version of ConsoleOne is already installed on the Linux server:

```
ls /usr/ConsoleOne
```

- 6 (Conditional) If the `ConsoleOne` directory exists, uninstall ConsoleOne:

```
./c1-uninstall
```

- 7 Install the *GroupWise 2012* version of ConsoleOne:

```
./c1-install
```

- 8 Enter the numbers for the languages that you want to install.
- 9 Enter 3 to install the LDAP snap-in.
- 10 Decline the installation of the bundled JRE 1.4.2, which is incompatible with the JRE installed in [Step 3](#) above.
ConsoleOne, along with other supporting packages, is then installed to `/usr/ConsoleOne`.
- 11 Continue with [Installing the GroupWise Administrator Snap-Ins to Linux ConsoleOne](#).

2.1.2 Installing the GroupWise Administrator Snap-Ins to Linux ConsoleOne

After Linux ConsoleOne is installed, use the GroupWise Installation program to install the GroupWise Administrator snap-ins to ConsoleOne to the ConsoleOne installation on that server.

- 1 Mount the primary domain directory of your GroupWise system to the server where you are installing the GroupWise Administrator snap-ins to ConsoleOne.

If you need assistance with this task, see [Section 2.1.5, “Mounting a Linux File System for a Domain or a Post Office,” on page 42](#)

- 2 Change to the root of the *GroupWise 2012* software image.
- 3 Start the GroupWise Installation program:

```
./install
```

- 4 Select the language in which you want to run the GroupWise Installation program, then click *OK*.

- 5 Click *Install Products > GroupWise Administration*.
- 6 Click *Install Administration*, then click *OK* when installation is complete.
- 7 Click *Configure Administration*.
- 8 Review the introduction, then click *Next*.
- 9 Accept the License Agreement, then click *Next*.
- 10 Click *Next* to accept the default software distribution directory:

```
/opt/novell/groupwise/software
```

- 11 Select *GroupWise Administration*, then click *Next*.
- 12 When the software has been copied to the software distribution directory, click *Next*.
- 13 Click *Next* to accept the default of *Updating an existing GroupWise system*.
- 14 Browse to and select the primary domain directory for your GroupWise system, then click *Update*.
- 15 Exit the GroupWise Administration program.

For convenience, ConsoleOne and the GroupWise Administrator snap-ins should be installed on each Linux server where a domain is located. For some administration tasks, ConsoleOne on the local server needs to have remote servers mounted. For more information, see [Section 2.1.5, "Mounting a Linux File System for a Domain or a Post Office,"](#) on page 42.

- 16 (Conditional) If you installed ConsoleOne on Open Enterprise Server (OES) Linux, continue with [Enabling File Locking on OES Linux](#)

or

(Conditional) If you installed ConsoleOne on SUSE Linux Enterprise Server (SLES), skip to [Section 2.1.4, "Starting Linux ConsoleOne,"](#) on page 41

2.1.3 Enabling File Locking on OES Linux

(Conditional) If you have installed ConsoleOne on OES Linux:

- 1 As root, edit the following file:


```
/etc/opt/novell/ncpserv.conf
```
- 2 Add the following line at the bottom of the file:


```
CROSS_PROTOCOL_LOCKS 1
```
- 3 Restart the Novell eDirectory daemon:


```
rcnstd restart
```
- 4 Continue with [Starting Linux ConsoleOne](#).

2.1.4 Starting Linux ConsoleOne

- 1 Make sure that any domain directories and post office directories that you want to access from ConsoleOne are mounted to your local Linux server.

If you need assistance with this task, see [Section 2.1.5, "Mounting a Linux File System for a Domain or a Post Office,"](#) on page 42

- 2 As root, enter the following command:

```
/usr/ConsoleOne/bin/ConsoleOne
```

IMPORTANT: Do not start ConsoleOne using the desktop icon. You cannot access the properties of GroupWise objects in eDirectory if you start ConsoleOne from the Linux desktop.

2.1.5 Mounting a Linux File System for a Domain or a Post Office

To administer a domain that is located on a remote Linux server, you must mount the domain directory to the local Linux server. To administer a post office that is located on a remote Linux server, the domain directory for the owning domain and the post office directory must both be mounted to the local Linux server. In addition, you might also want to mount the primary domain server to each secondary domain server, so that administrative messages can flow from one secondary domain to another through the primary domain.

- ♦ [“Working with the Linux Mount Directory” on page 42](#)
- ♦ [“Mounting an OES Linux File System Using NetWare Core Protocol \(NCP\)” on page 42](#)
- ♦ [“Mounting a SLES File System Using Samba” on page 43](#)

Working with the Linux Mount Directory

The first time you run Linux ConsoleOne on a server, you are prompted to provide a Linux mount directory on that server. The default location is `/mnt`. For more information, see [“Linux Mount Directory”](#) in [“Planning a Basic GroupWise System”](#) in the *GroupWise 2012 Installation Guide*. For convenience, you can later change the Linux mount directory, as described in [Section 2.1.6, “Changing the Linux Mount Directory,” on page 46](#).

Underneath the Linux mount directory, you must create a subdirectory for each file system where a domain or post office resides on a remote Linux server, that you want to be able to access from Linux ConsoleOne on the local Linux server. For example, if you have a domain directory named `prov01` on a remote Linux server, you would create a `prov01` subdirectory under `/mnt` on the local Linux server where you want to run ConsoleOne.

Mounting an OES Linux File System Using NetWare Core Protocol (NCP)

- ♦ [“Configuring NCP” on page 42](#)
- ♦ [“Mounting an NCP Volume” on page 43](#)

Configuring NCP

- 1 In a terminal window on the OES Linux server, become root by entering `su -` and the root password.
- 2 If you are creating a new domain or post office, create the directory where you want to create the GroupWise domain and/or post office.

or

If you are not creating a new domain or post office, make sure you know where the existing directory is located.

- 3 Enter the following command to create the NCP volume:

```
ncpcon create volume volume_name /directory
```

3a Replace *volume_name* with a unique name for the location where you want to create the GroupWise domain and/or post office.

3b Replace *directory* with the directory referenced in [Step 2](#).

- 4 Verify that the volume has been created:

```
more /etc/opt/novell/ncpserv.conf
```

The new volume should be listed at the end of the NCP server configuration file.

- 5 Restart the Novell eDirectory daemon:

```
rcnstd restart
```

- 6 Continue with [Mounting an NCP Volume](#).

Mounting an NCP Volume

- 1 Use the following command to mount the NCP volume to the OES Linux server:

```
ncpmount -S fully_qualified_hostname -V volume_name -A ip_address  
-U fully_qualified_administrator_user /linux_mount_directory
```

- 1a Replace *fully_qualified_hostname* with the name of the remote Linux server that you are mounting to the local Linux server, such as `provo1.novell.com`.
 - 1b Replace *volume_name* with the name of the NCP volume that you created in [Step 3](#) in “[Configuring NCP](#)” on page 42.
 - 1c Replace *ip_address* with the IP address of the remote server specified in [Step 1a](#) above.
 - 1d Replace *linux_mount_directory* with the full path for the directory that you created in “[Working with the Linux Mount Directory](#)” on page 42.
- 2 Create a script in the `/mnt` directory containing the resulting mount command, then run the script.
- 3 Change to the domain or post office directory that you have mounted, then enter the following command:

```
touch test
```

This creates a file named `test` across the mount and shows that ConsoleOne can also write across the mount.
- 4 To make the mount persistent, so that it is automatically available whenever you reboot the Linux server, edit the `/etc/fstab` (<http://en.wikipedia.org/wiki/Fstab>) file with the same information that you used in the mount command.

Mounting a SLES File System Using Samba

- ♦ “[Identifying the Directory Structure for the Samba Share](#)” on page 44
- ♦ “[Preparing Your Firewall to Allow Samba Connections](#)” on page 44
- ♦ “[Configuring the Samba Server](#)” on page 44
- ♦ “[Configuring the Samba Web Administration Tool \(SWAT\)](#)” on page 44
- ♦ “[Accessing SWAT](#)” on page 44
- ♦ “[Setting the Samba Password](#)” on page 45
- ♦ “[Creating a Samba Share](#)” on page 45
- ♦ “[Mounting a Samba Share](#)” on page 45

Identifying the Directory Structure for the Samba Share

- 1 In a terminal window on the SLES server, become root by entering `su -` and the root password.
- 2 If you are creating a new domain or post office, create the directory structure new domain and/or post office.
or
If you are not creating a new domain or post office, make sure you know where the existing directory is located.
- 3 Continue with [Preparing Your Firewall to Allow Samba Connections](#).

Preparing Your Firewall to Allow Samba Connections

- 1 In YaST, click *Security and Users > Firewall*, then click *Interfaces*.
- 2 Click *Change*, select *Internal Zone*, then click *OK*.
- 3 Click *Next* to view the summary, then click *Finish*.
- 4 Continue with [Configuring the Samba Server](#).

Configuring the Samba Server

- 1 In YaST, click *Network Services > Samba Server*.
- 2 Specify a workgroup or domain name, then click *Next*.
For use in your GroupWise system, the Samba server does not need to be part of a workgroup or domain, so it does not matter what you put in this field. For example, you could use GWSYSTEM.
- 3 Select *Not a Domain Controller*, then click *Next*.
For use in your GroupWise system, the Samba server does not need to be a domain controller.
- 4 Under *Service Start*, select *During Boot*.
Because you prepared the firewall in “[Preparing Your Firewall to Allow Samba Connections](#)” on [page 44](#), the *Firewall Settings* section shows that the firewall port for Samba is already open.
- 5 Click *OK* to finish the basic configuration of the Samba server.
- 6 Continue with [Configuring the Samba Web Administration Tool \(SWAT\)](#).

Configuring the Samba Web Administration Tool (SWAT)

- 1 In YaST, click *Network Services > Network Services (xinetd)*.
- 2 Select *Enable*.
- 3 In the *Currently Available Services* list, select *swat*, then click *Toggle Status (On or Off)*.
SWAT is off by default; this turns it on.
- 4 Click *Finish*.
- 5 Continue with [Accessing SWAT](#).

Accessing SWAT

- 1 Display SWAT in your Web browser with the following URL:
`http://localhost:901`
- 2 Specify the root user name and password, then click *OK*.

- 3 On the SWAT toolbar, click *Status* to verify that `smbd` and `nmbd` are running.
It is not necessary for `winbindd` to be running.
- 4 Continue with [Setting the Samba Password](#).

Setting the Samba Password

- 1 On the SWAT toolbar, click *Password*.
The *User Name* field defaults to `root`.
- 2 Type, then retype, the `root` password, then click *Add New User*.
This sets up `root` as a Samba user, so that Samba mounts have the read/write access required by ConsoleOne.
- 3 Continue with [Creating a Samba Share](#).

Creating a Samba Share

- 1 On the SWAT toolbar, click *Shares*.
- 2 In the *Create Share* field, type a unique name for the share, such as `gwsystem`, then click *Create Share*.
- 3 In the *Path* field, specify the directory referenced in [“Identifying the Directory Structure for the Samba Share” on page 44](#).
- 4 In the *Read Only* field, select *No*.
- 5 In the *Available* field, select *Yes*.
- 6 Click *Commit Changes*.
- 7 Continue with [Mounting a Samba Share](#).

Mounting a Samba Share

- 1 Use the appropriate command to mount the Samba share to the SLES server where you want to run ConsoleOne:

```
SLES 11: mount -t cifs //fully_qualified_hostname/windows_share_name  
         /linux_mount_directory -o username=root,noserverino
```

The `noserverino` option uses client-generated inode numbers instead of server-generated inode numbers, which produces a more reliable CIFS mount.

```
SLES 10: mount -t smbfs //fully_qualified_hostname/windows_share_name  
         /linux_mount_directory -o username=root
```

NOTE: The SLES 11 `mount` command does not accept `smbfs` as a valid mount type. [CIFS \(http://en.wikipedia.org/wiki/Cifs\)](http://en.wikipedia.org/wiki/Cifs) (Common Internet File System) is an update to the [SMB \(http://en.wikipedia.org/wiki/Server_Message_Block\)](http://en.wikipedia.org/wiki/Server_Message_Block) (Samba) protocol.

- 1a Replace `fully_qualified_hostname` with the name of the server that you are mounting the local server, such as `prov01.novell.com`.
 - 1b Replace `share_name` with the name of the Samba share that you created in [“Creating a Samba Share” on page 45](#).
 - 1c Replace `linux_mount_directory` with the full path for the directory that you created in [“Identifying the Directory Structure for the Samba Share” on page 44](#).
- 2 Create a script in the `/mnt` directory with the resulting `mount` command, then run the script.

- 3 Change to the domain or post office directory that you have mounted, then enter the following command:

```
touch test
```

This creates a file named `test` across the mount and shows that ConsoleOne will also be able to write across the mount.

- 4 To make the mount persistent, so that it is automatically available whenever you reboot the Linux server, edit the `/etc/fstab` (<http://en.wikipedia.org/wiki/Fstab>) file with the same information that you used in the `mount` command.

2.1.6 Changing the Linux Mount Directory

During creation of your basic GroupWise system, you established a Linux mount directory on the server where you created your basic GroupWise system, as described in “[Selecting a Linux Mount Directory](#)” in “[Installing a Basic GroupWise System](#)” in the *GroupWise 2012 Installation Guide*. The mount directory information is stored in the `.consoleone/SnapinPrefs.ser` file in the `/root` directory, which is the home directory for the `root` user.

To change the mount directory later in ConsoleOne:

- 1 Click *Tools > GroupWise System Operations*.
- 2 Click *System Preferences > Linux Settings*.
- 3 In the *Linux Mount Directory* field, browse to and select the desired mount directory, then click *OK*.

2.2 ConsoleOne on Windows

You can run Windows ConsoleOne on any Windows server or workstation that meets the requirements listed in “[GroupWise Administration Requirements](#)” in the *GroupWise 2012 Installation Guide*.

- ♦ [Section 2.2.1, “Installing ConsoleOne and the GroupWise Snap-Ins on Windows,” on page 46](#)
- ♦ [Section 2.2.2, “Configuring Your Windows Machine for ConsoleOne,” on page 47](#)
- ♦ [Section 2.2.3, “Starting ConsoleOne on Windows,” on page 47](#)
- ♦ [Section 2.2.4, “Mapping a Drive for a New Domain or Post Office,” on page 47](#)

2.2.1 Installing ConsoleOne and the GroupWise Snap-Ins on Windows

When you created your basic GroupWise system using the GroupWise Installation program (`install.exe`), the GroupWise Administrator snap-ins to ConsoleOne were installed to the ConsoleOne installation on that server, along with ConsoleOne itself if necessary.

After you set up your basic GroupWise system, you can use the GroupWise Installation program to install ConsoleOne and the GroupWise Administrator snap-ins from the *GroupWise 2012* software image to additional Windows servers and workstations as needed.

- 1 Make the downloaded *GroupWise 2012* software image available on the Windows machine where you want to install ConsoleOne and the GroupWise Administrator snap-ins.
- 2 Start the GroupWise Installation program (`setup.exe`) at the root of the software image.
- 3 Select the language in which you want to run the GroupWise Installation program, then click *OK*.

- 4 Click *Install GroupWise System*, then click *Yes* to accept the License Agreement.
- 5 Click *Next* to accept the default of a Standard installation.
- 6 Click *Install individual components*, deselect *GroupWise Agents*, then click *Next*.
- 7 Deselect *Copy files to a software distribution directory*, then click *Next*.
- 8 (Conditional) If ConsoleOne is not already installed on the Windows machine, click *Install ConsoleOne*, then follow the prompts to install ConsoleOne.
- 9 Click *Next* to accept the default location of the ConsoleOne software:

`c:\novell\consoleone\1.2`

or

Browse to and select the actual location of the ConsoleOne software on the Windows machine, then click *Next*.

- 10 Review the settings you have selected, then click *Install*.
- 11 When the installation is completed, click *Finish*.
- 12 Download and install the LDAP snap-in for ConsoleOne from [Novell Downloads \(http://download.novell.com/Download?buildid=FACT5LqrhcGI-\)](http://download.novell.com/Download?buildid=FACT5LqrhcGI-).

2.2.2 Configuring Your Windows Machine for ConsoleOne

To ensure GroupWise database integrity across the network:

- 1 Right-click **N** on the Windows taskbar, then click *Novell Client Properties*.
- 2 Click *Advanced Settings*.
- 3 Set *File Caching* to *Off*.
- 4 Set *File Commit* to *On*.
- 5 Click *OK* to save the new Novell Client settings, then reboot the Windows machine to put the new settings into effect.

2.2.3 Starting ConsoleOne on Windows

When you install ConsoleOne, a ConsoleOne icon is automatically created on your Windows desktop for starting ConsoleOne. You can also start it from the Windows *Start* menu.

2.2.4 Mapping a Drive for a New Domain or Post Office

In order to create a new domain in ConsoleOne, you must map a drive to the Windows server where you want to create the domain. If you want to create a new post office, you must also map a drive to the Windows server where you want to create the post office.

- 1 Right-click the Computer object, then click *Map network drive*.
- 2 In the *Drive* field, select the drive letter to use for the Windows server where you want to create the new domain or post office.
- 3 In the *Folder* field, specify the location of the server in the following format:

`\\ip_address\share_name`

Replace *ip_address* with the IP address of the Windows server. Replace *share_name* with the name of the share that you have set up on the remote Windows server.

- 4 Select *Reconnect at logon*.
- 5 (Conditional) If the user name and password required to access the remote Windows server are different from the user name and password for the local Windows server, select *Connect using different credentials*.
- 6 Click Finish.
- 7 (Conditional) If prompted, specify the administrator user name and password for the remote Windows server, then click *OK*.
The mapped drive appears in Windows Explorer and can now be accessed from Windows ConsoleOne.

2.3 ConsoleOne in a Multiple-Platform Environment

If your GroupWise system includes both Linux and Windows, you can administer Linux domains and post office from Windows ConsoleOne and administer Windows domains and post offices from Linux ConsoleOne.

NOTE: If your GroupWise system still includes NetWare domains and post offices, see [“Migrating Away from NetWare”](#) in [“Update”](#) in the *GroupWise 2012 Installation Guide* for NetWare-specific considerations.

This section helps you set up the cross-platform connections that enable ConsoleOne to successfully access GroupWise databases on any platform.

- ♦ [Section 2.3.1, “Using Linux ConsoleOne to Access Domains and Post Offices on Windows,”](#) on page 48
- ♦ [Section 2.3.2, “Using Windows ConsoleOne to Access Domains and Post Offices on Linux,”](#) on page 50

2.3.1 Using Linux ConsoleOne to Access Domains and Post Offices on Windows

In order for you to be able to use Linux ConsoleOne to administer domains and post offices that are located on Windows, the domain and post office directories on the Windows servers must be mounted as Linux filesystems.

- ♦ [“Working with the Linux Mount Directory”](#) on page 49
- ♦ [“Making a Windows Server Visible in Linux ConsoleOne”](#) on page 49
- ♦ [“Accessing a Domain or Post Office on NetWare or Windows from Linux ConsoleOne”](#) on page 50

Working with the Linux Mount Directory

The first time you run Linux ConsoleOne on a server, you are prompted to provide a Linux mount directory on that server. The default location is `/mnt`. For more information, see “Linux Mount Directory” in “Planning a Basic GroupWise System” in the *GroupWise 2012 Installation Guide*. For convenience, you can later change the Linux mount directory, as described in [Section 2.1.6, “Changing the Linux Mount Directory,”](#) on page 46.

Underneath the Linux mount directory, you must create a subdirectory for each directory where a domain or post office resides on a Windows server, that you want to be able to access from Linux ConsoleOne. For example, if you have a domain directory named `provo1` on a Windows server, you would create a `provo1` subdirectory under `/mnt` on the Linux server where you want to run ConsoleOne.

Making a Windows Server Visible in Linux ConsoleOne

- 1 Use the appropriate command to mount the Windows share to the Linux server where you want to run ConsoleOne:

```
SLES 11: mount -t cifs //fully_qualified_hostname/windows_share_name
          /linux_mount_directory
          -o username=windows_administrator,noserverino
```

The `noserverino` option uses client-generated inode numbers instead of server-generated inode numbers, which produces a more reliable CIFS mount.

```
SLES 10: mount -t smbfs //fully_qualified_hostname/windows_share_name
           /linux_mount_directory -o username=windows_administrator
```

NOTE: The SLES 11 mount command does not accept `smbfs` as a valid mount type. [CIFS](http://en.wikipedia.org/wiki/Cifs) (<http://en.wikipedia.org/wiki/Cifs>) (Common Internet File System) is an update to the [SMB](http://en.wikipedia.org/wiki/Server_Message_Block) (http://en.wikipedia.org/wiki/Server_Message_Block) (Samba) protocol.

- 1a Replace `fully_qualified_hostname` with the name of the Windows server that you are mounting the Linux server where you want to run ConsoleOne, such as `provo1.novell.com`.
 - 1b Replace `share_name` with the name of the Windows share on the Windows server, such as `C`.
 - 1c Replace `linux_mount_directory` with the full path for the directory that you created in “Working with the Linux Mount Directory” on page 49.
 - 1d Replace `windows_administrator` with the user name of the administrator user of the Windows server, such as `Administrator`.
- 2 Create a script in the `/mnt` directory with the resulting mount command, then run the script.
- 3 Change to the domain or post office directory that you have mounted, then enter the following command:

```
touch test
```

This creates a file named `test` across the mount and shows that Linux ConsoleOne will also be able to write across the mount.

- 4 To make the mount persistent, so that it is automatically available whenever you reboot the Linux server, edit the `/etc/fstab` (<http://en.wikipedia.org/wiki/Fstab>) file with the same information that you used in the mount command.

Accessing a Domain or Post Office on NetWare or Windows from Linux ConsoleOne

After you have made the Windows server visible from Linux:

- 1 Mount the domain directory to the Linux server.
- 2 In Linux ConsoleOne, authenticate to the eDirectory tree where the Domain object is located.
- 3 Click *Tools > GroupWise System Operations > Select Domain*.
- 4 Browse to and select the domain directory, then click *OK*.

You can now use Linux ConsoleOne to administer all GroupWise objects that belong to the domain that is located on Windows.

2.3.2 Using Windows ConsoleOne to Access Domains and Post Offices on Linux

In order for you to be able to use Windows ConsoleOne to administer domains and post offices that are located on Linux, the Linux servers where the domains and post offices are located must be accessible from Windows. To make a Linux server visible from Windows, you need to configure it so that you can map a drive to it as if it were a Windows server. There are a variety of ways to accomplish this.

- ♦ [“Using NetWare Core Protocol to Connect from Windows to an OES Linux Server” on page 50](#)
- ♦ [“Using Samba to Connect from Windows to an OES Linux Server” on page 52](#)
- ♦ [“Using Samba to Connect from Windows to a SLES Server” on page 54](#)

Using NetWare Core Protocol to Connect from Windows to an OES Linux Server

On OES Linux, if you are using the ext3 or reiserfs filesystem, you use Novell Core Protocol (NCP) to configure the Linux server for access from Windows. Then, on Windows, you use the Novell Map Network Drive feature to map a drive from Windows to the Linux filesystem where the domain or post office is located.

- ♦ [“Configuring the OES Linux Server for NCP Access from Windows” on page 50](#)
- ♦ [“Mapping a Windows Drive to the NCP Volume” on page 51](#)

Configuring the OES Linux Server for NCP Access from Windows

- 1 In a terminal window on the OES server, become `root` by entering `su -` and the `root` password.
- 2 If you are creating a new domain or post office on the OES Linux server, create the base directory where you want to use Windows ConsoleOne to create the domain and/or post office directory structure.
or
If you are not creating a new domain or post office on the OES Linux server, make sure you know where the existing base directory is located.
- 3 Enter the following command to create the NCP volume on the OES Linux server:

```
ncpcon create volume volume_name /directory
```

- 3a** Replace *volume_name* with a unique name for the location where you want to create the domain and/or post office directory structure
 - 3b** Replace *directory* with the directory referenced in [Step 2](#) above.
- 4** Verify that the volume has been created:

```
more /etc/opt/novell/ncpserv.conf
```

The new volume should be listed at the end of the NCP server configuration file.

- 5** Enable cross-protocol locks so that Windows ConsoleOne can safely access GroupWise databases across the connection between Windows and Linux:

- 5a** Enter the following command

```
ncpcon set cross_protocol_locks=1
```

or

Add the following line at the bottom of the `ncpserv.conf` file:

```
CROSS_PROTOCOL_LOCKS 1
```

- 5b** Restart the Novell eDirectory daemon:

```
rcnstd restart
```

- 6** Continue with [Mapping a Windows Drive to the NCP Volume](#).

Mapping a Windows Drive to the NCP Volume

- 1** On the Windows server, right-click **N** on the Windows taskbar, then click *Novell Map Network Drive*.
- 2** Select the drive letter to map to the NCP volume on the OES Linux server.
- 3** Specify the network path to the NCP volume in the following format:

```
\\linux_hostname\ncp_volume
```

 - 3a** Replace *linux_hostname* with the hostname of the OES Linux server.
 - 3b** Replace *ncp_volume* with the name of the NCP volume that you just created.
- 4** For the network user name, specify the fully qualified administrator user name for eDirectory, such as `admin.users.novell`.
- 5** Select *Check to always map this drive letter when you start Windows*.
- 6** Click *Map*.
- 7** (Conditional) If prompted, log in to eDirectory:
 - 7a** In the *Password*, specify the eDirectory password for the administrator user.
 - 7b** In the *Context* field, specify the eDirectory context where the administrator User object is located.
- 8** Click *OK*.

The mapped drive to the OES Linux server opens in Windows Explorer and can now be accessed from Windows ConsoleOne.

Using Samba to Connect from Windows to an OES Linux Server

On OES Linux, if you are using the Novell Storage Services (NSS) filesystem, you use Samba to create the connection between Linux and Windows. Then, on Windows, you use the Novell Map Network Drive feature to map a drive from Windows to the Samba share.

- ♦ [“Identifying the Directory Structure for the Samba Share” on page 52](#)
- ♦ [“Installing Samba” on page 52](#)
- ♦ [“Logging In to iManager” on page 52](#)
- ♦ [“Configuring the eDirectory Universal Password for Samba” on page 53](#)
- ♦ [“Setting the eDirectory Universal Password for the Samba Administrator User” on page 53](#)
- ♦ [“Creating a Samba Share” on page 53](#)
- ♦ [“Setting the eDirectory Rights for the Samba Share” on page 53](#)
- ♦ [“Testing Samba on the OES Server” on page 53](#)
- ♦ [“Mapping a Windows Drive to the Samba Share on the OES Linux Server” on page 54](#)

Identifying the Directory Structure for the Samba Share

- 1 In a terminal window on the OES Linux server, become root by entering `su -` and the root password.
- 2 If you are creating a new domain or post office, create the base directory for the new domain and/or post office.
or
If you are not creating a new domain or post office, make sure you know where the existing directory is located.
- 3 Continue with [Installing Samba](#).

Installing Samba

If you installed Samba when you installed OES Linux, skip to [“Logging In to iManager” on page 52](#).

If you did not install Samba when you installed OES Linux, install it now:

- 1 Start YaST.
- 2 Under *Groups*, click *Open Enterprise Server*, then click *OES Install and Configuration*.
- 3 Under *OES Services*, select *Novell Samba*, then click *Accept*.
- 4 Follow the prompts to install Novell Samba.
- 5 Continue with [Logging In to iManager](#).

Logging In to iManager

- 1 Access the following URL:
`https://ip_address/nps/servlet/webacc?taskid=fw Startup`
Replace *ip_address* with the IP address of the OES Linux server.
- 2 Specify the eDirectory administrator user name, such as `admin.users.novell`, the password for the user name, and the IP address of the eDirectory tree, then click *Login*.
- 3 Continue with [Configuring the eDirectory Universal Password for Samba](#).

Configuring the eDirectory Universal Password for Samba

- 1 In iManager, click *Passwords > Password Policies*.
- 2 Click *Samba Default Password Policy*.
- 3 On the *Policy Assignment* tab, browse to and click the name of the administrator User object that you want to administer the Samba share, then click *OK* to add the user to the list.
- 4 Click *OK* to complete the process.
- 5 Continue with [Setting the eDirectory Universal Password for the Samba Administrator User](#).

Setting the eDirectory Universal Password for the Samba Administrator User

- 1 Under *Passwords*, click *Set Universal Password*.
- 2 Browse to and click the name of the Samba administrator User object, then click *OK*.
- 3 Specify the password for the Samba administrator user, retype the password for confirmation, then click *OK*.
- 4 Click *Passwords* to close the *Passwords* menu.
- 5 Continue with [Creating a Samba Share](#).

Creating a Samba Share

- 1 Click *File Protocols*, then click *Samba*.
- 2 Browse to and click the name of the Server object where you are setting up the Samba share.
- 3 On the *Shares* tab, create a new Samba share for the directory on the Linux server reference in [“Identifying the Directory Structure for the Samba Share” on page 52](#):
 - 3a Click *New*.
 - 3b Specify a unique name for the Samba share, such as `gwsystem`.
 - 3c Specify the full path name on the Linux server for the domain or post office, click *OK* to add the location to the list of Samba shares, then click *Close*.
 - 3d Click *File Protocols* to close the *File Protocols* menu.
- 4 Continue with [Setting the eDirectory Rights for the Samba Share](#).

Setting the eDirectory Rights for the Samba Share

- 1 Click *Files and Folders*, then click *Properties*.
- 2 Browse to and click the name of the Linux partition or directory where you created the new share, then click *OK*.
- 3 Click *Rights*.
- 4 In the *Add Trustee* field, browse to and click the name of the Samba administrator User object, then click *OK*.
- 5 Grant all file system rights to the Samba administrator user, then click *OK*.
- 6 Continue with [Testing Samba on the OES Server](#).

Testing Samba on the OES Server

- 1 Double-click the Home Directory icon on the Linux desktop.
- 2 Click 

- 3 In the Location field, type `smb://user_name@ip_address`
 - 3a Replace `user_name` with the user name of the Samba administrator user.
 - 3b Replace `ip_address` with the IP address of the Linux server.

The File Browser should display all Samba shares, including the new one that you created for the domain and/or post office.
- 4 Continue with [Mapping a Windows Drive to the Samba Share on the OES Linux Server](#).

Mapping a Windows Drive to the Samba Share on the OES Linux Server

- 1 In Windows Explorer, right-click the Computer object, then click *Map network drive*.
- 2 In the *Drive* field, select the drive letter for the new Samba share.
- 3 In the *Folder* field, specify the location of the Samba share in the following format:
`\\ip_address\share_name`
 - 3a Replace `ip_address` with the IP address of the Linux server.
 - 3b Replace `share_name` with the name of the new Samba share.
- 4 Select *Reconnect at logon*.
- 5 Select *Connect using different credentials*.
- 6 Specify the Samba administrator user name and password, then click *OK*.

The Samba share for the OES Linux file system opens in Windows Explorer and can now be accessed from Windows ConsoleOne.

Using Samba to Connect from Windows to a SLES Server

On SLES, you use YaST and the Samba Web Administration Tool (SWAT) to configure Samba. Then you use the Windows Map Network Drive feature to map a drive from Windows to the Samba share.

- ♦ [“Identifying the Directory Structure for the Samba Share” on page 54](#)
- ♦ [“Preparing Your Firewall to Allow Samba Connections” on page 55](#)
- ♦ [“Configuring the Samba Server” on page 55](#)
- ♦ [“Configuring the Samba Web Administration Tool \(SWAT\)” on page 55](#)
- ♦ [“Accessing SWAT” on page 55](#)
- ♦ [“Creating a Samba Share” on page 55](#)
- ♦ [“Mapping a Windows Drive to the Samba Share on the SLES Server” on page 56](#)

Identifying the Directory Structure for the Samba Share

- 1 In a terminal window on the OES server, become root by entering `su -` and the root password.
- 2 If you are creating a new domain or post office, create the base directory for the new domain and/or post office directory structure.

or

If you are not creating a new domain or post office, make sure you know where the existing directory is located.
- 3 Continue with [Preparing Your Firewall to Allow Samba Connections](#).

Preparing Your Firewall to Allow Samba Connections

- 1 In YaST, click *Security and Users > Firewall*, then click *Interfaces*.
- 2 Click *Change*, select *Internal Zone*, then click *OK*.
- 3 Click *Next* to view the summary, then click *Finish*.
- 4 Continue with [Configuring the Samba Server](#).

Configuring the Samba Server

- 1 In YaST, click *Network Services > Samba Server*.
- 2 Specify a workgroup or domain name, then click *Next*.
For use in your GroupWise system, the Samba server does not need to be part of a workgroup or domain, so it does not really matter what you put in this field. For example, you could use GWSYSTEM.
- 3 Select *Not a Domain Controller*, then click *Next*.
For use in your GroupWise system, the Samba server does not need to be a domain controller.
- 4 Under *Service Start*, select *During Boot*.
Because you prepared the firewall in “[Preparing Your Firewall to Allow Samba Connections](#)” on [page 55](#), the firewall port for Samba is already open.
- 5 Click *OK* to finish the basic configuration of the Samba server.
- 6 Continue with [Configuring the Samba Web Administration Tool \(SWAT\)](#).

Configuring the Samba Web Administration Tool (SWAT)

- 1 In YaST, click *Network Services > Network Services (xinetd)*.
- 2 Select *Enable*.
- 3 In the *Currently Available Services* list, select *swat*, then click *Toggle Status (On or Off)*.
SWAT is off by default. This turns it on.
- 4 Click *Finish*.
- 5 Continue with [Accessing SWAT](#).

Accessing SWAT

- 1 Display SWAT in your Web browser with the following URL:
`http://localhost:901`
- 2 Specify the root user name and password, then click *OK*.
- 3 On the SWAT toolbar, click *Status* to verify that *smbd* and *nmbd* are running.
It is not necessary for *winbindd* to be running.
- 4 Continue with [Creating a Samba Share](#).

Creating a Samba Share

- 1 On the SWAT toolbar, click *Shares*.
- 2 In the *Create Share* field, type a unique name for the share, such as *gwsystem*, then click *Create Share*.

- 3 In the *Path* field, specify the directory that you created in [“Identifying the Directory Structure for the Samba Share”](#) on page 54.
- 4 In the *Read Only* field, select *No*.
- 5 In the *Available* field, select *Yes*.
- 6 Click *Commit Changes*.

Mapping a Windows Drive to the Samba Share on the SLES Server

- 1 On the Windows desktop, right-click the Computer object, then click *Map network drive*.
- 2 In the *Drive* field, select the drive letter for the new Samba share.
- 3 In the *Folder* field, specify the location of the Samba share in the following format:

`\\ip_address\share_name`

- 3a Replace *ip_address* with the IP address of the Linux server.
 - 3b Replace *share_name* with the name of the new Samba share.
- 4 Select *Reconnect at logon*.
- 5 Select *Connect using different credentials*.
- 6 Specify the Samba administrator user name and password, then click *OK*.

The Samba share on the SLES server opens in Windows Explorer and can now be accessed from Windows ConsoleOne.

2.4 Remote Access to ConsoleOne on a Linux Server

If your GroupWise system includes domains on Linux servers, file system mounts are required for a few specific GroupWise administration tasks. However, you can perform the bulk of typical domain, post office, and user administration without needing file system mounts between Linux servers where domains and post offices reside. You can perform these administration tasks from either Linux or Windows.

- ♦ [Section 2.4.1, “Administrative Tasks Requiring File System Mounts,”](#) on page 56
- ♦ [Section 2.4.2, “Remote ConsoleOne Access with a VNC Client,”](#) on page 57
- ♦ [Section 2.4.3, “Remote ConsoleOne Access with a Secure Shell \(SSH\) Connection,”](#) on page 58

2.4.1 Administrative Tasks Requiring File System Mounts

ConsoleOne requires file system mounts to both the primary domain database and a secondary domain database simultaneously to perform the following tasks:

- ♦ Create Domain
- ♦ Rebuild Domain Database
- ♦ Sync Primary with Secondary
- ♦ Replace Primary with Secondary
- ♦ Merge/Release

For more information, see [Section 4.1.2, “Understanding the Need for Domain Connections,”](#) on page 71.

Aside from these fairly specialized administrative tasks, you can connect directly to a secondary domain database on a Linux server from either Linux or Windows, and then run Linux ConsoleOne to conveniently perform other GroupWise administration tasks remotely.

2.4.2 Remote ConsoleOne Access with a VNC Client

Remote administration can be made possible by using a VNC (Virtual Network Connection) client where you want to run ConsoleOne (on either Linux or Windows) and by enabling Remote Administration on each remote Linux server where you need to access a domain database.

- ♦ [“Selecting a VNC Client” on page 57](#)
- ♦ [“Enabling Remote Administration” on page 57](#)
- ♦ [“Using Your VNC Client on Linux or Windows to Run ConsoleOne on the Linux Server” on page 58](#)

Selecting a VNC Client

Many VNC clients are available for use on Linux and Windows. To investigate your options, you can google “VNC clients”. Review their capabilities and select one that appeals to you. RealVNC is a common favorite. Install the VNC client where you want to run ConsoleOne with direct access to remote Linux servers.

Enabling Remote Administration

By default, Linux servers do not allow remote administration for understandable security reasons. To use your VNC client, you must enable Remote Administration on each remote Linux server.

- 1 In YaST:
 - 1a (Conditional) On OES, click *Network Devices > Remote Administration*.
 - or
 - 1b (Conditional) On SLES, click *Network Services > Remote Administration*.
- 2 Select *Allow Remote Administration*.

If your firewall is properly configured, *Open Port in Firewall* is selected by default. The default port number used for remote administration is 5901.
- 3 (Conditional) If *Open Port in Firewall* is not selected:
 - 3a Click *Abort* to cancel *Remote Administration* setup.
 - 3b Click *Security and Users > Firewall*.
 - 3c In the left pane, click *Interfaces*, then click *Change* to configure the firewall interface.
 - 3d In the *Interface Zone* drop-down list, select the zone appropriate for the Linux server where you are enabling Remote Administration, then click *OK*.
 - 3e Click *Next* to list your current firewall settings, then click *Finish* to put the updated setting into effect.
 - 3f Return to [Step 1](#) to enable Remote Administration.
- 4 After enabling Remote Administration, click *Finish* to put the settings into effect.

Using Your VNC Client on Linux or Windows to Run ConsoleOne on the Linux Server

After you have enabled Remote Administration on the remote Linux servers:

- 1 Access the remote Linux server in your VNC client by providing the remote server's IP address and the remote administration port number, for example:

```
137.16.5.18:5901
```

- 2 In the window that opens on the remote Linux server, start ConsoleOne:

```
/usr/ConsoleOne/bin/ConsoleOne
```

- 3 Authenticate to the eDirectory tree to start ConsoleOne as usual.
- 4 Attach to the domain on the Linux server.
- 5 Proceed with your GroupWise administration tasks.
- 6 When you are finished with GroupWise administration on the remote Linux server, exit ConsoleOne.
- 7 Close the window where you have been running ConsoleOne, to close the connection with the remote Linux server.

2.4.3 Remote ConsoleOne Access with a Secure Shell (SSH) Connection

As an alternative to the Remote Administration feature in YaST, you can use a secure shell (SSH) connection to a remote Linux server in order to run ConsoleOne on the remote Linux server.

- ♦ [“Configuring a Linux Server to Allow a Secure Shell Connection” on page 58](#)
- ♦ [“Using a Secure Shell Connection on Linux to Run ConsoleOne on the Linux Server” on page 59](#)
- ♦ [“Using a Secure Shell Connection on Windows to Run ConsoleOne on the Linux Server” on page 59](#)

Configuring a Linux Server to Allow a Secure Shell Connection

- ♦ [“On OES 11 and SLES 11” on page 58](#)
- ♦ [“On OES 2 and SLES 10” on page 59](#)

On OES 11 and SLES 11

- 1 In YaST, click *Network Service > SSHD Configuration*.
- 2 Ensure that *Allow X11 Forwarding* is selected.
This is the default setting.
- 3 Click *Finish* to enable SSHD.
- 4 Configure your firewall to allow the SSHD connection:
 - 4a Under *Security and Users*, click *Firewall*.
 - 4b Click *Allowed Services*.
 - 4c In the *Service to Allow* drop-down list, select *Secure Shell Server*, then click *Add*.
 - 4d Click *Next*, then click *Finish*.

On OES 2 and SLES 10

- 1 Check the `/etc/ssh/sshd_config` file to ensure that `X11Forwarding` is set to `yes`.
This is the default setting.
- 2 Configure your firewall to allow the SSH connection:
 - 2a Under *Security and Users*, click *Firewall*.
 - 2b Click *Allowed Services*.
 - 2c In the *Service to Allow* drop-down list, select *SSH*, then click *Add*.
 - 2d Click *Next*, then click *Finish*.

Using a Secure Shell Connection on Linux to Run ConsoleOne on the Linux Server

- 1 Enter the following command to establish a secure shell connection to the remote Linux server:

```
ssh -X network_address
```

Replace `network_address` with the IP address or DNS hostname of the remote Linux server.

- 2 Enter the password to access the remote Linux server as `root`.
The command prompt changes to the name of the remote Linux server.
- 3 Start ConsoleOne on the Linux server:

```
/usr/ConsoleOne/bin/ConsoleOne
```

- 4 Authenticate to the eDirectory tree as usual.
- 5 Connect to the domain on the Linux server.
- 6 Proceed with your GroupWise administration tasks.
- 7 When you are finished with GroupWise administration on the remote Linux server, exit ConsoleOne.
- 8 Exit the terminal window where you have been connected to the remote Linux server, to close the secure shell session.

Using a Secure Shell Connection on Windows to Run ConsoleOne on the Linux Server

Because Windows does not include an X server, setting up a secure shell from Windows to Linux requires additional software that is not free nor especially easy to set up. If you still want to pursue this option, refer to the Cool Solutions article, "[Remote Management Using SSH and X-Forwarding on Windows](http://www.novell.com/coolsolutions/feature/19258.html)" (<http://www.novell.com/coolsolutions/feature/19258.html>).

3 GroupWise View

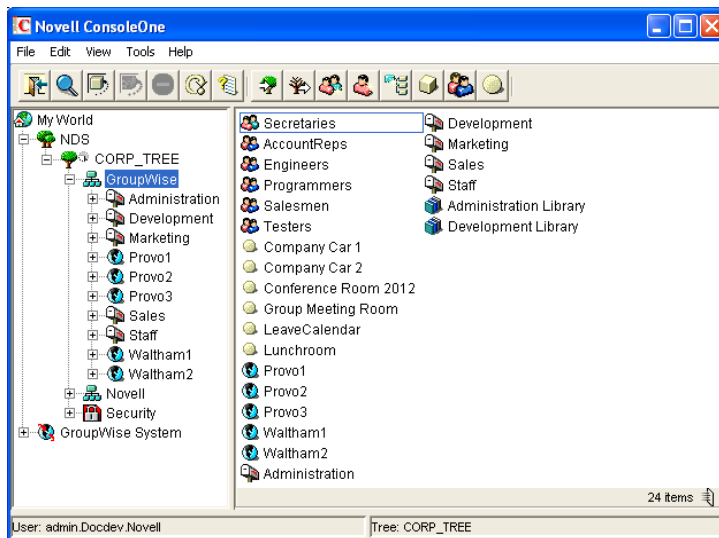
When administering GroupWise in ConsoleOne, you can use the standard Novell eDirectory View or you can use the GroupWise View. The following sections discuss the GroupWise View and how to use it:

- ◆ [Section 3.1, “eDirectory View versus GroupWise View,” on page 61](#)
- ◆ [Section 3.2, “GroupWise Object Icons,” on page 62](#)
- ◆ [Section 3.3, “Customizing the GroupWise View,” on page 64](#)
- ◆ [Section 3.4, “Searching in the GroupWise View,” on page 66](#)
- ◆ [Section 3.5, “Performing Administrative Tasks from the GroupWise View,” on page 67](#)

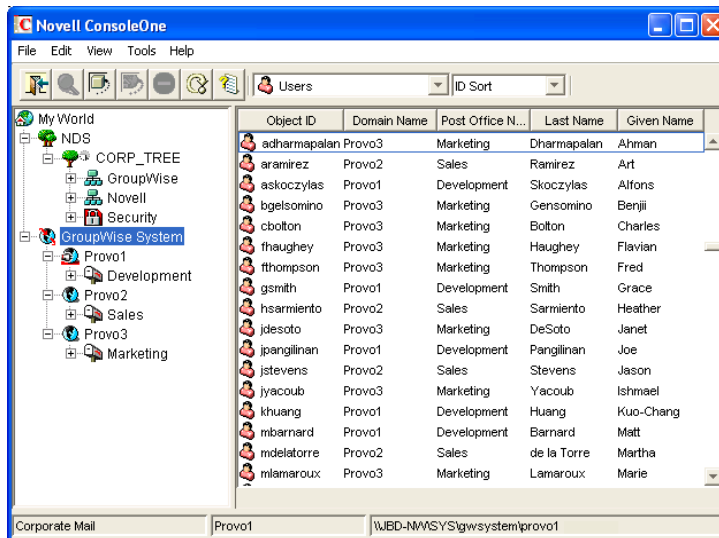
NOTE: The ConsoleOne illustrations used in the guide show ConsoleOne on Windows. ConsoleOne on Linux looks different but provides substantially the same functionality.

3.1 eDirectory View versus GroupWise View

The eDirectory View displays the GroupWise objects in their contexts in the eDirectory tree, as shown in the following example:








The GroupWise View filters out all non-GroupWise objects and shows how the GroupWise objects relate to each other in the GroupWise system, as shown in the following example.



















In the left pane, all Domain objects are displayed under the GroupWise system, and all Post Office objects are subordinate to the domains where they reside. You can select the GroupWise system, a domain, or a post office in the left pane and then use the drop-down list of GroupWise objects on the toolbar to display associated objects (Users, Resources, Message Transfer Agents, and so on) in the right pane. In the above example, the GroupWise System is selected in the left pane and the GroupWise Object list is set to Users, so the right pane is displaying all users in the entire GroupWise system.

3.2 GroupWise Object Icons

The following table lists all the GroupWise objects that are displayed in the eDirectory View or GroupWise View in ConsoleOne.

Icon	GroupWise Object	Additional Information
	GroupWise System	Represents the GroupWise system you are currently connected to. The GroupWise system's name is displayed in the lower left corner of the ConsoleOne window.
	Primary Domain	Represents the system's primary domain. To ensure consistency, all replication of GroupWise information to the GroupWise domain and post office databases takes place through the primary domain. For additional information, see Part II, "Domains," on page 129 .
	Secondary Domain	Represents any additional domains, other than the primary, created in the GroupWise system. For additional information, see Part II, "Domains," on page 129 .
	Current Domain	Represents the domain to which ConsoleOne is currently connected. For information about changing the current domain, see Section 9.1, "Connecting to a Domain," on page 145 .
	External Domain	Represents a domain from another GroupWise system.

Icon	GroupWise Object	Additional Information
	Non-GroupWise Domain	Represents all or part of a non-GroupWise system.
	Post Office	Represents a collection of user accounts (mailboxes). For additional information, see Part III, "Post Offices," on page 171 .
	External Post Office	Represents a post office in an external GroupWise system or a non-GroupWise system.
	User	Represents an eDirectory user who has been given a GroupWise account in a post office. For additional information, see Part IV, "Users," on page 217 .
	External Entity	Represents a user not listed in eDirectory who has been given a GroupWise account in a post office. For additional information, see Part IV, "Users," on page 217 .
	External User	Represents a user in an external GroupWise system or a non-GroupWise system.
	Resource	Represents a conference room or some other resource that can be scheduled by users. For additional information, see Part V, "Resources," on page 263 .
	External Resource	Represents a resource that belongs to an external GroupWise system or a non-GroupWise system.
	Distribution List	Represents a group of users or resources that can all be addressed by using the distribution list's name. For additional information, see Part VI, "Distribution Lists, Groups, and Organizational Roles," on page 279 .
	Group	Represents an eDirectory group. eDirectory groups, like distribution lists, can be addressed by using the group's name. Any members of the group who have GroupWise accounts receive the message. For additional information, see Part VI, "Distribution Lists, Groups, and Organizational Roles," on page 279 .
	Organizational Role	Represents an eDirectory organizational role. eDirectory organizational roles, like distribution lists, can be addressed by using the organizational role's name. Any members of the role who have GroupWise accounts receive the message. For additional information, see Part VI, "Distribution Lists, Groups, and Organizational Roles," on page 279 .
	Library	Represents a collection of documents. For additional information, see Chapter 21, "Document Management Services Overview," on page 315 .
	Nickname	Represents an additional address associated with a user, resource, or distribution list. For additional information, see Part IV, "Users," on page 217 , Part V, "Resources," on page 263 , or Part VI, "Distribution Lists, Groups, and Organizational Roles," on page 279 .
	Message Transfer Agent	Represents a Message Transfer Agent (MTA) associated with a domain. For additional information, see Part X, "Message Transfer Agent," on page 619 .
	Post Office Agent	Represents a Post Office Agent (POA) associated with a post office. For additional information, see Part IX, "Post Office Agent," on page 469 .
	Gateway	Represents a method of linking to another email system or transport. For additional information, see the GroupWise gateway guides (http://www.novell.com/documentation/gwgateways) . GroupWise gateways are legacy products that are not supported with the current GroupWise version.

3.3 Customizing the GroupWise View

You can change the column display, order, and width to customize the GroupWise View.

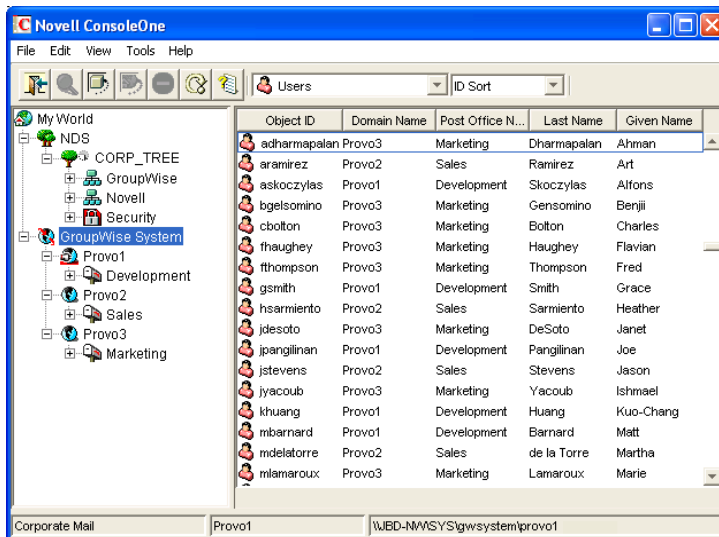
Changes are preserved from one ConsoleOne session to the next. In addition, your last view is persistent from session to session. For example, if you last used the Distribution Lists view, the next time you start ConsoleOne and open the GroupWise View, the Distribution Lists view is displayed. If the last-used view is not applicable (for example, you had the Gateways view open and when the new ConsoleOne session starts you select a Post Office object), the GroupWise View defaults to the Users view.

- ◆ [Section 3.3.1, “Changing the Column Display and Order,” on page 64](#)
- ◆ [Section 3.3.2, “Changing the Column Widths,” on page 66](#)

3.3.1 Changing the Column Display and Order

For each view (Users, Distribution Lists, Gateways, Post Offices, and so on), you can determine which columns are displayed and the order in which they are displayed.

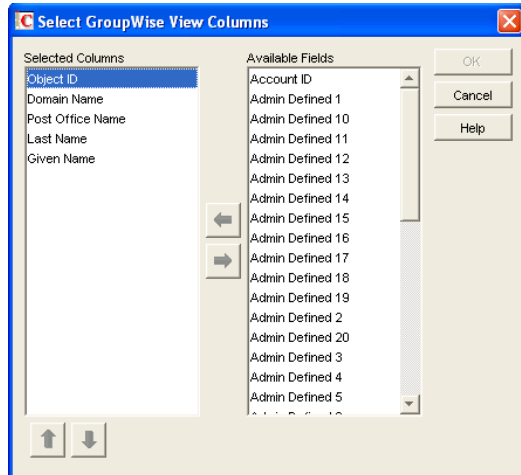
- 1 Select *GroupWise System* in the left (tree) pane, then select the view (for example, *Users*).



- 2 (Conditional) If you are changing the *Users* view, use the drop-down list to select how you want to sort users (ID Sort, User Name Sort, First Name Sort, or Last Name Sort).

The *Users* view allows you to sort by ID, user name, first name, or last name. Each of these is treated as a separate *Users* view for which you can determine the column display and order. The views for different objects offer different sort options.

- 3 Click *View > Edit Columns* to display the Select GroupWise View Columns dialog box.



- 4 To add a column, select the column in the *Available Fields* list, then click the left-arrow to add it to the *Selected Columns* list.

Many kinds of useful information can be added to an object's display in ConsoleOne.

For users, displayable information includes:

- ◆ Current mailbox size
- ◆ File ID (FID)
- ◆ Last client login time
- ◆ Move error

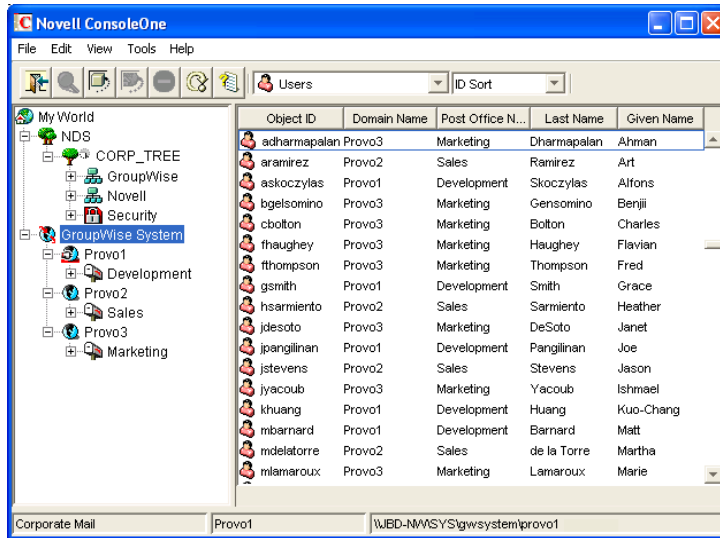
For POAs, displayable information includes:

- ◆ Port numbers
- ◆ Thread numbers
- ◆ Log level
- ◆ Platform

- 5 To determine the display order, select a column in the *Selected Columns* list, then click the up-arrow and down-arrow to move it to the desired position.
- 6 To remove a column, select the column in the *Selected Columns* list, then click the right-arrow to add it to the *Available Fields* list.
- 7 When you are finished, click *OK* to save your changes.

3.3.2 Changing the Column Widths

You can change column widths in a view by dragging the right or left edge of the column label.



3.4 Searching in the GroupWise View

You can search for a specific entry in a view. The search is performed on the first column. For example, if the Resources view is displayed, you can search for a specific resource based on its object ID. If the *Users* view (with Last Name Sort selected) is displayed, you can search for a specific user based on the user's last name.

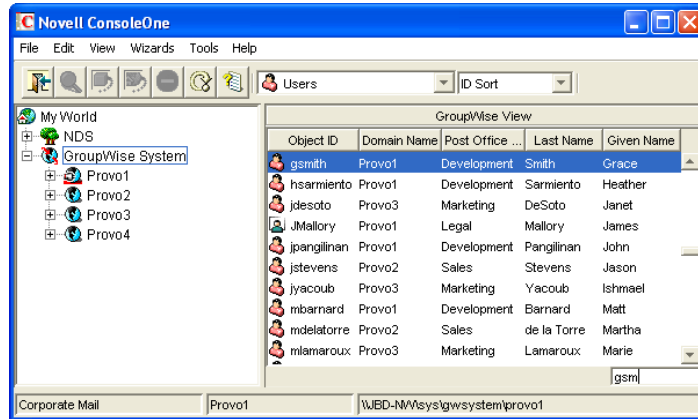
With the *Users* view, if you have *First Name Sort* or *Last Name Sort* selected, you can search for a complete user name (both first and last name) by using a comma as a delimiter between the names. A space after the comma is optional.

For example, if the *Users* view displays first names in the first column and last names in the second column, you can type John,Smith to go directly to that user name. If the columns were reversed, you could use Smith,John.

To perform a search:

- 1 Change to the view you want to search.
- 2 Select the first entry in the view.
- 3 Type the text to search for.

As you type text, a text box appears in the lower right corner of the GroupWise View.



3.5 Performing Administrative Tasks from the GroupWise View

You can perform many GroupWise administrative tasks from the GroupWise View as well as from the eDirectory View. For example, you can:

- ◆ Create new objects.
- ◆ Modify the properties of an object.
- ◆ Move, rename, or delete an object from the GroupWise system.
- ◆ Use the GroupWise utilities, system operations, and diagnostic options on the *Tools* menu.

In addition, external objects must be created and managed in the GroupWise View because they are, by definition, external to eDirectory and have no eDirectory context. For example, if you install the GroupWise Internet Agent (GWIA) and want to simplify addressing for your users by adding the Internet as a non-GroupWise domain, you must perform the task in the GroupWise View.

4 GroupWise System Operations

The GroupWise system operations in ConsoleOne allow you to perform various tasks to maintain and optimize your GroupWise system. The following sections provide information about the system operations included on the *Tools* menu (*Tools > GroupWise System Operations*):

- ◆ [Section 4.1, “Select Domain,” on page 69](#)
- ◆ [Section 4.2, “System Preferences,” on page 72](#)
- ◆ [Section 4.3, “eDirectory User Synchronization,” on page 79](#)
- ◆ [Section 4.4, “Admin-Defined Fields,” on page 79](#)
- ◆ [Section 4.5, “Pending Operations,” on page 80](#)
- ◆ [Section 4.6, “Addressing Rules,” on page 80](#)
- ◆ [Section 4.7, “Time Zones,” on page 81](#)
- ◆ [Section 4.8, “External System Synchronization,” on page 84](#)
- ◆ [Section 4.9, “Software Directory Management,” on page 84](#)
- ◆ [Section 4.10, “Restore Area Management,” on page 89](#)
- ◆ [Section 4.11, “Internet Addressing,” on page 89](#)
- ◆ [Section 4.12, “Trusted Applications,” on page 90](#)
- ◆ [Section 4.13, “LDAP Servers,” on page 93](#)
- ◆ [Section 4.14, “Global Signatures,” on page 94](#)

NOTE: If the majority of the items on the *GroupWise System Operations* menu are dimmed, you are connected to a secondary domain in a GroupWise system where *Restrict System Operations to Primary Domain* has been selected under *System Preferences*. This option is selected by default. For more information, see [Section 4.2, “System Preferences,” on page 72](#).

4.1 Select Domain

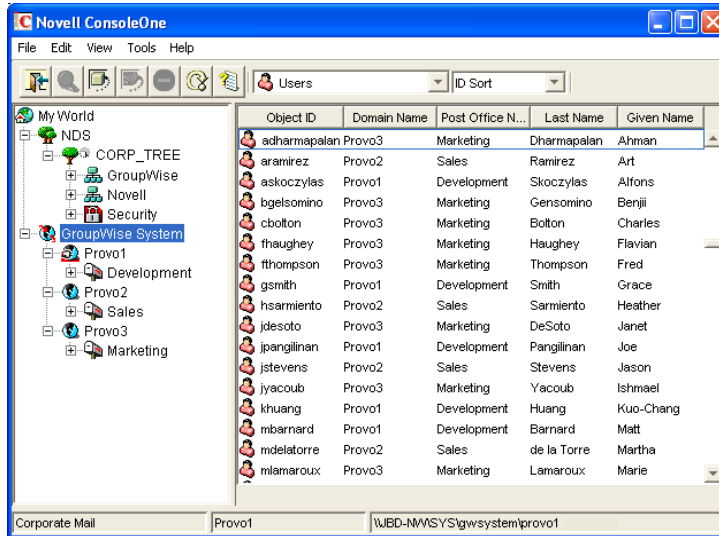
By default, ConsoleOne must be connected to a GroupWise domain in order for you to administer your GroupWise system. Being connected to a GroupWise domain ensures that information is replicated not only in Novell eDirectory but also in the GroupWise domain and post office databases.

- ◆ [Section 4.1.1, “Selecting a Domain to Connect To,” on page 70](#)
- ◆ [Section 4.1.2, “Understanding the Need for Domain Connections,” on page 71](#)
- ◆ [Section 4.1.3, “Handling Cross-Platform Domain Connections,” on page 71](#)

4.1.1 Selecting a Domain to Connect To

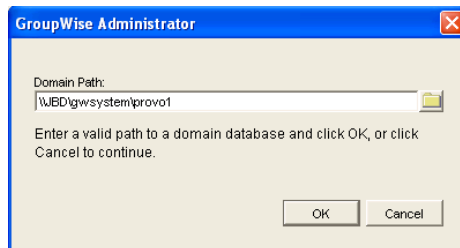
You can be connected to any domain in the GroupWise system. Being connected to a domain means that ConsoleOne has write access to the domain database (`wpdomain.db`).

As shown in the following example, the domain to which you are currently connected is indicated by a plug on the domain's icon. In addition, the connected domain is listed at the bottom of the ConsoleOne window.



To change the domain to which you are connected:

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > Select Domain*.



- 2 Browse to and select the domain directory, then click *OK* to connect to the domain.

You can also connect to a domain by right-clicking the domain in the GroupWise View and clicking *Connect*. However, in certain cross-platform situations, the Select Domain feature must be used to create the connection.

4.1.2 Understanding the Need for Domain Connections

Some administrative tasks require you to be connected to a specific domain but others do not. In general, operations that create new GroupWise container objects or delete GroupWise container objects require you to be connected to the domain where the object resides. Operations that add or delete leaf objects or modify the properties of an existing object do not require you to be connected to the object's domain.

In addition to eDirectory considerations, administrative tasks that require file system access to domain directories require direct connections.

- ♦ **Create Domain:** When you create a new domain, you must be attached to the primary domain and have direct access to the server where you want to create the new secondary domain so that ConsoleOne can create the new secondary domain database.
- ♦ **Rebuild Domain Database:** When you rebuild a secondary domain database, ConsoleOne needs direct access to the primary domain in order to rebuild the secondary domain database.
- ♦ **Sync Primary with Secondary:** If your primary domain becomes out of date for some reason, ConsoleOne requires direct access to the primary domain and a secondary domain in order to update the data in the primary domain database based on the data available in the secondary domain database.
- ♦ **Replace Primary with Secondary:** If you have structural problems with your primary domain database, ConsoleOne requires direct access to the primary domain and a secondary domain in order to reconstruct the primary domain database from the data available in the secondary domain database.
- ♦ **Merge/Release:** If you are combining or separating GroupWise systems, ConsoleOne requires direct access to the primary domain and a secondary domain that is being merged or released.

4.1.3 Handling Cross-Platform Domain Connections

How the write access between ConsoleOne and a domain database is achieved depends on the platform where you are running ConsoleOne and the platform where the domain is located.

ConsoleOne Platform	Domain Platform	Connection Options
Linux ConsoleOne	Linux server	Local directory Mounted file system where the mount point directory matches the domain directory on the mounted file system
	Windows server	Mounted file system where the mount point directory matches the Windows server hostname and share
Windows ConsoleOne	Linux server	Samba mount where the path to the domain on the Linux server is prefixed by the Linux server hostname from the point of view of ConsoleOne
	Windows server	Local drive Mapped drive

Instructions for mounting file systems and setting up Samba shares are provided in [Chapter 2, "ConsoleOne Administration Tool,"](#) on page 39.

The database location is stored internally in UNC path format (`\\server\volume\directory`) but is displayed on the Domain object Identification page in ConsoleOne based on the platform of ConsoleOne and the database location.

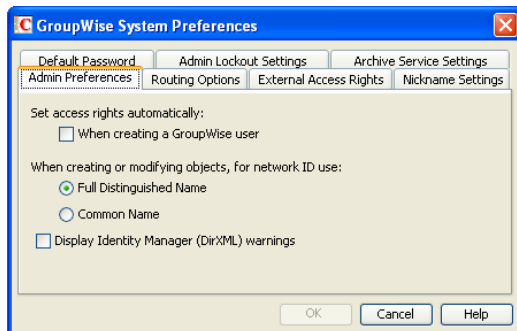
ConsoleOne Platform	Domain Platform	Database Location
Linux ConsoleOne	Linux server	<code>/domain_directory</code>
	Windows server	<code>/mnt/windows_server/share/domain_directory</code>
Windows ConsoleOne	Linux server	<code>\\linux_server\domain_directory</code>
	Windows server	<code>\\windows_server\share\domain_directory</code>

When you click *Connect* in the GroupWise View, ConsoleOne uses the domain's UNC path to automatically connect you to the correct domain if possible; otherwise, you must use the Select Domain feature to manually browse to and select the domain database in order to connect to the domain.

4.2 System Preferences

You can use the GroupWise system preferences to configure the defaults for various GroupWise system settings.

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > System Preferences*.



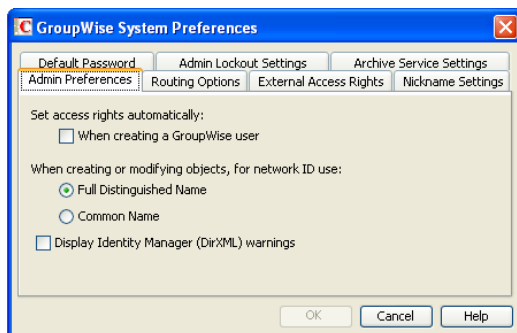
The GroupWise System Preferences dialog box contains the following tabs:

- ◆ **Admin Preferences:** Controls how rights are assigned and what network ID format is used when creating new GroupWise users. By default, rights are assigned automatically and the fully distinguished name format is used.
- ◆ **Routing Options:** Controls default message routing for your GroupWise system. By default, no routing domain is assigned.
- ◆ **External Access Rights:** Controls the access that users on external GroupWise systems have to your GroupWise users' information. By default, Busy Search and status tracking information is not returned to users on external GroupWise systems.
- ◆ **Nickname Settings:** Controls how addressing is handled after you move a user from one post office to another. By default, nicknames representing old addresses are not automatically created when users are moved.

- ♦ **Default Password:** Assigns a default password for new GroupWise user accounts. By default, you must manually assign a password for each GroupWise account you create.
 - ♦ **Admin Lockout Settings:** Controls access to the GroupWise administration functions in ConsoleOne. By default, there are no restrictions.
 - ♦ **Archive Service Settings:** Sets the default archive service for your GroupWise system. Archive services are third-party applications that can function as GroupWise trusted applications, such as [Messaging Architects M+Archive Email Archiving Software](http://www.messagingarchitects.com/products/m-archive-email-archiving.html) (<http://www.messagingarchitects.com/products/m-archive-email-archiving.html>). When you install an archive service to a server, the archive service is added to the list of archive service trusted applications that displays in ConsoleOne.
 - ♦ **Linux Settings (Linux ConsoleOne Only):** Establishes the mount directory where ConsoleOne can find mounted file systems where domains and post offices are located.
- 2 Change the system preferences as needed.
 - 3 Click *OK* to save the changes.

4.2.1 Admin Preferences

- 1 In the [GroupWise System Preferences](#) dialog box, click the *Admin Preferences* tab to modify any of the following options:



Set Access Rights Automatically: Users require specific eDirectory and file system rights in order to use GroupWise (see [Chapter 89, “GroupWise User Rights,”](#) on page 1141). Select this option to automatically grant these rights when creating a GroupWise account for users.

Appropriate eDirectory object rights enable the GroupWise client to log in to the user’s post office without prompting the user for the post office location (IP address, UNC path, or mapped drive.)

Appropriate file system rights enable the GroupWise client to directly access the post office directory rather than use client/server access.

When Creating or Modifying Objects, For Network ID Use: Select *Full Distinguished Name* (for example, paul.engineering.ny) when users' mailboxes reside on a NetWare server and users have an eDirectory connection to the server where the post office resides.

Starting in GroupWise 2012, NetWare is no longer a supported GroupWise platform. However, Novell eDirectory is still required (version 8.7 or later). The supported versions of eDirectory use full distinguished names for network IDs.

Do not select *Common Name* (for example, paul).

Display Identity Manager (DirXML) Warnings: The Identity Manager Driver for GroupWise provides data integration between GroupWise users and groups in eDirectory. For example, you can have an email account automatically created as soon as an employee is hired. The same driver can also disable an email account when a user is no longer active.

If you are using the Identity Manager Driver for GroupWise, some GroupWise operations that you perform in ConsoleOne require you to take preliminary actions with the driver. For example, if you recover a deleted account, you need to stop the driver before recovering the account and restart it after the operation is complete.

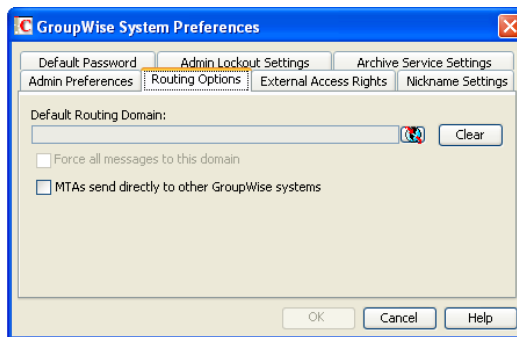
This option enables you to receive a warning message whenever you perform a GroupWise operation in ConsoleOne that is affected by the Identity Manager driver. The warning message includes instructions about the actions you need to take with the driver before continuing with the GroupWise operation. If you are using the Identity Manager Driver for GroupWise, we strongly recommend that you enable this option. If you are not using the driver, you can disable the option to avoid receiving unnecessary messages.

For more information, see “[GroupWise DirXML Driver for Novell Identity Manager](#)” in the *GroupWise 2012 Interoperability Guide*.

- 2 Click *OK* to save the changes.

4.2.2 Routing Options

- 1 In the [GroupWise System Preferences](#) dialog box, click the *Routing Options* tab to modify any of the following options:



Default Routing Domain: If a domain’s MTA cannot resolve a message’s address, the message is routed to this default domain’s MTA. The default domain’s MTA can then be configured to handle the undeliverable messages. This might involve routing the message to another GroupWise domain or to an Internet address (by performing a DNS lookup). Browse to and select the GroupWise domain you want to use as the default routing domain.

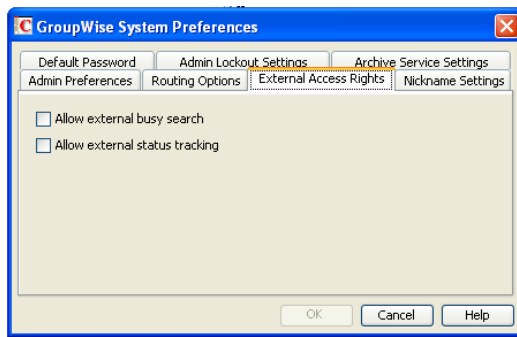
Force All Messages to this Domain: This option applies only if you select a default routing domain. Select this option to force all messages to be routed through the default routing domain regardless of the links you have configured for your GroupWise system’s domains.

MTAs Send Directly to Other GroupWise Systems: Select this option if you want all MTAs in your GroupWise system to perform DNS lookups and route messages out across the Internet. If you deselect this option, you can designate individual MTAs to perform DNS lookups and route messages to the Internet. For more information, see “[Using Dynamic Internet Links](#)” in “[Connecting to Other GroupWise Systems](#)” in the *GroupWise 2012 Multi-System Administration Guide*.

- 2 Click *OK* to save the changes.

4.2.3 External Access Rights

- 1 In the [GroupWise System Preferences](#) dialog box, click the *External Access Rights* tab to modify any of the following options:



Allow External Busy Search: Select this option to enable users in other GroupWise systems to perform Busy Searches on your GroupWise users' Calendars.

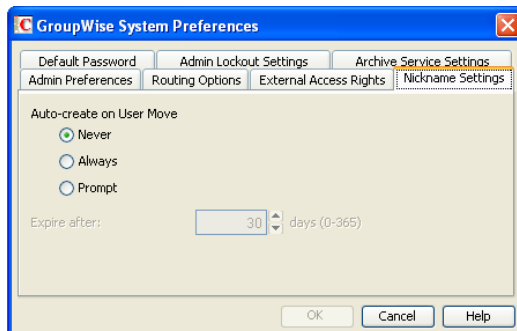
Allow External Status Tracking: Select this option to enable users in other GroupWise systems to receive message status information (such as whether a message has been delivered, opened, and so on) when messages arrive in your GroupWise system.

- 2 Click **OK** to save the changes.

4.2.4 Nickname Settings

A nickname is an additional GroupWise address that can be associated with a user, resource, or distribution list. For background information, see [Section 14.7.4, "Creating a Nickname for a User," on page 252](#).

- 1 In the [GroupWise System Preferences](#) dialog box, click the *Nickname Settings* tab to modify any of the following options:



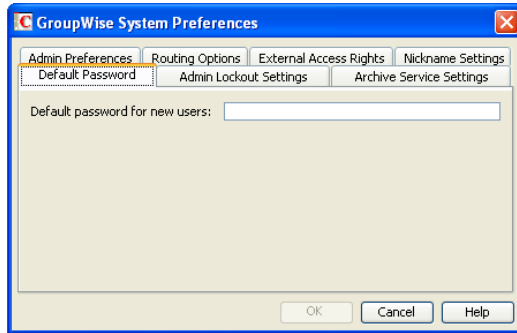
Auto-Create on User Move: Whenever you move a user, GroupWise can automatically create a nickname with the user's old post office. This enables messages sent to the old address to be automatically forwarded to the user's new address. Select whether or not you want GroupWise to never create nicknames, always create nicknames, or prompt you during the move process.

Expire After: This option applies only if you selected *Always* or *Prompt*. If you want the nickname to be automatically removed after a period of time, specify the time period (in days). Valid values range from 1 to 365 days. A setting of 0 indicates that the nickname will not be automatically removed.

- 2 Click **OK** to save the changes.

4.2.5 Default Password

- 1 In the **GroupWise System Preferences** dialog box, click the *Default Password* tab to modify any of the following options:

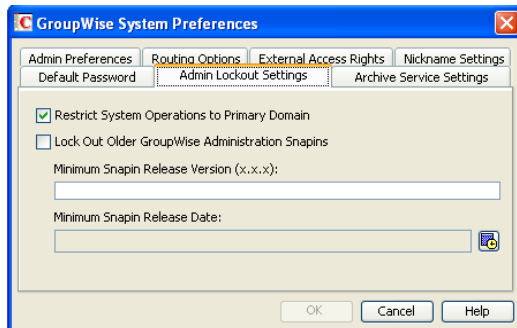


Default Password for New Users: Specify the default password you want assigned to new GroupWise user accounts.

- 2 Click *OK* to save the changes.

4.2.6 Admin Lockout Settings

- 1 In the **GroupWise System Preferences** dialog box, click the *Admin Lockout Settings* tab to modify any of the following options:



Restrict System Operations to Primary Domain: Disable this option to allow an administrator to perform system operations (*Tools > GroupWise System Operations*) when he or she is not connected to the primary domain. This option is enabled by default, which means that all operations except *Select Domain*, *Pending Operations*, *Software Directory Management*, and *Restore Area Management* are unavailable when connected to a secondary domain.

Lock Out Older GroupWise Administration Snap-Ins: Enable this option to prevent administrators from using older GroupWise ConsoleOne snap-ins for accessing GroupWise objects in eDirectory. You can override these system lockout settings for individual domains (Domain object > *GroupWise > Admin Lockout Settings*).

In versions of GroupWise earlier than 2012, there are four GroupWise snap-ins to ConsoleOne, one for general administration, one for Internet Agent (GWIA) administration, and two for WebAccess administration. In GroupWise 2012, WebAccess configuration information is no longer stored in eDirectory, so no WebAccess eDirectory objects are needed. The ability to lock out older GroupWise snap-ins starts with GroupWise 6.5.

In the *Minimum Snap-In Release Version (x.x.x)* field, specify the version number of the oldest GroupWise snap-ins that can be used to administer your GroupWise system.

In the *Minimum Snap-in Release Date* field, select the date of the oldest GroupWise snap-ins that can be used to administer your GroupWise system.

You can specify the minimum version, the minimum date, or both. If you specify both minimums, any administrator using snap-ins that are older than both minimums cannot use the GroupWise snap-ins. However, such an administrator can still run ConsoleOne for other purposes but must update the GroupWise snap-ins before GroupWise administration features are available again. Default admin lockout settings can be overridden on individual domains as needed.

The date for GroupWise 2012 is January 17, 2012.

IMPORTANT: The specified release version and release date affect the Identity Manager GroupWise Driver as well as the ConsoleOne snap-ins. If you are using Identity Manager with GroupWise, do not specify a release version or date that is newer than the release version and date of the Identity Manager GroupWise Driver that you are running.

- 2 Click *OK* to save the changes.

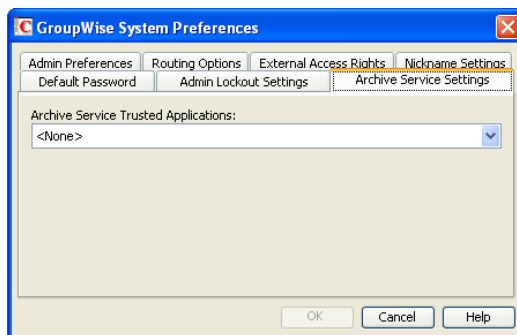
4.2.7 Archive Service Settings

When you use a message retention service with GroupWise, as described in [Chapter 33, “Retaining User Messages,” on page 441](#), you have the option of associating an archive service with the message retention service. The message retention service and its associated archive service must be set up as a GroupWise trusted application, as described in [Section 4.12, “Trusted Applications,” on page 90](#). Different archive services provide differing storage alternatives (memory, disk, or tape, for example) and differing alternatives for speed and cost. You can configure multiple archive services for your GroupWise system.

- ♦ [“Selecting the System Default Archive Service” on page 77](#)
- ♦ [“Overriding the System Default Archive Service” on page 78](#)

Selecting the System Default Archive Service

- 1 In the [GroupWise System Preferences](#) dialog box, click the *Archive Service Settings* tab to select the system default archive service for your GroupWise system.



Archive Service Trusted Applications: Lists the third-party archive services that are available to your GroupWise system as trusted applications.

Select the archive service that you want to use as the default for your GroupWise system. You can override the system default on individual post offices.

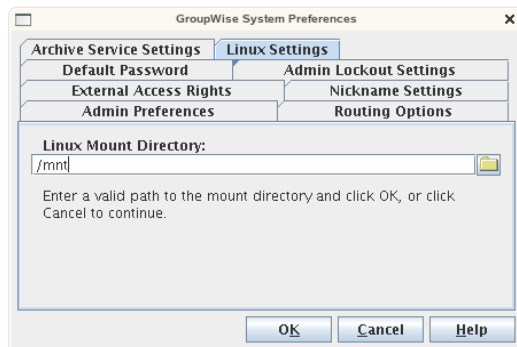
- 2 Click *OK* to save your selection.

Overriding the System Default Archive Service

- 1 Browse to and right-click the Post Office object where you want to override the default, then click *Properties*
- 2 Click *GroupWise > Post Office Settings*.
- 3 In the *Default Archive Service Trusted Application* field, select *Override*.
- 4 Select the archive service for that post office, then click *OK*.

4.2.8 Linux Settings (Linux ConsoleOne Only)

- 1 In the [GroupWise System Preferences](#) dialog box, on Linux, click the *Linux Settings* tab to specify the mount directory.



Mount Directory: Specify the mount directory where ConsoleOne can find mounted file systems where domains and post offices are located.

GroupWise databases can be located on Linux servers or Windows servers. In the Linux mount directory, you create directories that have the same names as the servers that are mounted to those mount points. You do this for each server where a domain or post office is located that you want to access from ConsoleOne. The following table illustrates the correspondence between UNC paths and mount point directories for GroupWise database locations on Linux and Windows, assuming the typical mount point directory of /mnt:

Platform	GroupWise Domain UNC Path	Corresponding Linux Mount Point
Linux	\\linux_server\gw_partition\domain_directory	/mnt/linux_server/ gw_partition
Windows	\\windows_server\gw_share\domain_directory	/mnt/windows_server/ gw_share

GroupWise administrators can have different mount points depending on the workstation or server where they are running ConsoleOne. The mount directory information is stored in a user-specific preferences file (.consoleone/SnapinPrefs.ser in each GroupWise administrator's home directory).

- 2 Click *OK* to save the changes.

4.3 eDirectory User Synchronization

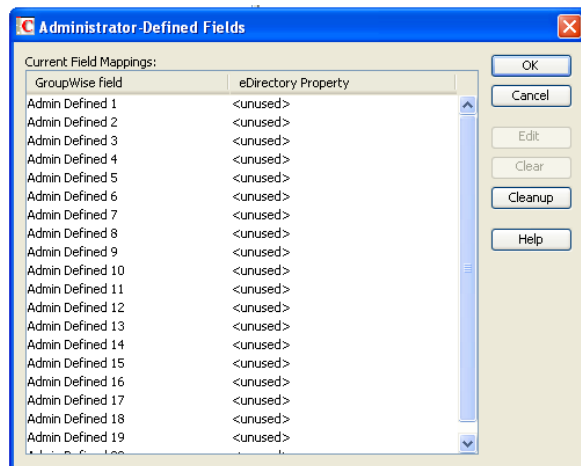
For user information to be displayed in the GroupWise Address Book, the information must be stored not only in eDirectory but also in the GroupWise domain and post office databases. If you add or modify user information using an installation of ConsoleOne with the GroupWise Administrator snap-in, the GroupWise Administrator snap-in adds the user information to the GroupWise databases. However, if you add or modify user information using a ConsoleOne installation that is not running the GroupWise Administrator snap-in, the user information is not changed in the GroupWise databases. This is also true if you add or modify user information using Novell iManager or older administration tools such as NetWare Administrator to manage a legacy GroupWise domain.

To ensure that the user information stored in the GroupWise databases is always synchronized with the user information in eDirectory, you can set up eDirectory user synchronization. For detailed information see [Section 42.4.1, “Using eDirectory User Synchronization,” on page 652](#).

4.4 Admin-Defined Fields

eDirectory includes user information that is not associated to GroupWise user fields. By default, such eDirectory fields are not displayed in the GroupWise Address Book. However, you can use the Admin-Defined Fields feature to map eDirectory user fields to GroupWise fields so that they can be displayed in the GroupWise Address Book.

- 1 Click *Tools > System Operations > Admin-Defined Fields*.



eDirectory fields that you associate with GroupWise fields here are available for use in all domains throughout your GroupWise system. You can also customize the GroupWise Address Book for individual domains, as described in [Section 6.1.1, “Adding eDirectory Fields to the Address Book,” on page 106](#)

- 2 Select the first available admin-defined field, then click *Edit*.
- 3 Select the eDirectory property that you want to associated with the admin-defined field, then click *OK*.
- 4 To remove an admin-defined field, select the field, then click *Clear*.

You are prompted for whether to remove the corresponding values from user records. This might be a time-consuming process.

- 5 Click *Yes* to clean up all obsolete references to deleted admin-defined fields in all user records.

or

Click *No* to perform the cleanup later.

At any time, you can click *Cleanup* to remove obsolete references to deleted admin-defined fields from all user records. It is a good practice to run *Cleanup* periodically to ensure that the admin-defined fields in ConsoleOne match the admin-defined fields that appear in user records.

4.5 Pending Operations

Pending operations are the results of administrative operations, such as adding GroupWise objects and modifying GroupWise object properties, that have not yet been permanently written to the appropriate GroupWise databases. While operations are pending, GroupWise data is not in a consistent state.

For example, you can maintain any domain's objects you have administrative rights over. However, because a secondary domain owns its own objects, any operation you perform from the primary domain on a secondary domain's objects must be validated by the secondary domain. While the operation is being validated, the Pending Operations dialog box displays object details and the pending operation.

While the operation is pending, the object is marked *Unsafe* in the primary domain database. The *Operation* field in the dialog box displays the pending operation. An unsafe object can have other operations performed on it, such as being added to a distribution list; however, the object record is not distributed to other domains and post offices in the system until it is marked *Safe*.

All pending operations require confirmation that the operation was either successfully performed or could not be performed. If the operation was successful, the pending operation is removed from the list, the record is marked in the database as *Safe*, and the record is distributed to all other domains and post offices in your system. If the operation could not be performed, the pending operation remains in the list where you can monitor and manage it.

- 1 In ConsoleOne, connect to the domain whose pending operations you want to view, as described in [Section 4.1, "Select Domain,"](#) on page 69.
- 2 Make sure the agents are running for the domain and/or post office where you are checking for pending operations
- 3 Click *Tools > GroupWise System Operations > Pending Operations*.
While an operation is being validated, the Pending Operations dialog box displays the object and the operation waiting completion and confirmation.
- 4 For more detailed information, select the pending operation, then click *View*.
- 5 If conditions on the network have changed so that a pending operation might now succeed, select the pending operation, then click *Retry*.
- 6 If you want to cancel a pending operation that has not yet taken place, select the pending operation, then click *Undo*.

4.6 Addressing Rules

You can use the Addressing Rules feature to configure GroupWise so that users can enter shortened forms of email addresses for use through GroupWise gateways.

NOTE: GroupWise gateways are legacy products that are not supported with the current GroupWise version.

4.7 Time Zones

When you create a domain or post office, you select the time zone in which it is located. This ensures that GroupWise users in other time zones receive Calendar events and tracking information adjusted for local time.

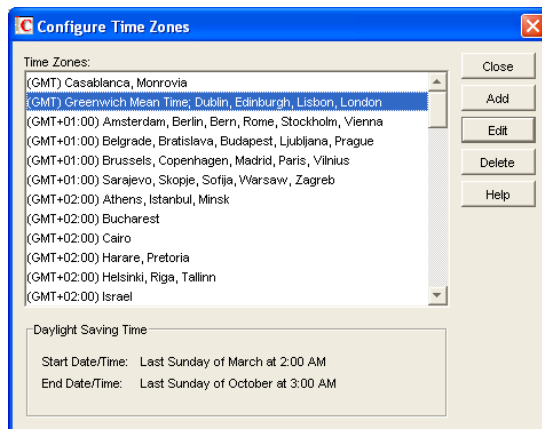
The time zone list includes predefined definitions for each time zone. Most time zones include multiple definitions to account for different locations within the time zone. Each time zone definition allows you to specify the Daylight Saving Time dates and bias (1 hour, 30 minutes, etc.).

You can modify existing time zone definitions, add new definitions, or delete definitions.

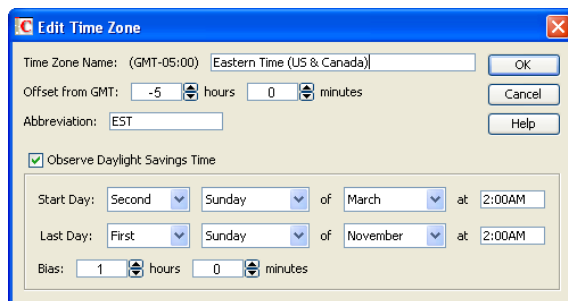
- ◆ [Section 4.7.1, “Modifying a Time Zone Definition,” on page 81](#)
- ◆ [Section 4.7.2, “Adding a Time Zone Definition,” on page 82](#)
- ◆ [Section 4.7.3, “Deleting a Time Zone Definition,” on page 83](#)

4.7.1 Modifying a Time Zone Definition

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > Time Zones*.



- 2 Select the time zone to modify, then click *Edit* to display the Edit Time Zone dialog box.



- 3 Modify any of the following fields:

Time Zone Name: Provide a name for the time zone definition (for example, some of the major cities in the time zone). We suggest you include a reference (+ or -) to GMT, for example (GMT-07:00). The time zone list is sorted by the GMT offset.

Offset from GMT: Specify the hours and minutes that the time zone is offset from Greenwich Mean Time. The offset from GMT keeps your different locations synchronized. For example, if a conference call is scheduled for 4:00 p.m. June 1 in Salt Lake City, the call would appear on a schedule in Adelaide at 8:30 a.m. June 2. If you are in the western hemisphere (west of the Greenwich Meridian and east of the International Date Line) be sure the hour offset is negative (-). If you are in the eastern hemisphere (east of the Greenwich meridian and west of the International Date Line) be sure the hour offset is positive.

Abbreviation: Specify an abbreviation for the time zone. For example, the abbreviation for Atlantic Standard Time could be AST; the abbreviation for Atlantic Daylight Time could be ADT.

Observe Daylight Saving Time: If the time zone observes daylight saving time, click the *Observe Daylight Saving Time* box, then fill out the remaining fields.

Start Day: Select the week, day, month, and hour daylight saving time starts.

Last Day: Select the week, day, month, and hour daylight saving time ends.

Bias: Enter the number of hours and minutes that the clock changes at the daylight saving time start day, such as 1 hour or 1 hour 30 minutes.

Example:

Start day: Second Sunday of March at 2:00 am.

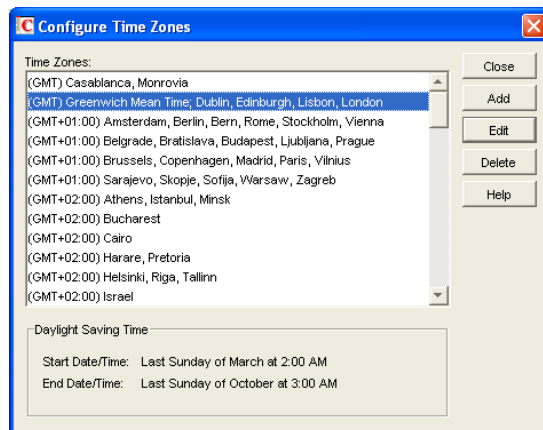
Last day: First Sunday of November at 2:00 am.

Bias: 1 hour 0 minutes

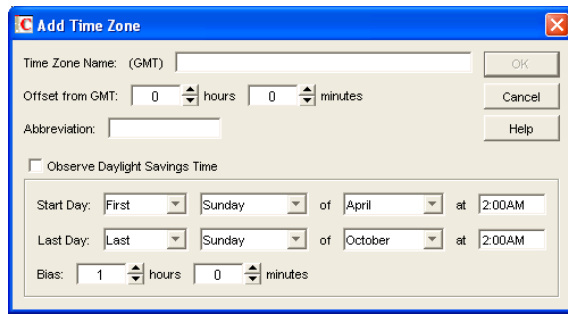
- 4 Click *OK* to save the changes.

4.7.2 Adding a Time Zone Definition

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > Time Zones*.



- 2 Click *Add* to display the Add Time Zone dialog box.



3 Fill in the following fields:

Time Zone Name: Provide a name for the time zone definition (for example, some of the major cities in the time zone). We suggest you include a reference (+ or -) to GMT, for example (GMT-07:00). The time zone list is sorted by the GMT offset.

Offset from GMT: Specify the hours and minutes that the time zone is offset from Greenwich Mean Time. The offset from GMT keeps your different locations synchronized. For example, if a conference call is scheduled for 4:00 p.m. June 1 in Salt Lake City, the call would appear on a schedule in Adelaide at 8:30 a.m. June 2. If you are in the western hemisphere (west of the Greenwich Meridian and east of the International Date Line) be sure the hour offset is negative (-). If you are in the eastern hemisphere (east of the Greenwich meridian and west of the International Date Line) be sure the hour offset is positive.

Abbreviation: Specify an abbreviation for the time zone. For example, the abbreviation for Atlantic Standard Time could be AST; the abbreviation for Atlantic Daylight Time could be ADT.

Observe Daylight Saving Time: If the time zone observes daylight saving time, click the *Observe Daylight Saving Time* box, then fill out the remaining fields:

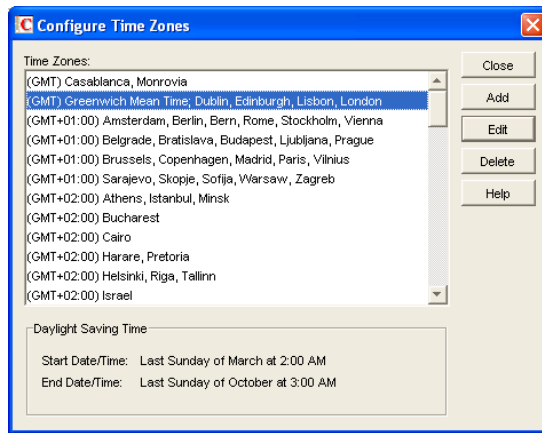
- ◆ **Start Day:** Select the day and time that daylight saving time starts.
- ◆ **Last Day:** Select the day and time that daylight saving time ends.
- ◆ **Bias:** Select the number of hours and minutes that the clock changes at the daylight saving time start day, such as 1 hour or 1 hour 30 minutes.

4 Click *OK* to add the definition to the time zone list.

4.7.3 Deleting a Time Zone Definition

When you delete a time zone from the list, you can no longer select it for a domain or post office.

- 1** In ConsoleOne, click *Tools > GroupWise System Operations > Time Zones*.



- 2 Select the time zone to remove from the list, click *Delete*, then click *Yes* to confirm the deletion.

4.8 External System Synchronization

The External System Synchronization feature lets you automatically synchronize information between your system and an external GroupWise system connected to your system. For information about connecting GroupWise systems and keeping information synchronized between them, see [“Connecting to Other GroupWise Systems”](#) in the *GroupWise 2012 Multi-System Administration Guide*.

4.9 Software Directory Management

The Software Directory Management feature lets you manage GroupWise software distribution directories. A software distribution directory is simply a copy or partial copy of the downloaded *GroupWise 2012* software image located on a network server. Diagrams of the contents of software distribution directories are provided in [“Directory Structure Diagrams”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*:

- ♦ [“Linux Software Distribution Directory”](#)
- ♦ [“Windows Software Distribution Directory”](#)

From this network location, you can distribute the GroupWise Windows client software to users or install additional GroupWise software such as the Message Transfer Agent, Post Office Agent, Internet Agent, WebAccess Application, Calendar Publishing Host Application, and Monitor.

When you install GroupWise, one software distribution directory is created automatically. Using Software Directory Management, you can create additional software distribution directories, update existing software distribution directories, or delete existing software distribution directories. A single software distribution directory can service multiple post offices and can contain software for multiple platforms.

- ♦ [Section 4.9.1, “Creating a Software Distribution Directory,”](#) on page 85
- ♦ [Section 4.9.2, “Updating a Software Distribution Directory,”](#) on page 87
- ♦ [Section 4.9.3, “Deleting a Software Distribution Directory,”](#) on page 88

4.9.1 Creating a Software Distribution Directory

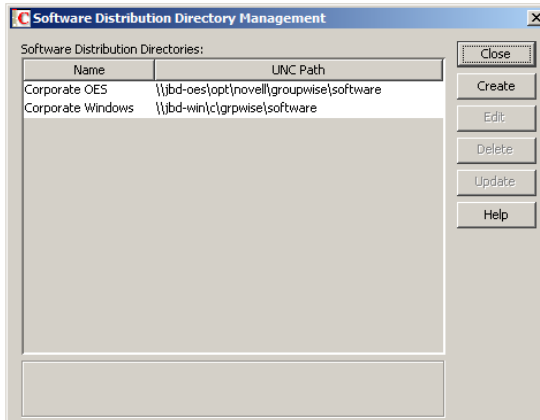
During installation on a Linux server, the initial software installation directory is created automatically in `/opt/novell/groupwise/software` and the GroupWise agent software is automatically copied there. You can select additional GroupWise software components to copy into the initial software distribution directory.

During installation on a Windows server, the default location for the software distribution directory is `c:\grpwise\software`, but you can change the location as needed. You can select any GroupWise software components to copy into the initial software distribution directory.

After installation, you can create additional software distribution directories on any servers where you want the GroupWise software to be easily accessible for future installations.

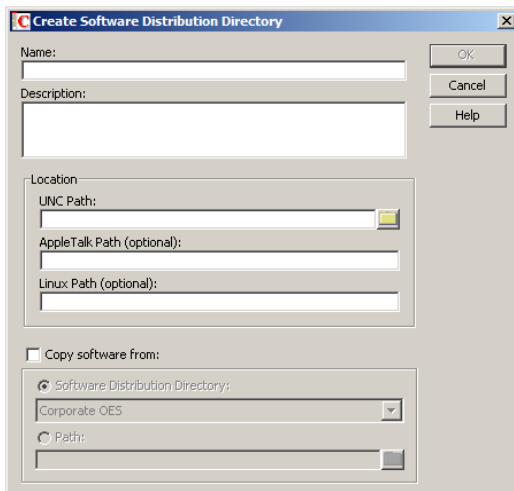
IMPORTANT: In general, for simplicity of administration in a multiple-platform environment, use Linux ConsoleOne to create and maintain software distribution directories on Linux servers. Use Windows ConsoleOne to create and maintain software distribution directories on Windows servers.

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > Software Directory Management* to display the Software Distribution Directory Management dialog box.



The *Software Distribution Directories* list includes all software distribution directories defined in your GroupWise system.

- 2 Click *Create* to display the Create Software Distribution Directory dialog box.



3 Fill in the following fields:

Name: Specify a name to identify the software distribution directory within your GroupWise system. For example, whenever you create a post office, you associate it with a software distribution directory. The software distribution directory's name, not its location, appears in the list of directories from which you can select. The name can include any characters; there are no restrictions.

Description: Specify an optional description for the software distribution directory. You might want to use this description to indicate the software version or to give other pertinent information.

Location: Specify the location where you want to create the new software distribution directory. If you specify a path to a directory that does not exist, ConsoleOne creates the directory for you.

Linux ConsoleOne: In the *UNC Path* field, specify the location where you want to create the new software distribution directory in UNC path format. Linux ConsoleOne automatically converts the UNC path format into a Linux path from the point of view where you are running ConsoleOne

The GroupWise Windows client software can be distributed from a Linux server rather than a Windows server, if the required cross-platform connection has been established, as described in [Section 77.1, "Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client," on page 1069](#). However, you must use Windows ConsoleOne in order to specify the UNC path as required to access the Windows client software, because Linux ConsoleOne converts the UNC path into a Linux path, which makes the Windows client software inaccessible from the point of view of Windows.

The AutoUpdate functionality does not apply to the GroupWise Linux client.

GroupWise Linux administration, agents, and applications can be installed on new Linux servers after the software has been distributed to those servers.

In the *Linux Path* field, specify the location of the software distribution directory as a Linux path from the point of view of the Linux POA that needs to access it. This is required when the software distribution directory is on a Linux server.

Windows ConsoleOne: In the *UNC Path* field, specify the location where you want to create the new software distribution directory in UNC path format. Do not use mapped drive format.

If you enable AutoUpdate, as described in [Section 77.1, "Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client," on page 1069](#), the GroupWise Windows client checks this location for software updates.

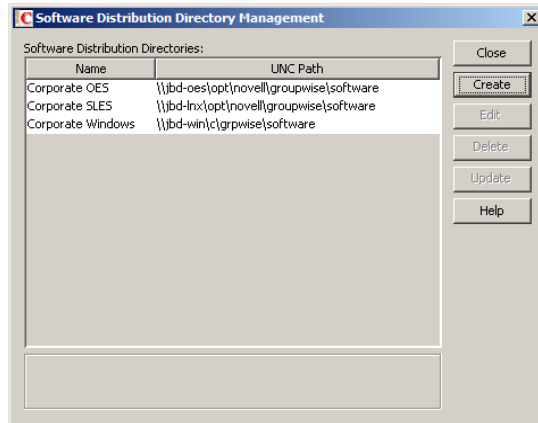
IMPORTANT: If the Windows client software is located in a software distribution directory on a Linux server, you must use Windows ConsoleOne in order to specify the UNC path to access the Windows client software. Linux ConsoleOne converts the UNC path into a Linux path, which makes the Windows client software inaccessible from the point of view of Windows.

GroupWise Windows administration, agents, and applications can be installed on new Windows servers after the software has been distributed to those servers.

Copy Software From: Select this option to copy GroupWise software from the existing location to the new location, then choose from the following source locations:

- ♦ **Software Distribution Directory:** If you want to copy software from an existing software distribution directory, select this option, then select the software distribution directory. All directories are copied.
- ♦ **Path:** If you want to copy software from a location that is not defined as a software distribution directory in your GroupWise system, such as the downloaded *GroupWise 2012* software image, select this option, then browse to and select the correct path.

- 4 Click *OK* to create the software distribution directory and add it to the list.



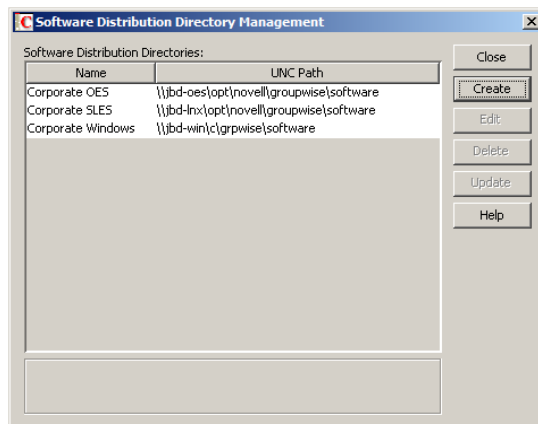
- 5 Click *Close* to exit the dialog box.

Each time it starts, the POA checks to make sure it can access the software distribution directory that is assigned to its post office. If it encounters a problem accessing its software distribution directory, the POA notifies you of the problem through the POA agent console and the POA log file. This helps ensure that each software distribution directory is always available.

4.9.2 Updating a Software Distribution Directory

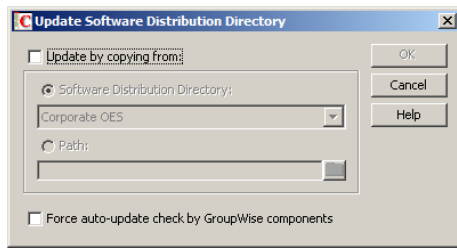
When you install updated GroupWise software, the installation process includes updating one software distribution directory. After installation, you use the Software Directory Management feature to copy the updated software to all other software distribution directories in your GroupWise system.

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > Software Directory Management* to display the Software Distribution Directory Management dialog box.



The *Software Distribution Directories* list includes all software distribution directories defined in your GroupWise system.

- 2 Select the software distribution directory to update, then click *Update* to display the Update Software Distribution Directory dialog box.



3 Fill in the following fields:

Update by Copying From: Select this option, then choose from the following source locations:

- ◆ **Software Distribution Directory:** If you want to copy updated software from an existing software distribution directory, select this option, then select the software distribution directory. All files and subdirectories are copied.
- ◆ **Path:** If you want to copy updated software from a location that is not defined as a software distribution directory in your GroupWise system, such as the downloaded *GroupWise 2012* software image, select this option, then browse for and select the correct path.

Force Auto-Update Check by GroupWise Components: This option causes the GroupWise Post Office Agent to check the software distribution directory for a new version of the GroupWise Windows client. If a new version is found, the next time a user starts the GroupWise Windows client, he or she is prompted to update the client software.

Select this option to automatically inform users whenever updated software is available.

Even if you do not select the *Update by Copying From* option, you can still select this option, then click *OK*. This forces an auto-update check of the client software version, but the software distribution directory's files are not updated.

To determine the current client software version in ConsoleOne, click *Tools > GroupWise Diagnostics > Record Enumerations* to display a list of record types in the domain database. From the drop-down list, select *Areas by ID*, select a software distribution directory, then click *Info* to list detailed information about the software distribution directory. Look at the *Software Version* field to determine the GroupWise client software version.

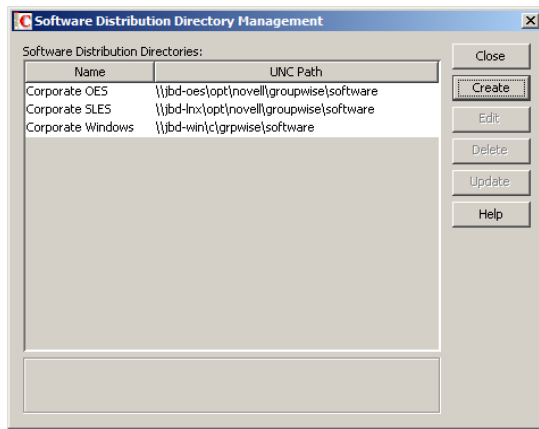
4 Click *OK* to update the directory's software.

4.9.3 Deleting a Software Distribution Directory

When you delete a software distribution directory, the directory is removed from the file system and no longer appears in the list of software distribution directories. You cannot delete a software distribution directory if any post offices are still configured to access it.

To delete a software distribution directory:

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > Software Directory Management* to display the Software Distribution Directory Management dialog box.



The *Software Distribution Directories* list includes all software distribution directories defined in your GroupWise system.

- 2 Select the directory to delete, click *Delete*, then click *Yes* to confirm the deletion.

4.10 Restore Area Management

A restore area is a location you designate to hold a backup copy of a post office so that you or GroupWise users can access it to retrieve mailbox items that are unavailable in your live GroupWise system. The Restore Area Management feature lets you manage your GroupWise system's restore areas.

Detailed information for using restore areas is provided in [Section 32.5, "Restoring Deleted Mailbox Items," on page 435](#). Information about backing up post offices is provided in [Section 31.2, "Backing Up a Post Office," on page 431](#).

4.11 Internet Addressing

By default, GroupWise uses a proprietary address format consisting of a user's ID, post office, and domain (*userID.post_office.domain*). After you install the GroupWise Internet Agent (GWIA), you can configure your GroupWise system to handle one or more formats of Internet email addresses. For setup instructions, see [Chapter 52, "Configuring Internet Addressing," on page 743](#).

4.12 Trusted Applications

Trusted applications are third-party programs that can log into Post Office Agents (POAs) and Internet Agents (GWIAs) in order to access GroupWise mailboxes without needing personal user passwords. Trusted applications might perform such services as message retention or synchronization with mobile devices. The Trusted Application feature allows you to edit and delete trusted applications that are available in your GroupWise system.

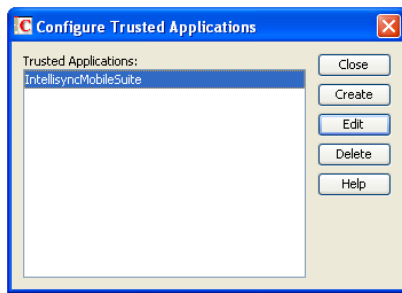
For information about creating and installing trusted applications, search for *GroupWise Trusted Application API* at the [Novell Developer Kit Web site \(http://developer.novell.com/wiki/index.php/Category:Novell_Developer_Kit\)](http://developer.novell.com/wiki/index.php/Category:Novell_Developer_Kit). For security guidelines for managing trusted applications, see [Section 93.6, “Protecting Trusted Applications,” on page 1154](#)

- ♦ [Section 4.12.1, “Creating a Trusted Application and Key,” on page 90](#)
- ♦ [Section 4.12.2, “Editing a Trusted Application,” on page 92](#)
- ♦ [Section 4.12.3, “Deleting a Trusted Application,” on page 93](#)

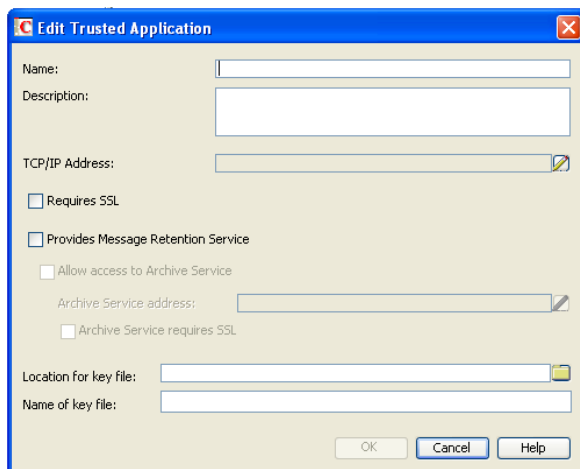
4.12.1 Creating a Trusted Application and Key

A trusted application key allows a third-party program to authenticate to the POA or the GWIA and obtain GroupWise information that would otherwise be available only by logging in to GroupWise mailboxes. You can create a trusted application and its associated key in ConsoleOne for use with both Linux and Windows trusted applications.

- 1 Click *Tools > GroupWise System Operations > Trusted Applications* to display the Configure Trusted Applications dialog box.



- 2 Click *Create*.



3 Fill in the following fields as needed for your trusted application:

Name: Specify the name of the trusted application as you want it to be listed in ConsoleOne.

Description: Specify a description for the trusted application.

TCP/IP Address: If you want to restrict the location from which the trusted application can run, specify the IP address of the server from which the application can run. To do so, click the *Edit* (pencil) button, then specify the IP address or DNS hostname of the trusted application's server.

If you want to allow the trusted application to be run from any server, do not specify an IP address or DNS hostname.

IMPORTANT: If you are creating the trusted application for use with the Data Synchronizer Connector for GroupWise, as described in "GroupWise Trusted Application" in "Mobility Pack Installation" in the *Mobility Pack Installation Guide*, do not specify an IP address or DNS hostname.

Requires SSL: Select this option to require a secure (SSL) connection between the trusted application and POAs and GWIAs.

Provides Message Retention Service: Select this option if the purpose of the trusted application is to retain GroupWise user messages by copying them from GroupWise mailboxes into another storage medium.

Turning on this option defines the trusted application as a Message Retention Service application. However, in order for GroupWise mailboxes to support message retention, you must also turn on the *Enable Message Retention Service* option in GroupWise Client Options (*Tools > GroupWise Utilities > Client Options > Environment > Retention*). You can enable individual mailboxes, all mailboxes in a post office, or all mailboxes in a domain by selecting the appropriate object (User, Post Office, or Domain) before selecting *Client Options*. For more information, see [Chapter 76, "Setting Defaults for the GroupWise Client Options," on page 1025](#).

For information about the complete process required to use a trusted application for message retention, see [Chapter 33, "Retaining User Messages," on page 441](#).

Allow Access to Archive Service: Select this option if your message retention service interacts with an archive service. Different archive services provide differing storage alternatives (memory, disk, or tape, for example) and differing alternatives for speed and cost. You can configure multiple archive services for your GroupWise system.

For more information about configuring GroupWise to work with an archive service, see [Section 4.2.7, "Archive Service Settings," on page 77](#).

Archive Service Address: If the trusted application for the message retention service uses the [GroupWise Stubbing API](http://developer.novell.com/wiki/index.php/GroupWise_Stubbing) (http://developer.novell.com/wiki/index.php/GroupWise_Stubbing), specify the IP address or DNS hostname of the server where the archive service is running. This allows the POA to interact directly with the archive service in support of the message retention service. The advantage to this configuration is that the archive service can be behind the firewall along with the POA. If retrieval is required, the POA accesses the archive service and provides the retrieved data to the GroupWise client.

If the message retention trusted application does not use the GroupWise Stubbing API, do not specify an IP address or DNS hostname. Without the Stubbing API, the trusted application communicates with the POA to create stubs for archived messages. The stubs contain the URLs for the archived messages. When a GroupWise user clicks the stub for an archived message, the GroupWise client accesses the URL to retrieve the archived message.

Archive Service Requires SSL: Select this option if you want to use a secure connection between the message retention service and the archive service.

Location for Key File: Browse to and select the directory where you want to create the trusted application key file.

Name of Key File: Specify the name of the trusted application key file to create. The third-party program must be designed to successfully access the trusted application key file where you create it.

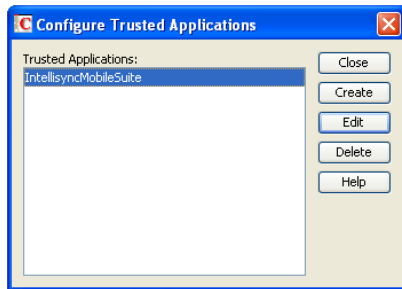
- 4 Click *OK* to save the trusted application configuration information.

For information about how the POA handles trusted application processing of message files, see [Section 36.3.6, “Configuring Trusted Application Support,” on page 517.](#)

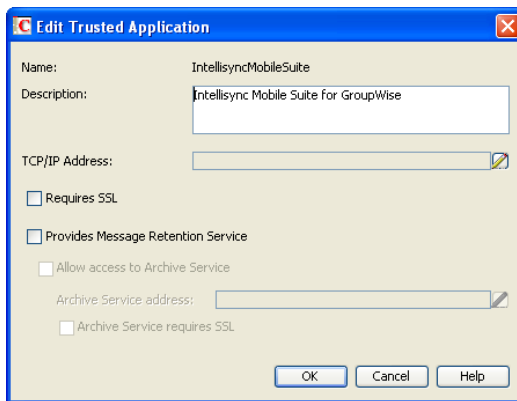
4.12.2 Editing a Trusted Application

You can edit a trusted application’s description, IP address, port, and SSL settings.

- 1 Click *Tools > GroupWise System Operations > Trusted Applications* to display the Configure Trusted Applications dialog box.



- 2 In the *Trusted Applications* list, select the application you want to edit, then click *Edit*.



- 3 Modify the following fields as needed for your trusted application:

Name: This field displays the trusted application’s name. You cannot change the name.

Description: Specify a description for the trusted application.

TCP/IP Address: If you want to restrict the location from which the trusted application can run, specify the IP address of the server from which the application can run. To do so, click the *Edit* (pencil) button, then specify the IP address or DNS hostname of the trusted application’s server.

If you want to allow the trusted application to be run from any server, do not specify an IP address or DNS hostname.

Requires SSL: Select this option to require a secure (SSL) connection between the trusted application and POAs and GWIAs.

Provides Message Retention Service: Select this option if the purpose of the trusted application is to retain GroupWise user messages by copying them from GroupWise mailboxes into another storage medium.

Turning on this option defines the trusted application as a Message Retention Service application. However, in order for GroupWise mailboxes to support message retention, you must also turn on the *Enable Message Retention Service* option in GroupWise Client Options (*Tools > GroupWise Utilities > Client Options > Environment > Retention*). You can enable individual mailboxes, all mailboxes in a post office, or all mailboxes in a domain by selecting the appropriate object (User, Post Office, or Domain) before selecting *Client Options*. For more information, see [Chapter 76, “Setting Defaults for the GroupWise Client Options,” on page 1025](#).

For information about the complete process required to use a trusted application for message retention, see [Chapter 33, “Retaining User Messages,” on page 441](#).

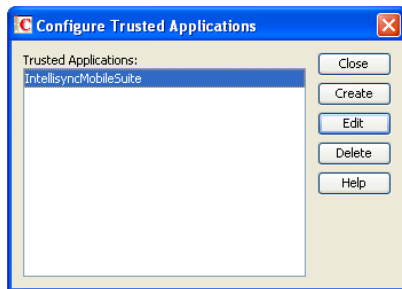
Allow Access to Archive Service: Select this option if you have also installed an archive service, as described in [Section 4.2.7, “Archive Service Settings,” on page 77](#). Specify the IP address or DNS hostname of the server where the archive service is running. Select *Archive Service Requires SSL* if you want to use a secure connection between the message retention service and the archive service.

- 4 Click *OK* to save the trusted application configuration information.

For information about how the POA handles trusted application processing of message files, see [Section 36.3.6, “Configuring Trusted Application Support,” on page 517](#).

4.12.3 Deleting a Trusted Application

- 1 Click *Tools > GroupWise System Operations > Trusted Applications* to display the Configure Trusted Applications dialog box.



- 2 In the *Trusted Applications* list, select the application you want to delete, click *Delete*, then click *Yes* to confirm the deletion.

4.13 LDAP Servers

The LDAP Servers feature lets you define the LDAP servers you want to use for LDAP authentication to GroupWise mailboxes. For setup instructions, see [“Providing LDAP Authentication for GroupWise Users” on page 510](#).

4.14 Global Signatures

You can build a list of globally available signatures that can be automatically appended to messages sent by GroupWise client users. The global signature is appended to messages after any personal signatures that users create for themselves. For setup instructions, see [Section 14.3, "Adding a Global Signature to Users' Messages,"](#) on page 231.

5 GroupWise Utilities

The GroupWise utilities in ConsoleOne are used to perform various maintenance and configuration tasks for your GroupWise system. The following sections provide information about the system utilities included on the *Tools* menu (*Tools > GroupWise System Utilities*):

- ♦ [Section 5.1, “Mailbox/Library Maintenance,” on page 95](#)
- ♦ [Section 5.2, “System Maintenance,” on page 96](#)
- ♦ [Section 5.3, “Backup/Restore Mailbox,” on page 96](#)
- ♦ [Section 5.4, “Recover Deleted Account,” on page 96](#)
- ♦ [Section 5.5, “Client Options,” on page 96](#)
- ♦ [Section 5.6, “Expired Records,” on page 96](#)
- ♦ [Section 5.7, “Email Address Lookup,” on page 96](#)
- ♦ [Section 5.8, “Synchronize,” on page 97](#)
- ♦ [Section 5.9, “User Move Status,” on page 97](#)
- ♦ [Section 5.10, “Link Configuration,” on page 97](#)
- ♦ [Section 5.11, “Document Properties Maintenance,” on page 97](#)
- ♦ [Section 5.12, “New System,” on page 98](#)
- ♦ [Section 5.13, “Check eDirectory Schema,” on page 98](#)
- ♦ [Section 5.14, “Gateway Alias Migration,” on page 98](#)
- ♦ [Section 5.15, “GW / eDirectory Association,” on page 99](#)
- ♦ [Section 5.16, “Standalone GroupWise Utilities,” on page 103](#)

In addition to the system utilities included on the *Tools* menu in ConsoleOne, GroupWise includes the following standalone utilities:

- ♦ [GroupWise Check Utility \(GWCheck\)](#)
- ♦ [GroupWise Backup Time Stamp Utility \(GWTMSTMP\)](#)
- ♦ [GroupWise Database Copy Utility \(DBCOPY\)](#)
- ♦ [GroupWise Generate CSR Utility \(GWCSRGEN\)](#)

5.1 Mailbox/Library Maintenance

You can use the Mailbox/Library Maintenance utility to check the integrity of and repair user/resource, message, and library databases, and to free disk space in post offices.

For detailed information and instructions, see [Chapter 27, “Maintaining User/Resource and Message Databases,” on page 409](#), [Chapter 28, “Maintaining Library Databases and Documents,” on page 415](#), and [Chapter 30, “Managing Database Disk Space,” on page 423](#).

5.2 System Maintenance

You can use the System Maintenance utility to check the integrity of and repair domain and post office databases.

For detailed information and instructions, see [Chapter 26, “Maintaining Domain and Post Office Databases,”](#) on page 401.

5.3 Backup/Restore Mailbox

You can use the Backup/Restore Mailbox utility to restore an individual user’s Mailbox items from a backup copy of the post office database.

For detailed information and instructions, see [Chapter 31, “Backing Up GroupWise Databases,”](#) on page 431 and [Chapter 32, “Restoring GroupWise Databases from Backup,”](#) on page 433.

5.4 Recover Deleted Account

If you have a reliable backup procedure in place, you can use the Recover Deleted Account utility to restore recently deleted user and resource accounts from the backup version of the GroupWise primary domain database. After the account has been re-created, you can then restore the corresponding mailbox and its contents to complete the process. Membership in distribution lists and ownership of resources must be manually re-established.

For complete instructions, see [Section 32.6, “Recovering Deleted GroupWise Accounts,”](#) on page 438.

5.5 Client Options

You can use the Client Options utility to set the default options (preferences) for the GroupWise client. You can set options at the domain, post office, or user level. Options set at the domain level apply to all users in the domain, and options set at the post office level apply to all users in the post office. If you don’t want users to change options, you can lock the options.

For detailed information and instructions, see [Chapter 76, “Setting Defaults for the GroupWise Client Options,”](#) on page 1025.

5.6 Expired Records

You can use the Expired Records utility to view and manage the GroupWise user accounts that have an expiration date assigned to them.

For detailed information and instructions, see [Chapter 14.11, “Removing GroupWise Accounts,”](#) on page 255.

5.7 Email Address Lookup

You can use the Email Address Lookup utility to search for the GroupWise object (User, Resource, Distribution List) that an email address is associated with. You can then view the object’s information. For more information, see [Section 14.7.1, “Ensuring Unique Email Addresses,”](#) on page 248.

5.8 Synchronize

GroupWise automatically replicates information (domain, post office, user, resource, and so on) to all domain and post office databases throughout your GroupWise system. This ensures that the information in each database is synchronized.

Situations might occur, however, that result in information not being replicated to all domain and post office databases. If you think that some information has not been replicated correctly, you can cause the information to be replicated again so that it becomes synchronized throughout your entire GroupWise system. For example, if you notice that a user's information is incorrect in the Address Book, you can synchronize that user's eDirectory User object so that his or her information is replicated to all domain and post office databases again.

For detailed information and instructions, see [Chapter 29, "Synchronizing Database Information," on page 419](#).

5.9 User Move Status

You can use the User Move Status utility to track progress as you move users from one post office to another. Using the User Move Status utility, you can:

- ◆ List users that are currently being moved and filter the list by domain, post office, and object.
- ◆ View the current status of the move for each object and see any errors that have occurred.
- ◆ Immediately retry a move where some of the information on the user inventory list failed to arrive at the destination post office. By default, the POA retries automatically every 12 hours for seven days to move all the information included on the user inventory list.
- ◆ Stop the POA from continuing its automatic retries.
- ◆ Restart (from the beginning) a move that has stopped before successful completion.
- ◆ Refresh the list to display current move status and clear completed moves from the list.

For more information, see [Section 14.4.5, "Monitoring User Move Status," on page 240](#).

5.10 Link Configuration

GroupWise domains and post offices must be properly linked in order for messages to flow throughout your GroupWise system. You can use the Link Configuration utility to ensure that your domains and post offices are properly linked and to optimize the links if necessary. For detailed information and instructions, see [Chapter 10, "Managing the Links between Domains and Post Offices," on page 155](#).

5.11 Document Properties Maintenance

Each document stored in the GroupWise Document Management Services (DMS) has properties associated with it. These properties identify the document, determine its disposition (archive, delete, keep), set its level of security, and provide information for locating it in searches. Certain document properties are standard in GroupWise. You can also customize DMS for your organization by defining additional properties. For detailed information and instructions, see [Section 23.2.1, "Customizing Document Properties," on page 362](#).

NOTE: On Linux, Document Properties Maintenance is not available in ConsoleOne.

5.12 New System

You can use the New System utility to create a new GroupWise system.

The process for creating a new GroupWise system is similar to the process of creating your initial GroupWise system (see “[Installing a Basic GroupWise System](#)” in the *GroupWise 2012 Installation Guide*), except that you don’t install the software from the downloaded *GroupWise 2012* software image. Instead, during creation of the new system, you are asked to specify an existing software distribution directory to use in the new system. If you don’t want to share software distribution directories between systems, you should create a new distribution directory. For information about creating software distribution directories, see [Section 4.9, “Software Directory Management,” on page 84](#).

5.13 Check eDirectory Schema

GroupWise systems include GroupWise-specific objects that are not available in eDirectory until the eDirectory schema for the tree has been extended for these objects. Schema extension takes place automatically when you create a GroupWise system using the GroupWise Setup Advisor. You can check an eDirectory tree to determine whether its schema has been extended for GroupWise.

- 1 In ConsoleOne, select a tree to check.
- 2 Click *Tools > GroupWise Utilities > Check eDirectory Schema*.
If the eDirectory tree has not yet been extended for GroupWise, the eDirectory Schema Extension dialog box lists the changes that are required for GroupWise.
- 3 Click *Yes* to extend the schema for GroupWise so that you can create GroupWise objects in the selected tree.
or
Click *No* if you decide you do not want to be able to create GroupWise objects in the selected tree.

If the schema of the tree has already been extended for GroupWise objects, a message notifies you of this and you can immediately create new GroupWise objects in the selected tree.

5.14 Gateway Alias Migration

If you have been using SMTP gateway aliases to handle email addresses that do not fit the default format expected by the Internet Agent (GWIA) or to customize users’ Internet addresses, the Gateway Alias Migration utility can convert the user names in those gateway aliases into preferred email IDs. The Preferred E-Mail ID feature was first introduced in GroupWise 6.5 and is the suggested method for overriding the current email address format, as described in [Section 14.7.2, “Changing a User’s Internet Addressing Settings,” on page 249](#). The Gateway Alias Migration utility can also update users’ preferred Internet domain names based on their existing gateway aliases.

For usage instructions, see [Section 52.3, “Transitioning from SMTP Gateway Aliases to Internet Addressing,” on page 754](#).

5.15 GW / eDirectory Association

The GW / eDirectory Association menu includes the following options:

- ♦ [Section 5.15.1, “Graft GroupWise Objects,”](#) on page 99
- ♦ [Section 5.15.2, “Invalid Associations,”](#) on page 100
- ♦ [Section 5.15.3, “Associate Objects,”](#) on page 101
- ♦ [Section 5.15.4, “Disassociate GroupWise Attributes,”](#) on page 102
- ♦ [Section 5.15.5, “Convert External Entity to User,”](#) on page 102
- ♦ [Section 5.15.6, “Convert User to External Entity,”](#) on page 103

5.15.1 Graft GroupWise Objects

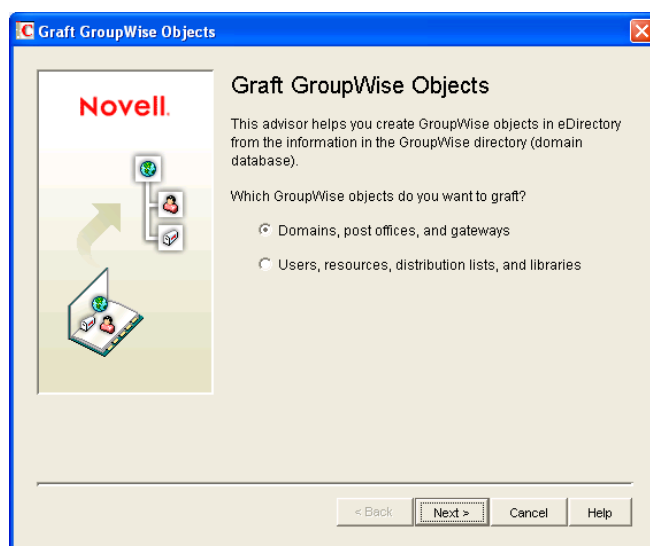
You can use the Graft GroupWise Objects utility to create GroupWise objects in the eDirectory tree from the information in your GroupWise domain database. The utility creates Domain, Post Office, and Gateway objects as well as User, Resource, and Distribution List objects. When grafting GroupWise user information from the GroupWise database into eDirectory, you can match the GroupWise user information to an existing User object, or you can create a new GroupWise External Entity object and convert it into an eDirectory User object, as described in [Section 5.15.5, “Convert External Entity to User,”](#) on page 102.

Grafting GroupWise objects from the GroupWise database into eDirectory can be useful in the following situations:

- ♦ The GroupWise database includes information that is not included in eDirectory.
- ♦ You want to move GroupWise information (domains, post offices, gateways, users, or resources) from one eDirectory tree to another.

To graft GroupWise objects:

- 1 In ConsoleOne, select a container in the eDirectory view.
- 2 Click *Tools > GroupWise Utilities > GW / eDirectory Associations > Graft GroupWise Object* to display the Graft GroupWise Objects dialog box.



- 3 Follow the on-screen prompts. If you need information about a dialog box, click the *Help* button.

5.15.2 Invalid Associations

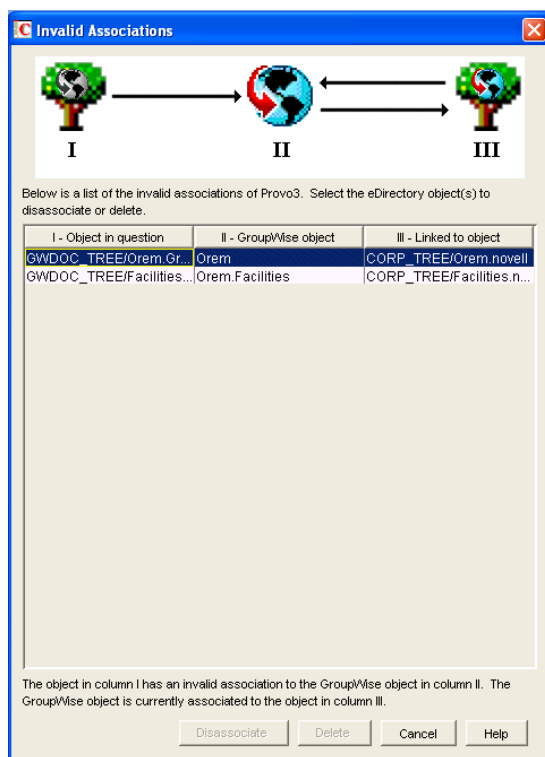
Normally, a GroupWise object in eDirectory points to corresponding information in the GroupWise domain database. In turn, the information in the GroupWise domain database points back to its corresponding object in eDirectory.

Occasionally, a situation might arise where information in the GroupWise domain database no longer points to the same eDirectory object that points to it. This results in an invalid association between the information in the two directories.

You can use the Invalid Associations utility to correct invalid associations between information in the GroupWise domain database and eDirectory.

To check for invalid associations:

- 1 In the eDirectory View in ConsoleOne, select the container whose objects you want to check for invalid associations (for example, an Organization, Organizational Unit, Domain, or Post Office).
- 2 Click *Tools > GroupWise Utilities > GW / eDirectory Associations > Invalid Associations* to display the Invalid Associations dialog box.



The dialog box lists each invalid association for the objects in the selected container. The dialog box fields are described below:

- ♦ **Object in Question (Column I):** This field lists the eDirectory object that has an invalid association to a GroupWise object. The eDirectory object points to the GroupWise object listed in Column II, but the GroupWise object, according to the GroupWise domain database, does not point back to the eDirectory object.
- ♦ **GroupWise Object (Column II):** This field lists the GroupWise object to which the eDirectory object listed in Column I is associated.

- ♦ **Linked to Object (Column III):** This field lists the eDirectory object to which the GroupWise object listed in Column II has a valid association.
- 3 To remove the invalid association by disassociating the eDirectory object in Column I with the GroupWise object in Column II, select the association, then click *Disassociate*.
 - 4 To remove the invalid association by deleting the eDirectory object listed in Column I, select the association, then click *Delete*.

5.15.3 Associate Objects

You can use the Associate Objects utility to associate GroupWise information with an eDirectory object.

For example, if you delete a user's eDirectory account but not his or her GroupWise account, the user's GroupWise information is retained as a GroupWise External User object in the GroupWise database and can be viewed in the GroupWise View. You can then associate the GroupWise External User object with another eDirectory User object. In essence, you are moving the GroupWise information from one eDirectory User object to another.

In some circumstances, it is possible for the link between an eDirectory User object and its GroupWise information to be lost. If this occurs, the GroupWise information, which still exists in the GroupWise database, appears as a GroupWise External User object in the GroupWise View. You can use the Associate Objects utility to reassociate the GroupWise information with the eDirectory User object.

The Associate Objects utility can be used to associate the following objects:

- ♦ GroupWise User or External User objects with eDirectory User objects
- ♦ GroupWise External Entity objects with eDirectory External Entity objects

Associating GroupWise User or External User Objects with eDirectory User Objects

- 1 In the GroupWise View in ConsoleOne, select the GroupWise User or External User object you want.

or

In the eDirectory View, select the eDirectory User object you want.

- 2 Click *Tools > GroupWise Utilities > GW / eDirectory Associations > Associate Objects*.

- 3 If you selected a GroupWise User or External User object in [Step 1](#), select the eDirectory User object you want to associate with it.

or

If you selected an eDirectory User object in [Step 1](#), select the GroupWise User object you want to associate with it.

- 4 Click *OK* to create the association.

If the eDirectory User object is already associated with another GroupWise object, you receive a warning message indicating this. If you continue, the eDirectory User object is associated with the selected GroupWise object and its association with the other GroupWise object is removed.

If the GroupWise User or External User object is already associated with another eDirectory User object, you receive a warning message indicating this. If you continue, the GroupWise User object is associated with the selected eDirectory object and its association with the other eDirectory object is removed.

Associating GroupWise External Entity Objects with eDirectory External Entity Objects

- 1 In the GroupWise View in ConsoleOne, select the GroupWise External Entity object you want.

or

In the eDirectory View, select the eDirectory External Entity object you want.

- 2 Click *Tools > GroupWise Utilities > GW / eDirectory Associations > Associate Objects*.

- 3 If you selected a GroupWise External Entity object in [Step 1](#), select the eDirectory External Entity object you want to associate with it.

or

If you selected an eDirectory External Entity object in [Step 1](#), select the GroupWise External Entity object you want to associate with it.

- 4 Click *OK* to create the association.

If the eDirectory External Entity object is already associated with another GroupWise object, you receive a warning message indicating this. If you continue, the eDirectory External Entity object is associated with the selected GroupWise object and its association with the other GroupWise object is removed.

If the GroupWise External Entity object is already associated with another eDirectory External Entity object, you receive a warning message indicating this. If you continue, the GroupWise External Entity object is associated with the selected eDirectory object and its association with the other eDirectory object is removed.

5.15.4 Disassociate GroupWise Attributes

You can use the Disassociate GroupWise Attributes utility to disassociate GroupWise information from an eDirectory User object. This results in two separate eDirectory objects:

- ♦ The User object, which no longer includes any GroupWise information.
- ♦ A GroupWise External User object, which represents the user's record in the GroupWise database and is displayed only in the GroupWise View. The External User object allows the user to continue to have access to GroupWise and also enables you to graft the user record to another eDirectory User object. For more information, see [Section 5.15.1, "Graft GroupWise Objects," on page 99](#).

To disassociate the GroupWise attributes from an eDirectory User object:

- 1 In ConsoleOne, select the User object whose GroupWise attributes you want to remove.
- 2 Click *Tools > GroupWise Utilities > GW / eDirectory Associations > Disassociate GroupWise Attributes*.

5.15.5 Convert External Entity to User

You can use the Convert External Entity to User utility to convert a GroupWise External Entity object to an eDirectory User object.

- 1 In ConsoleOne, select the GroupWise External Entity object that you want to convert to an eDirectory User object.
- 2 Click *Tools > GroupWise Utilities > GW / eDirectory Associations > Convert External Entity to User*.
- 3 Click *Yes* to confirm that you want the conversion performed.

5.15.6 Convert User to External Entity

You can use the Convert User to External Entity utility to convert a User object to a GroupWise External Entity object.

- 1 In ConsoleOne, select the User object that you want to convert to an GroupWise External Entity object.
- 2 Click *Tools > GroupWise Utilities > GW / eDirectory Associations > Convert User to External Entity*.
- 3 Click *Yes* to confirm that you want the conversion performed.

5.16 Standalone GroupWise Utilities

Although ConsoleOne provides the primary administrative tool for managing your GroupWise system, additional standalone utilities are provided to meet specialized needs. These utilities perform tasks that might be necessary in environments where ConsoleOne is not available.

- ♦ [Section 5.16.1, “GroupWise Check Utility \(GWCheck\),” on page 103](#)
- ♦ [Section 5.16.2, “GroupWise Backup Time Stamp Utility \(GWTMSTMP\),” on page 103](#)
- ♦ [Section 5.16.3, “GroupWise Database Copy Utility \(DBCOPY\),” on page 104](#)
- ♦ [Section 5.16.4, “GroupWise Generate CSR Utility \(GWCSRGEN\),” on page 104](#)

5.16.1 GroupWise Check Utility (GWCheck)

GroupWise Check is a standalone version of the ConsoleOne Mailbox/Library Maintenance utility. Like the Mailbox/Library Maintenance utility, GroupWise Check checks and repairs GroupWise user, message, library, and resource databases. However, in addition to checking post office, user, and library databases, it also checks users’ remote, caching, and archive databases.

For information about using GroupWise Check, see [Section 34.1, “GroupWise Check,” on page 447](#).

5.16.2 GroupWise Backup Time Stamp Utility (GWTMSTMP)

The GroupWise Backup Time Stamp utility (GWTMSTMP) can be used to place a time stamp on a GroupWise user database to indicate the last time the database was backed up. If a user deletes an item from his or her mailbox and purges it from the Trash, the item is only deleted from the user’s database if the time stamp shows that the item would have already been backed up. Otherwise, the item remains in the user’s database until the database is backed up, at which time it is deleted from the working database.

For information about using the GroupWise Backup Time Stamp utility, see [Section 34.2, “GroupWise Time Stamp Utility,” on page 457](#).

5.16.3 GroupWise Database Copy Utility (DBCOPY)

The GroupWise Database Copy utility (DBCOPY) copies files from a live GroupWise system to a static location for backup. During the copy process, DBCOPY prevents the files from being modified, using the same locking mechanism used by other GroupWise programs that access databases. This ensures that the backed-up versions are consistent with the originals even when large databases take a substantial amount of time to copy.

For information about using the GroupWise Database Copy utility, see [Section 34.3, “GroupWise Database Copy Utility,”](#) on page 463.

5.16.4 GroupWise Generate CSR Utility (GWCSRGEN)

To provide secure communication through an SSL (Secure Socket Layer) connection, the GroupWise Agents (MTA, POA, DVA, and GWIA) require access to a server certificate and private key.

You can use the GroupWise Generate CSR utility (GWCSRGEN) to generate a Certificate Signing Request (CSR) file and a Private Key file.

The CSR file, which is Base64 encoded, contains the information required for a Certificate Authority (CA) to issue you a server certificate. This server certificate, when paired with the private key generated by the GroupWise Generate CSR utility, enables GroupWise agents to use SSL connections.

For information about SSL and certificates, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107.

6 GroupWise Address Book

The GroupWise Address Book plays a central role in a GroupWise user's experience with addressing messages. The default configuration of the GroupWise Address Book is often sufficient for a typical GroupWise system, but a variety of customization options are available to enable the GroupWise Address Book to meet user needs.

- ♦ [Section 6.1, "Customizing Address Book Fields," on page 105](#)
- ♦ [Section 6.2, "Controlling Object Visibility," on page 110](#)
- ♦ [Section 6.3, "Updating Address Book Information," on page 110](#)
- ♦ [Section 6.4, "Controlling Users' Frequent Contacts Address Books," on page 111](#)
- ♦ [Section 6.5, "Controlling Address Book Synchronization for Caching and Remote Client Users," on page 112](#)
- ♦ [Section 6.6, "Publishing Email Addresses to eDirectory.," on page 113](#)
- ♦ [Section 6.7, "Enabling Wildcard Addressing," on page 114](#)
- ♦ [Section 6.8, "Adding External Users to the GroupWise Address Book," on page 116](#)

NOTE: In addition to the administrator-controlled changes you can make to the Address Book, GroupWise users can make individual changes such as creating personal address books, sharing personal address books, and accessing LDAP address books. For information about the Address Book functionality available to users, see:

- ♦ ["Contacts and Address Books" in the *GroupWise 2012 Windows Client User Guide*](#)
- ♦ ["Contacts and Address Books" in the *GroupWise 2012 WebAccess User Guide*](#)

Address books are not available in WebAccess Mobile.

6.1 Customizing Address Book Fields

The GroupWise clients displays specific fields in the GroupWise Address Book by default:

Windows Client	WebAccess
Name	Name
E-Mail Address	E-Mail Address
Title	
Office Phone Number	

NOTE: Address Book fields in GroupWise WebAccess are set permanently and cannot be changed by you or by users.

Windows client users can add more columns to their own Address Book. In the client, users right-click the Address Book column header, then select a column from the drop-down list or click *More Columns* to display a longer list of possible columns.

In ConsoleOne, you can add columns to the list that is displayed in the GroupWise clients when users click *More Columns*. This is configured at the domain level.

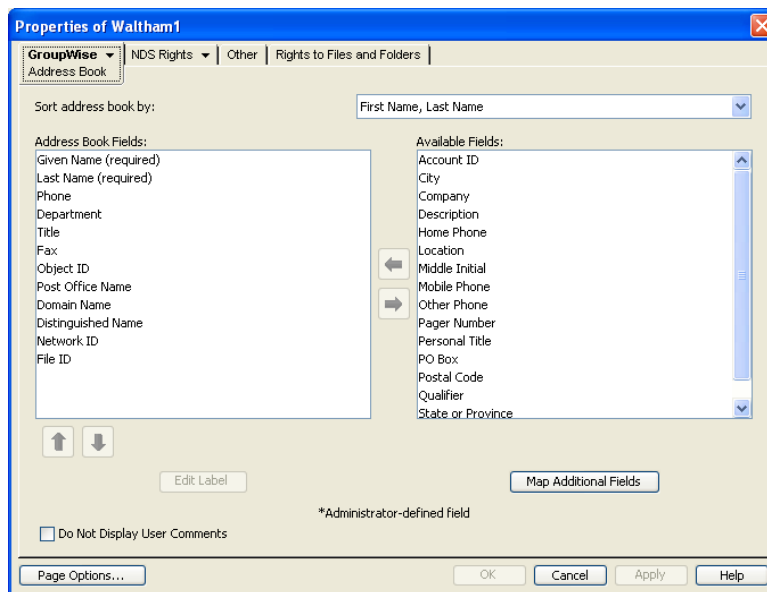
NOTE: The Address Book configuration you establish becomes the default configuration for new GroupWise users in the domain. Changes to Address Book configuration do not affect existing users.

- ♦ [Section 6.1.1, “Adding eDirectory Fields to the Address Book,” on page 106](#)
- ♦ [Section 6.1.2, “Adding LDAP Fields to the Address Book,” on page 107](#)
- ♦ [Section 6.1.3, “Changing the Default Sort Order,” on page 108](#)
- ♦ [Section 6.1.4, “Changing the Default Field Order,” on page 109](#)
- ♦ [Section 6.1.5, “Removing Fields from the Address Book,” on page 109](#)
- ♦ [Section 6.1.6, “Preventing the User Description Field from Displaying in the Address Book,” on page 109](#)

6.1.1 Adding eDirectory Fields to the Address Book

Adding an eDirectory field makes the field available in the GroupWise Address Book. Individual users can determine which available fields they want to display when they view the GroupWise Address Book in the GroupWise client.

- 1 In ConsoleOne, right-click the Domain object whose Address Book you want to modify, then click *Properties*.
- 2 Click *GroupWise > Address Book* to display the Address Book page.



The *Address Book Fields* list shows all fields that are available for selection in the Address Book in the GroupWise client.

The *Available Fields* list shows additional predefined GroupWise user fields that can be added to the Address Book. Novell eDirectory also includes user information that is not associated to GroupWise user fields. You can use the *Map Additional Fields* button to map eDirectory user fields to GroupWise fields so that they can be displayed in the GroupWise Address Book.

- 3 To add a field that is not displayed in the *Available Fields* list, click *Map Additional Fields*, select an unmapped Admin-defined field, click *Edit*, select the eDirectory property to map to the Admin-defined field, then click *OK* twice to add it to the *Available Fields* list.

To add fields independent of a specific domain's Address Book, use *Tools > GroupWise System Operations > Admin-Defined Fields* to display the Administrator-Defined Fields dialog box. The fields defined in this dialog box are available for selection and display in the Address Book belonging to any domain. For more information, see [Section 4.4, "Admin-Defined Fields," on page 79](#).

- 4 In the *Available Fields* list, select the field you want to make available in the Address Book, then click the left-arrow to move it to the Address Book Fields list.

The field is added to the bottom of the list. The Address Book displays the fields in the order they are listed.

- 5 If necessary, select the field, then use the up-arrow and down-arrow to move the field to the appropriate location in the list.
- 6 If the field is an Administrator-defined field and you want to change how the field is labeled in the Address Book, select the field, click *Edit Label*, specify a new label in the *Address Book Label field*, then click *OK*.

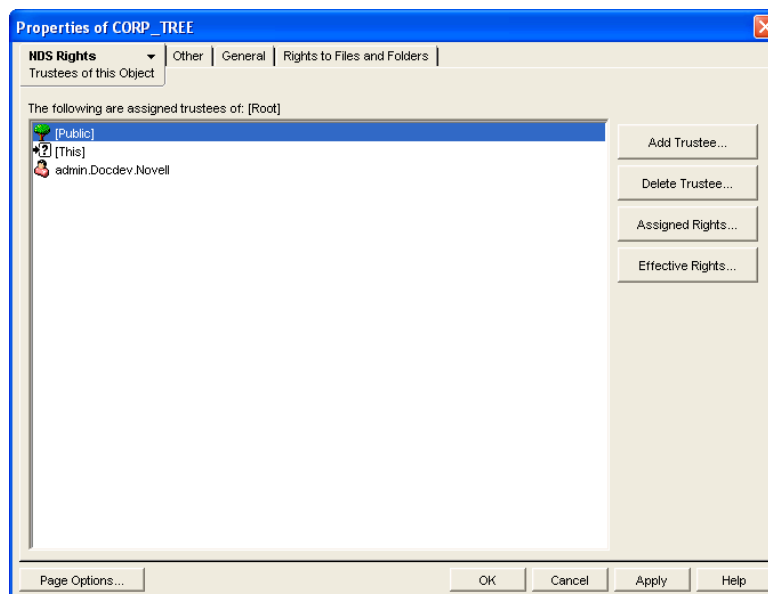
Administrator-defined fields are marked with an asterisk (*). You can only edit an Administrator-defined field that is in the Address Book Fields list.

- 7 When you are finished, click *OK* in the Address Book page to save your changes.

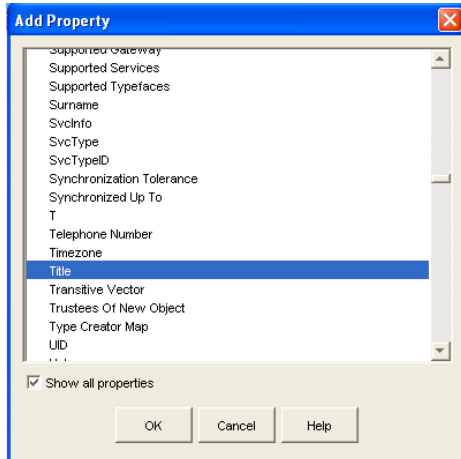
6.1.2 Adding LDAP Fields to the Address Book

A number of LDAP fields available in ConsoleOne are not listed on the Address Book property page of the Domain object. These LDAP fields can also be added to the GroupWise Address Book by making them visible in eDirectory.

- 1 In ConsoleOne, right-click your Tree object, then click *Properties*.

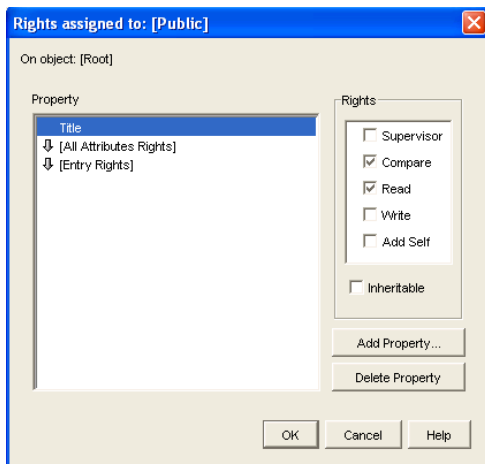


- 2 Select *Public*, click *Assigned Rights*, then click *Add Property*.



In the Add Property dialog box, all capitalized property names sort ahead of all uncapitalized property names.

- 3 Select *Show All Properties*, scroll down to locate the property you want to add to the GroupWise Address Book, select the property (for example, Title), then click *OK*.



- 4 With the new property highlighted, select *Inheritable*, then click *OK* twice to save the new property settings.

When you return to the Address Book property page of the Domain object, you can select the new property to display in the GroupWise Address Book, as described in [Section 6.1.1, “Adding eDirectory Fields to the Address Book,”](#) on page 106.

6.1.3 Changing the Default Sort Order

NOTE: The *Sort Address Book By* field on the Address Book page of the Domain object is obsolete and no longer affects Address Book sorting in the GroupWise clients.

The sort order determines whether addresses in the Address Book are sorted by first name or last name. The sort order you establish becomes the default for the Address Book and remains in effect until individual users change it.

The preset default sort order for the Address Book is First Name/Last Name. You can change the default sort order to Last Name/First Name.

On the [Address Book](#) page of the Domain object:

- 1 In the *Sort Address Book By* list, select the sort order you want to be the default.
- 2 Click *OK* to save your changes.

6.1.4 Changing the Default Field Order

The field order determines the order in which the GroupWise fields are displayed in the Address Book. The field order you establish becomes the default for the Address Book and remains in effect until individual users change the order.

On the [Address Book](#) page of the Domain object:

- 1 In the *Address Book Fields* list, select a field whose position you want to change, then use the up-arrow and down-arrow to move the field to its new position.
- 2 Repeat [Step 1](#) until you have established the field order you want.
- 3 Click *OK* to save your changes.

6.1.5 Removing Fields from the Address Book

If there are fields in the Address Book that are not used or that you don't want displayed to users, you can remove them.

On the [Address Book](#) page of the Domain object:

- 1 In the *Address Book Fields* list, select the field you want to remove, then click the right-arrow to move the field to the *Available Fields* list.

The fields in the *Available Fields* list are not displayed in the Address Book.

- 2 Repeat [Step 1](#) to remove additional fields you don't want to use.
- 3 Click *OK* to save your changes.

6.1.6 Preventing the User Description Field from Displaying in the Address Book

The GroupWise Address Book provides detailed user information as well as email addresses. A user's detailed information includes a comments field that displays the information stored in the User object *Description* field (User object > *General* > *Identification*). If you have included information in the *Description* field that you don't want displayed in the GroupWise Address Book, you can prevent the field's contents from being displayed.

TIP: To view a user's detailed information, including the comments field, in the Address Book, select the user's address, then click *View > Details*.

On the [Address Book](#) page of the Domain object:

- 1 Enable the *Do Not Display User Comments* option.
- 2 Click *OK* to save your changes.

6.2 Controlling Object Visibility

An object's visibility determines which post office databases the object's information is distributed to. A post office's users can only see an object's information in the Address Book if the object's information has been distributed to its post office.

Visibility applies to the following objects: user, external user, external entity, resource, external resource, distribution list, eDirectory group, eDirectory organizational role, and nickname.

IMPORTANT: Unlike the other objects listed above, nicknames that have been distributed to a post office do not actually appear in the post office's Address Book. Users must type the nickname's address in the message rather than select it from the Address Book.

You can choose from the following visibility levels:

- ♦ **System:** The object is visible in every post office Address Book throughout the system; if external system synchronization is turned on, it is also available for distribution to other GroupWise systems. This is the default for users, external users, resources, external resources, external entities, and nicknames.
- ♦ **Domain:** The object is visible only in the Address Book of the post offices located in the object's domain.
- ♦ **Post Office:** The object is visible only in the Address Book of the object's post office. This is the default for distribution lists, groups, and organizational roles.
- ♦ **None:** The object is not visible in the Address Book of any post offices.

For information about setting visibility for various GroupWise objects, see:

- ♦ [Section 14.7.3, "Changing a User's Visibility in the Address Book," on page 251](#)
- ♦ [Section 16.7.2, "Changing a Resource's Visibility in the Address Book," on page 275](#)
- ♦ [Section 18.9.2, "Changing a Distribution List's Visibility in the Address Book," on page 296](#)
- ♦ [Section 19.3, "Changing a Group's Visibility in the Address Book," on page 304](#)
- ♦ [Section 20.3, "Changing an Organizational Role's Visibility in the Address Book," on page 309](#)

6.3 Updating Address Book Information

Each post office database includes all the information displayed in the GroupWise Address Book that is stored in the domain. By keeping the information in the post office, the post office's users have quick access to it. Whenever changes are made in eDirectory that affect Address Book information, the information is replicated to each domain database and each post office database.

If information in a post office's Address Book is out-of-date or missing, you can synchronize the missing information with eDirectory or rebuild the post office database to obtain updated information from the domain.

- ♦ [Section 6.3.1, "Synchronizing Information," on page 111](#)
- ♦ [Section 6.3.2, "Rebuilding the Post Office Database," on page 111](#)

6.3.1 Synchronizing Information

The information for each object (user, resource, distribution list, and so on) in the GroupWise Address Book is contained in eDirectory. When an object's information is incorrect in a post office's Address Book, you can synchronize the object's information in the Address Book with the information stored in eDirectory. This causes the correct information to be replicated to each domain and post office database in the GroupWise system. For instructions, see [Chapter 29, "Synchronizing Database Information,"](#) on page 419.

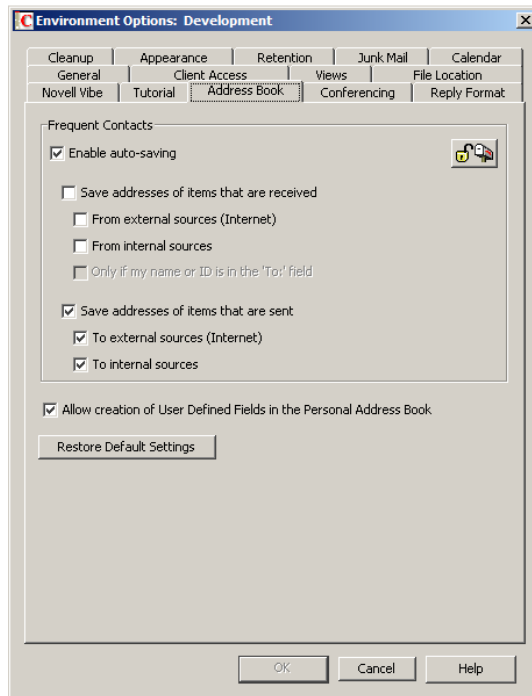
6.3.2 Rebuilding the Post Office Database

If the post office Address Book is missing a lot of information, or if you are having other difficulties with information in the Address Book, you might want to rebuild the post office database. This causes all information to be replicated to the post office database from the domain database. For instructions, see [Section 26.3, "Rebuilding Domain or Post Office Databases,"](#) on page 405.

6.4 Controlling Users' Frequent Contacts Address Books

By default, email addresses of those to whom users send messages are automatically added to their Frequent Contacts address books. Users can also choose to automatically save email addresses of those from whom they receive messages. You can restrict the types of addresses that users can collect in their Frequent Contacts address books.

- 1 In ConsoleOne, select a Domain, Post Office, or User object.
- 2 Click *Tools > GroupWise Utilities > Client Options*
- 3 Click *Environment > Address Book*.



- 4 With *Enable Auto-Saving* selected, adjust the auto-save options as needed.

Save Addresses of Items That Are Received: Select this option to allow users to automatically add external and internal email address from items that they receive to their Frequent Contacts address books. If desired, you can restrict users to collecting email addresses only if the user's name or email address appears in the *To* field, as opposed to the *CC* or *BC* fields.

Save Addresses of Items That Are Sent: Select this option to allow users to automatically add external and internal email address from items that they send to their Frequent Contacts address books.

or

Deselect *Enable Auto-Saving* to change the default so that email addresses are not collected unless users enable that functionality.

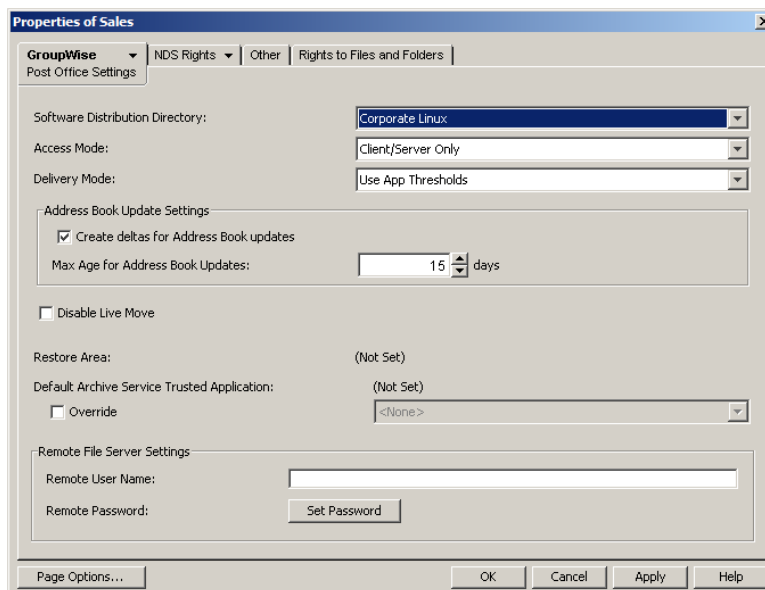
- 5 To prevent users from changing your Frequent Contacts address book settings, click the *Lock* button.
- 6 Click *OK* to save the Frequent Contacts address book settings.

6.5 Controlling Address Book Synchronization for Caching and Remote Client Users

By default, the POA automatically updates the post office database (`wphost.db`) with changes to the Address Book as they occur. As a result, whenever a Caching or Remote client connects to the GroupWise system, it automatically downloads any updates to the Address Book that have occurred since the last time it connected. This means that Caching or Remote client users always have an up-to-date Address Book to work with.

Because the Address Book updates are stored as records in the post office database, this feature causes the post office database to grow in size as time passes. Therefore, in ConsoleOne, you can specify the maximum number of days you want to store the incremental update records. The longer the incremental update records are stored, the larger the post office database becomes, which can impact available disk space and backup time. You can also disable this functionality, if necessary.

- 1 Browse to and right-click a Post Office object, then click *Properties*.
- 2 Click *GroupWise > Post Office Settings*.



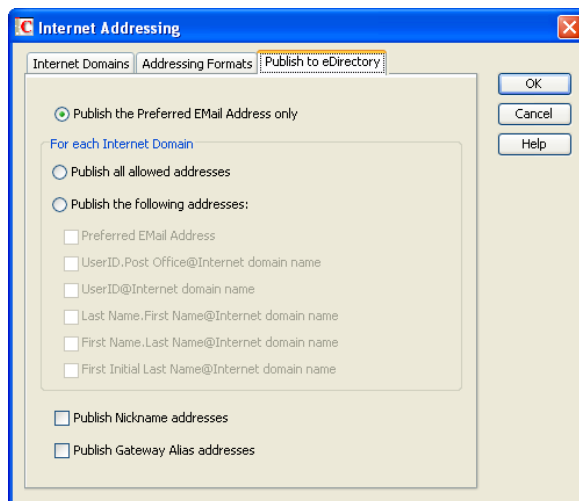
- 3 In the *Max Age for Address Book Updates* field, specify the number of days you want to retain Address Book update records.
The default is 15 days. The maximum number of days is 90.
- 4 (Optional) Deselect *Create Deltas for Address Book Updates* to disable this feature.
- 5 Click *OK* to save the setting.

Caching and Remote client users should not deselect *Refresh Address Books and Rules Every nn Days* because rules are still downloaded according to this schedule. Even if users do not want to download their rules, they still should not deselect this option because it turns off the Address Book delta sync. They can, however, set the option to a greater number of days to cause the download of the full Address Book to occur less frequently.

6.6 Publishing Email Addresses to eDirectory.

The GroupWise databases and eDirectory both contain information about users' email address formats. When you change settings for users' GroupWise email addresses, you can publish the changes to eDirectory so that user email address information matches in both places.

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > Internet Addressing*.
- 2 Click *Publish to eDirectory*.



By default, users' preferred email addresses are published to eDirectory only in the format established in the *Preferred Address Format* field on the Addressing Formats tab. This publishes one email address per user in the format established for your GroupWise system.

- 3 Select additional options to publish additional email addresses, as needed.
- 4 Click *OK* to save the address publishing settings.

6.7 Enabling Wildcard Addressing

By default, users address messages by selecting users and distribution lists from the Address Book. If you enable wildcard addressing, users can send items to all users in a post office, domain, GroupWise system, or connected GroupWise system by using asterisks (*) as wildcards in email addresses.

You can limit wildcard addressing to a specific level (system, domain, or post office) or allow unlimited wildcard addressing. The default is to limit the wildcard addressing to post office only, meaning that a user can use wild card addressing to send to all users on his or her post office only. You can change the default for individual users, post offices, or domains.

With wildcard addressing, the sender only sees whether the item was delivered to a domain, post office, or system (by viewing the item's properties). The properties do not show the individual user names or additional statuses. Recipients can reply to the sender only. Reply to All is unavailable.

- ◆ [Section 6.7.1, "Setting Wildcard Addressing Levels," on page 114](#)
- ◆ [Section 6.7.2, "Wildcard Addressing Syntax," on page 115](#)

NOTE: Wildcard addressing cannot be used for assigning shared folders or shared address books, granting proxy rights, performing busy searches, or sending routing slips.

6.7.1 Setting Wildcard Addressing Levels

By default, wildcard addressing is enabled at the post office level for all users in your GroupWise system. You can change the level (post office, domain, or system) or disable wildcard addressing.

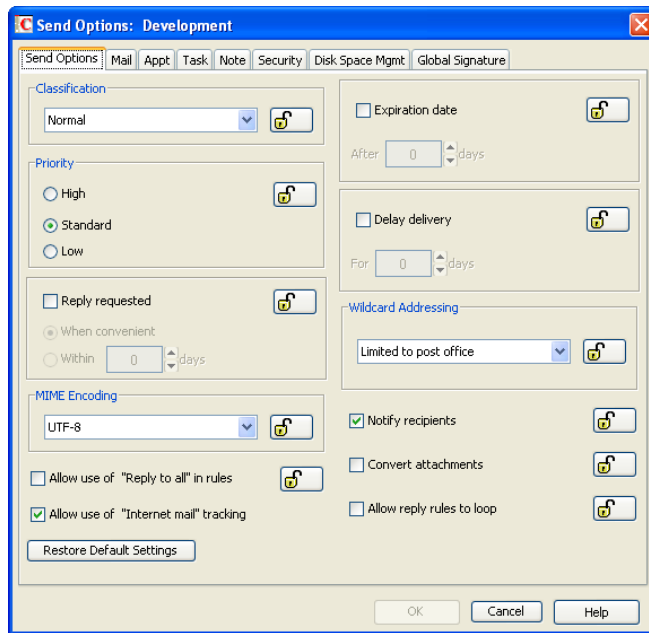
Wildcard addressing levels can be applied to a single user, to all users in a post office, or to all users in a domain.

To set wildcard addressing defaults:

- 1 In ConsoleOne, select a Domain, Post Office, or User object.
- 2 Click *Tools > GroupWise Utilities > Client Options* to display the GroupWise Client Options dialog box.



- 3 Click *Send* to display the Send Options dialog box.



4 In the *Wildcard Addressing* list, select from the following options:

- ◆ **Not Allowed:** Select this option to disable wildcard addressing.
- ◆ **Limited to Post Office (Default):** Select this option to limit wildcard addressing to the user's post office. The user can use wildcard addressing to send items to users in his or her post office only.
- ◆ **Limited to Domain:** Select this option to limit wildcard addressing to the user's domain. The user can use wildcard addressing to send items to users in his or her domain only.
- ◆ **Limited to System:** Select this option to limit wildcard addressing to the user's GroupWise system. The user can use wildcard addressing to send items to all users in his or her system only. This excludes external users (users from other systems) who have been added to your GroupWise address book.
- ◆ **Unlimited:** Select this option to allow unlimited use of wildcard addressing. The user can use wildcard addressing to send to all users (including external users and non-visible users) defined in the GroupWise address book.

5 Click *OK* to save the changes.

6.7.2 Wildcard Addressing Syntax

The following table shows the syntax for wildcard addressing.

Wildcard Addressing Setting	To send an item to...	Type in the To field...
Limited to Post Office	All users in your post office	*
Limited to Domain	All users in your post office	*
	All users in your domain	*.*
	All users in another post office in your domain	*.post_office

Wildcard Addressing Setting	To send an item to...	Type in the To field...
Limited to System	All users in your post office	*
	All users in your domain	*.*
	All users in another post office in your domain	*.post_office
	All users in a post office in another domain	*.post_office.domain
	All users in another domain	*.domain
	All users in your GroupWise system	*.*.*
Unlimited	All users in your post office	*
	All users in your domain	*.*
	All users in a different post office in your domain	*.post_office
	All users in a post office in another domain. You can also use this for external post offices and external domains.	*.post_office.domain
	All users in a another domain. You can also use this for external domains.	*.domain
	All users in the GroupWise address book (all users in the same system, all external users, and all non-visible users)	*.*.*

6.8 Adding External Users to the GroupWise Address Book

The GroupWise Address Book lists all users that belong to your GroupWise system. When users receive incoming messages, the senders are added to users' Frequent Contacts Address Books to facilitate replying to users who are not included in the GroupWise Address Book. If necessary, you can configure GroupWise so that external (non-GroupWise) users appear in the GroupWise Address Book and are therefore available to all GroupWise users.

The following sections help you add non-GroupWise users to the GroupWise Address Book:

- ♦ [Section 6.8.1, "Creating a Non-GroupWise Domain to Represent the Internet," on page 116](#)
- ♦ [Section 6.8.2, "Linking to the Non-GroupWise Domain," on page 117](#)
- ♦ [Section 6.8.3, "Creating a Non-GroupWise Post Office to Represent an Internet Host," on page 119](#)
- ♦ [Section 6.8.4, "Creating External Users," on page 120](#)
- ♦ [Section 6.8.5, "Configuring External Users and Resources to Appear in GroupWise Busy Searches," on page 121](#)

6.8.1 Creating a Non-GroupWise Domain to Represent the Internet

- 1 In ConsoleOne, right-click GroupWise System (in the left pane), then click *New > Non-GroupWise Domain*.



2 Fill in the fields:

Domain Name: Specify a name that has not been used for another domain in your system (for example, Internet).

Time Zone: This should match the time zone for the Internet Agent (GWIA). If it does not, select the correct time zone.

Link to Domain: Select a domain where the GWIA is running.

3 Click *OK* to create the non-GroupWise domain.

The non-GroupWise domain appears under GroupWise System in the left pane.

4 Continue with [Linking to the Non-GroupWise Domain](#).

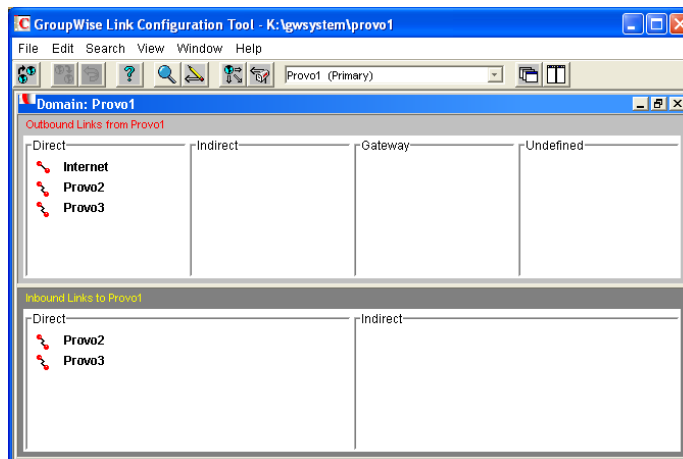
6.8.2 Linking to the Non-GroupWise Domain

After you have created the non-GroupWise domain, you must modify the link between the domain where the Internet Agent (GWIA) is running and the non-GroupWise domain. This enables the GroupWise system to route all Internet messages to the MTA of the GWIA domain. The MTA can then route the messages to the GWIA, which sends them to the Internet.

To modify the link to the non-GroupWise domain:

1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration* to display the Link Configuration tool.

By default, the Link Configuration tool displays the links for the domain that you are currently connected to.

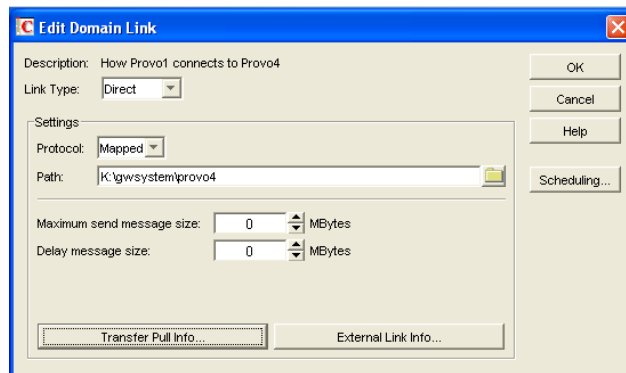


2 If the GWIA domain is not the currently displayed domain, select it from the list of domains on the toolbar.

The non-GroupWise domain should be displayed in the *Direct* column. In the graphic displayed under step 1, Internet is the non-GroupWise domain.

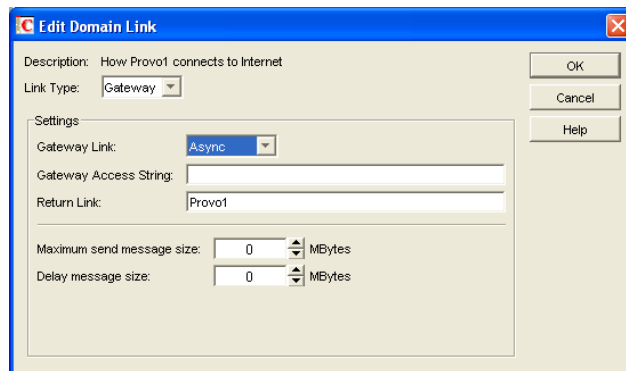
- 3 Double-click the non-GroupWise domain to display the Edit Domain Link dialog box.

If you are prompted that the mapped path is empty, click *Yes* to dismiss the prompt and display the Edit Domain Link dialog box.



- 4 In the *Link Type* field, select *Gateway*.

After you select *Gateway*, the dialog boxes changes to display the settings required for a gateway link.



NOTE: GroupWise gateways are legacy products that are not supported with the current GroupWise version.

- 5 Fill in the following fields:

Gateway Link: Select the GWIA.

Gateway Access String: If you want to specify the conversion format (RFC-822 or MIME) for messages sent to the domain, include the `-rfc822` or `-mime` parameter. If you do not use either of these parameters, the GWIA converts messages to the format specified in its startup file. The default is for MIME conversion (as specified by the GWIA's `/mime` startup switch).

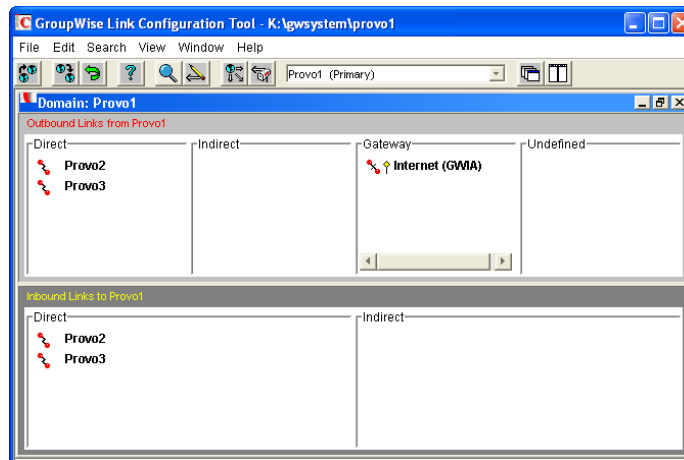
Return Link: Leave this field as is. It does not apply to the GWIA.

Maximum Send Message Size: If you want to limit the size of messages that the MTA for the GWIA domain passes to the GWIA, specify the maximum size. This is applied to all messages. If you want to limit the size of messages sent by specific users or groups of users, you can also use the Access Control feature. For details, see [Section 54.1, "Controlling User Access to the Internet," on page 787](#).

Delay Message Size: If you want the MTA to delay routing of large messages to the GWIA, specify the message size. Any messages that exceed the message size are assigned a lower priority by the MTA and are processed after the higher priority messages.

- 6 Click *OK* to save the changes.

The non-GroupWise domain is moved from the *Direct* column to the *Gateway* column. For a description of the link symbols next to the domain names, see the Help in the Link Configuration tool.



- 7 Click the *File* menu, click *Exit*, then click *Yes* to exit the Link Configuration tool and save your changes.
- 8 Continue with [Creating a Non-GroupWise Post Office to Represent an Internet Host](#).

6.8.3 Creating a Non-GroupWise Post Office to Represent an Internet Host

When you create a post office to represent an Internet host, the post office name cannot be identical to the hostname because the period that separates the hostname components (for example, novell.com) is not a valid character for post office names. GroupWise reserves the period for its addressing syntax of *user_ID.post_office.domain*. Therefore, you should choose a name that is closely related to the hostname.

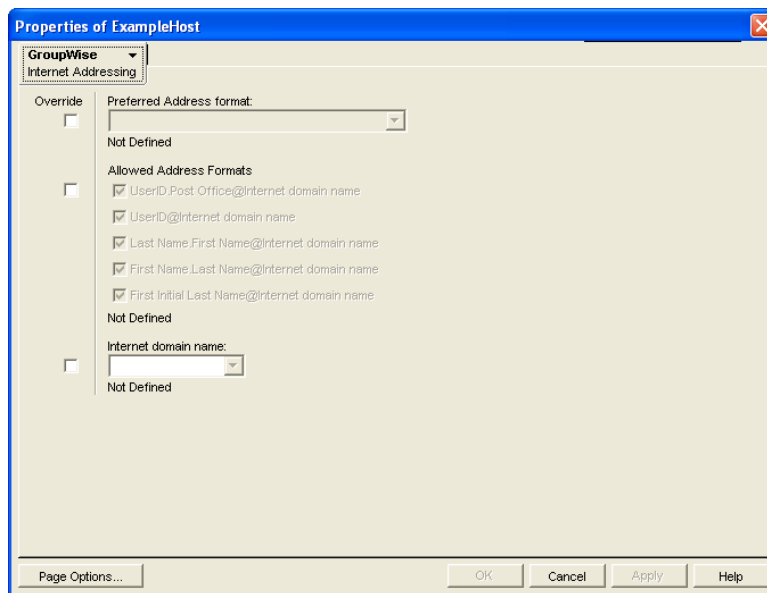
To create a non-GroupWise post office:

- 1 In ConsoleOne, right-click the non-GroupWise domain that represents the Internet, then click *New > External Post Office*.



- 2 Fill in the following fields:
 - Post Office Name:** Specify a name to associate the post office with the Internet host. Do not use the fully qualified hostname.
 - Time Zone:** Select the time zone in which the Internet host is located.
- 3 Click *OK* to create the post office.

The non-GroupWise post office is added under the non-GroupWise domain.
- 4 Right-click the new non-GroupWise post office, then click *Properties*.
- 5 Click *GroupWise > Internet Addressing*.



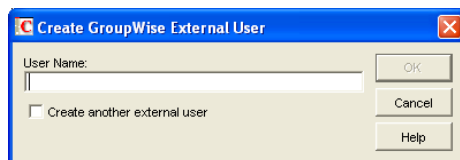
- 6 If you want to override the GroupWise system allowed address formats, select *Override* next to *Allowed Address Formats*, then select the allowed address formats for this Internet host.
- 7 Next to *Internet Domain Name*, select *Override*, then specify the actual name of the Internet host that the external post office represents.
- 8 Click *OK* to save your changes.
- 9 Continue with [Creating External Users](#).

6.8.4 Creating External Users

By creating external users, you add them to the GroupWise Address Book for easy selection by GroupWise users when addressing messages.

To add an Internet user to a post office:

- 1 In ConsoleOne, right-click the post office that represents the user's Internet host, then click *New > External User*.



- 2 In the *User Name* field, specify the exact user portion of the user's Internet address. If the address is `jsmith@novell.com`, the portion you would specify is `jsmith`.
- 3 Click *OK* to create the external user.
- 4 Provide personal information about the external user:
 - 4a Right-click the new External User object.
 - 4b Fill in the desired fields on the Identification page.

Because the user is displayed in the GroupWise Address Book, you might want to define the user's first name and last name. This is especially important if the allowed address formats for the Internet host include first name and last name information.

4c Click *OK* to save the user's personal information.

If you have only a few users on some Internet hosts, you can create a single external post office for these users, then define their Internet domain names on the Identification pages of the External User objects instead of on the External Post Office object.

6.8.5 Configuring External Users and Resources to Appear in GroupWise Busy Searches

You can define the URL where free/busy schedule status is published for a user or resource in an external email system. This enables GroupWise users to receive Busy Search results from this external user or resource along with Busy Search results from other GroupWise users.

- 1** In ConsoleOne, right-click an External User object or an External Resource object, then click *Properties*.
- 2** Click *GroupWise > Internet Free Busy Search*.
- 3** Specify the URL where free/busy schedule status for the user or resource is published, then click *OK*.

7 Multilingual GroupWise Systems

GroupWise is a multilingual email product that meets the needs of users around the world. The following sections provide guidance if your GroupWise system includes users who speak a variety of languages:

- ◆ [Section 7.1, “GroupWise User Languages,” on page 123](#)
- ◆ [Section 7.2, “GroupWise Administration and Agent Languages,” on page 124](#)
- ◆ [Section 7.3, “International Character Considerations,” on page 125](#)
- ◆ [Section 7.4, “MIME Encoding,” on page 125](#)
- ◆ [Section 7.5, “Multi-Language Workstations,” on page 127](#)

See also [Chapter 78, “Supporting the GroupWise Client in Multiple Languages,” on page 1087](#).

7.1 GroupWise User Languages

Users can run GroupWise in the following languages:

Language	Code	Language	Code
Arabic**	AR	Italian	IT
Bulgarian	BG	Japanese	JA
Chinese - Simplified	CS	Korean	KO
Chinese - Traditional	CT	Norwegian	NO
Czech	CZ	Polish	PL
Danish	DA	Portuguese	PT
Dutch	NL	Russian	RU
English	EN	Slovak*	SK
Finnish	FI	Slovenian*	SL
French	FR	Spanish	ES
German	DE	Swedish	SV
Hungarian	HU	Turkish	TR

NOTE: Languages marked with an asterisk (*) are available for the GroupWise Windows client, but not for GroupWise WebAccess. Languages marked with a double asterisk (**) are available for the GroupWise Windows client and for GroupWise WebAccess in a desktop browser, but are not available on tablet devices or mobile devices where a more simple interface is used.

Language codes are used to identify language-specific files and directories. They are also used as the values of the client language (/l) startup option. Users can select the languages they want when they install the GroupWise client.

Users should have at least 200 MB available on their workstations to install the GroupWise client software in one language. Users need an additional 20 MB of disk space for each additional language they install.

By default, the GroupWise client starts in the language of the operating system, if it is available. If the operating system language is not available, the next default language is English. When you start the GroupWise client, you can use the /l startup switch to override the English default and select an interface language from those that have been installed.

The online help available in the GroupWise clients is provided in all languages into which the client software is translated. The GroupWise client user guides available from the GroupWise clients and on the GroupWise Documentation Web site are translated only into the [administration languages](#). If you try to access a user guide from a client that is running in a language into which the user guide has not been translated, you can select any of the available languages.

By default, the GroupWise clients use UTF-8 for MIME encoding. This accommodates the character sets used by all supported languages.

7.2 GroupWise Administration and Agent Languages

You can run the GroupWise Installation program, administer your GroupWise system in ConsoleOne, and run the GroupWise agents in the following languages:

Language	Code
English	EN
French	FR
German	DE
Portuguese	PT
Spanish	ES

Language codes are used to identify language-specific files and directories. They are also used as the values of the GroupWise agent /language startup switches.

When you select a language for a domain, it determines the sorting order for items in the GroupWise Address Book. This language becomes the default for post offices that belong to the domain. You can override the domain language at the post office level if necessary.

For example, if you set the domain and post office language to English, the Address Book items are sorted according to English sort order rules. This is true even if some users in the post office are running non-English GroupWise clients such as German or Japanese. Their client interface and Help files are in German or Japanese, but the sort order is according to English standards.

By default, the agents start in the language selected for the domain. If that language has not been installed, the agents start in the language used by the operating system. If that language has not been installed, the agents start in English. You can also use the /language agent startup switch to select the language for the agent to start in.

The POA also includes language-specific files in all client languages so that information returned from the POA to the GroupWise client, such as message status and undeliverable messages, is displayed in the language of the GroupWise client rather than the language in which the POA interface is being displayed.

Currently, the DVA is available only in English.

7.3 International Character Considerations

GroupWise client users have complete flexibility in the characters they use in composing messages. Accented characters used by various European languages and double-byte characters used by various Asian and Middle Eastern languages are all acceptable in the GroupWise client and can even be combined in the same message text.

As an administrator, you must take the following limitations into account:

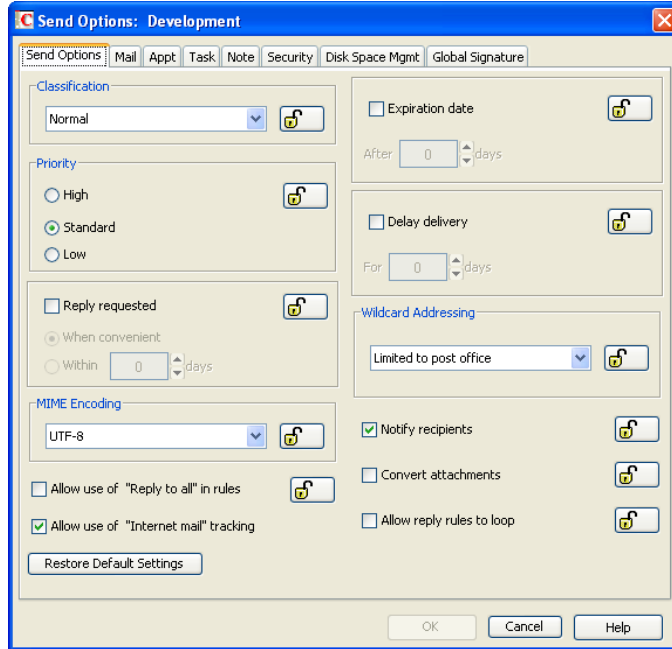
- ♦ Double-byte Asian and Middle Eastern characters should not be used in directory names and file names within your GroupWise system. This limitation is based on operating system capabilities. You should also not use double-byte characters in passwords. You can use double-byte characters in GroupWise user names, domain names, post office names, and so on.
- ♦ If you choose to use double-byte characters or extended characters such as accented characters in GroupWise user names or domain names, users must have Preferred E-mail IDs that contain only characters that are valid in the SMTP RFC. For instructions, see [Section 14.7.2, “Changing a User’s Internet Addressing Settings,”](#) on page 249.

7.4 MIME Encoding

MIME (Multipurpose Internet Mail Extensions) encoding must be used when messages are sent across the Internet, so that characters display correctly for users on computers that are configured for different languages. In ConsoleOne, you can set the default MIME encoding (for example, UTF-8, Windows Default, ISO Default, and so on) that is used by the GroupWise clients.

- 1 In ConsoleOne, browse to and select the domain, post office, or user where you want to change the maximum mailbox size.
- 2 Click *Tools > GroupWise Utilities*.

3 Click *Client Options > Send*.



4 In the *MIME Encoding* box on the *Send Options* tab, select the desired default MIME encoding, then click *OK* to save the setting.

GroupWise users can override the default MIME encoding in GroupWise, as described in:

- ◆ “[Changing the MIME Encoding for Email You Send](#)” in “[Email](#)” in the *GroupWise 2012 Windows Client User Guide*
- ◆ “[Changing the MIME Encoding of a Message](#)” in “[Email](#)” in the *GroupWise 2012 WebAccess User Guide*

The Windows client supports 24 character sets for MIME encoding. GroupWise WebAccess and ConsoleOne support 16 character sets, marked with asterisks in the table below.

Languages/Alphabets	Character Sets
	Windows Default*
	ISO Default*
	UTF-8*
Arabic	Windows 1256*
Arabic	ISO 8859-6
Baltic	Windows 1257*
Baltic	ISO 8859-4
Central European	Windows 1250*
Central European	ISO 8859-2
Chinese Simplified	GB2312*
Chinese Traditional	Big 5

Languages/Alphabets	Character Sets
Cyrillic	KOI8-R*
Cyrillic	ISO 8859-5
Hebrew	Windows 1255*
Hebrew	ISO 8859-8
Japanese	ISO 2022-JP*
Japanese	Shift-JIS
Korean	EUC-KR*
Thai	Windows 874*
Turkish	Windows 1254*
Turkish	ISO 8859-9
Western European	Windows 1252
Western European	ISO 8859-1
Western European	ISO 8859-15

The GWIA also has options for controlling MIME encoding when messages are set to and from the Internet, as described in:

- ◆ ConsoleOne settings: [Section 53.1.4, “Determining Format Options for Messages,”](#) on page 763
- ◆ Startup switches: [Section 59.6.4, “Message Formatting and Encoding,”](#) on page 868

7.5 Multi-Language Workstations

If GroupWise users receive messages in multiple languages, their workstations need to be configured to handle the character sets used by these languages.

On Windows 7:

- 1 In the Control Panel, click *Change Display Languages*.
- 2 In the *Display Language* box, click *Install/Uninstall Languages*.
- 3 Follow the on-screen instructions to install the required language files.

On Windows Vista:

- 1 In the Control Panel, double-click *Regional and Language Options*, then click *Keyboards and Languages*.
- 2 Under *Display Languages*, click *Install/Uninstall Languages*.
- 3 Follow the on-screen instructions to install the required language files.

On Windows XP:

- 1 In the Control Panel, double-click *Regional and Language Options*, then click *Languages*.
- 2 If you receive messages in Arabic, Hebrew, or other complex languages, select *Install Files for Complex Script and Right-to-Left Languages*.

- 3 If you receive messages in Chinese, Japanese, or other similar languages, select *Install Files for East Asian Languages*.
- 4 Click *OK* to install the required language files.

|| Domains

- ♦ [Chapter 8, “Creating a New Domain,” on page 131](#)
- ♦ [Chapter 9, “Managing Domains,” on page 145](#)
- ♦ [Chapter 10, “Managing the Links between Domains and Post Offices,” on page 155](#)

8 Creating a New Domain

As your GroupWise system grows, you might need to add new domains.

- ♦ [Section 8.1, “Understanding the Purpose of Domains,”](#) on page 131
- ♦ [Section 8.2, “Planning a New Domain,”](#) on page 132
- ♦ [Section 8.3, “Setting Up the New Domain,”](#) on page 138
- ♦ [Section 8.4, “What’s Next,”](#) on page 142
- ♦ [Section 8.5, “New Domain Summary Sheet,”](#) on page 142

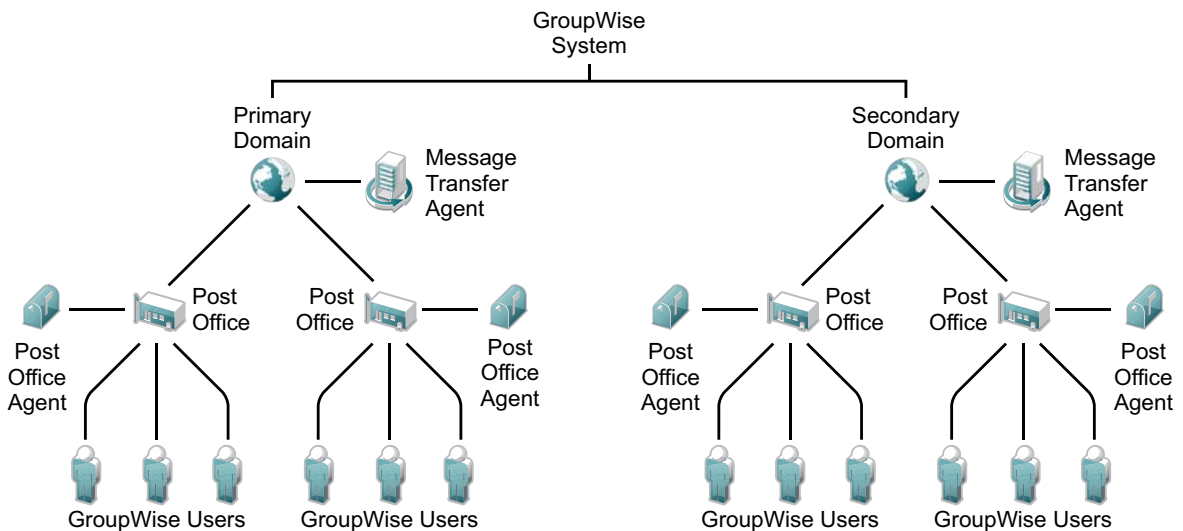
IMPORTANT: If you are creating a new domain in a clustered GroupWise system, see the [GroupWise 2012 Interoperability Guide](#) before you create the domain.

8.1 Understanding the Purpose of Domains

The domain functions as the main administrative unit for your GroupWise system. Each GroupWise system has one primary domain, which was created when you first installed GroupWise. All other domains that you add are secondary domains.

The domain serves as a logical grouping of one or more post offices and is used for addressing and routing messages. Each GroupWise user has a unique GroupWise address that consists of a user ID, the user’s post office name, the GroupWise domain name, and, optionally, an Internet domain name.

The following diagram illustrates the logical organization of a GroupWise system with multiple domains and post offices. All of the objects under the domain belong to that domain. All of the objects under a post office belong to that post office.



Messages are moved from user to user through your GroupWise system by the GroupWise agents. As illustrated above, each domain must have a Message Transfer Agent (MTA). The MTA transfers messages between domains and between post offices in the same domain. Each post office must have at least one Post Office Agent (POA). The POA delivers messages to users' mailboxes and performs a variety of post office and mailbox maintenance activities.

When you add a new domain to your GroupWise system, links define how messages are routed from one domain to another. When you add the first secondary domain, the links between the primary and secondary domains are very simple. As the number of domains grows, the links among them can become quite complex. Links are discussed in detail in [Chapter 10, "Managing the Links between Domains and Post Offices,"](#) on page 155.

Physically, a domain consists of a set of directories that house all the information stored in the domain. To view the structure of a domain directory, see "[Domain Directory](#)" in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*. The domain directory does not contain mailboxes or messages, but it does contain other vital information. For an overview, see [Section 41.3, "Information Stored in the Domain,"](#) on page 622. Domain directories can be located on Linux and Windows servers.

8.2 Planning a New Domain

After you have your basic GroupWise system up and running, you can expand it by adding one or more secondary domains. The GroupWise architecture lets you create a simple, single domain system, or a complex system that links dozens of secondary domains across a campus, a city, or around the world.

This section provides the information you need in order to decide when, where, and how to set up a new domain. The items in the worksheet are listed in the order you enter them when setting up your domain. This planning section does not follow the same order as the worksheet, but all worksheet items are covered. The "[New Domain Summary Sheet](#)" on page 142 lists all the information you need. You should print the worksheet and fill it out as you complete the tasks listed below.

- ♦ [Section 8.2.1, "Determining When to Add a New Domain,"](#) on page 133
- ♦ [Section 8.2.2, "Deciding Who Will Administer the New Domain,"](#) on page 133
- ♦ [Section 8.2.3, "Planning Post Offices in the New Domain,"](#) on page 134
- ♦ [Section 8.2.4, "Determining the Context for the Domain Object,"](#) on page 134
- ♦ [Section 8.2.5, "Choosing the Domain Name,"](#) on page 136
- ♦ [Section 8.2.6, "Deciding Where to Create the Domain Directory,"](#) on page 136
- ♦ [Section 8.2.7, "Deciding Where to Install the Agent Software,"](#) on page 137
- ♦ [Section 8.2.8, "Deciding How to Link the New Domain,"](#) on page 137
- ♦ [Section 8.2.9, "Selecting the Domain Language,"](#) on page 138
- ♦ [Section 8.2.10, "Selecting the Domain Time Zone,"](#) on page 138

After you have completed the tasks and filled out the "[New Domain Summary Sheet](#)" on page 142, you are ready to continue with [Section 8.3, "Setting Up the New Domain,"](#) on page 138.

8.2.1 Determining When to Add a New Domain

How do you know when you should add a domain? The answer to this depends on your administration policies and on physical and logical network organization.

Although a single domain can contain as many post offices and users as you want to add, there are some conditions that indicate the need for a new domain:

- ♦ **Administrative Convenience:** To spread out the administrative workload, you can create one or more new domains with their own administrators. Each new domain can be managed by a different administrator as long as each administrator has sufficient rights to connect to it and write to the domain database.
- ♦ **Remote Sites:** If communication between servers is slow, or if you have remote sites, you can add a new domain to minimize mail traffic between the servers. For example, if you have locations in three separate cities, you might have an organization that represents each location. You could then create a domain in each organization. You could administer all of the domains from one location or you could assign a different administrator for each one.
- ♦ **Demand on the MTA:** Each domain has its own MTA that routes messages between post offices within its domain. If your current domain has many post offices that are placing a heavy workload on the MTA, you might want to create another domain to handle additional post offices.
- ♦ **Multiple eDirectory Trees:** All of the objects that are logically subordinate to a GroupWise domain must be in the same Novell eDirectory tree as the domain. If you have users in other eDirectory trees that need GroupWise accounts, you must create secondary domains and post offices in each tree.

For additional guidance, visit the [GroupWise Best Practices Wiki \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

8.2.2 Deciding Who Will Administer the New Domain

Any user who is an Admin equivalent can administer GroupWise. The person who creates the new domain should be an Admin equivalent user so that he or she has the necessary rights to create objects and directories. You can then assign a different user as a domain administrator and limit rights to other objects if necessary. For more information, see [Chapter 87, "GroupWise Administrator Rights," on page 1127](#).

Depending upon the size, complexity, and layout of your eDirectory tree, you might choose a centralized administration model with one person administering both eDirectory and GroupWise, or you might choose a distributed administration model with the administration workload shared by two or more individuals. With a distributed administration model, each administrator obtains rights to the GroupWise objects and directory structures over which he or she has jurisdiction. If you want to restrict access to some network operations or to certain domains, you can limit access rights to domains the user should not administer.

The user assigned as the domain administrator must be able to create or modify objects in the domain and will receive an email message whenever an agent encounters a problem. You can designate yourself, one or more other users, or a distribution list as an administrator.

NEW DOMAIN SUMMARY SHEET

Under *Domain Administrator*, enter the ID of the user or distribution list that will administer this domain.

8.2.3 Planning Post Offices in the New Domain

Before adding the new domain, you should plan the post offices that you want to belong to the domain. Review [Section 11.2, “Planning a New Post Office,” on page 174](#) as part of planning your new domain.

8.2.4 Determining the Context for the Domain Object

When deciding where to place the new Domain object in the eDirectory tree, you should consider how you can most easily administer GroupWise and how the domain and its associated post offices fit into the logical organization of your eDirectory tree.

Domains and their associated objects, including Post Offices, Users, Resources, and Distribution Lists, must be located in the same eDirectory tree. If you have multiple trees, you must create a separate domain in each tree. The domains can all belong to the same GroupWise system, even though they are located in different trees.

You can place the domain in any Organization or Organizational Unit container in any context in an eDirectory tree. The following sections provide some examples of how domains can be placed in the eDirectory tree:

- ♦ [“GroupWise Objects Reflect Physical Locations” on page 134](#)
- ♦ [“GroupWise Objects Reflect Company Organization” on page 135](#)
- ♦ [“GroupWise Objects Are Grouped with Servers” on page 135](#)
- ♦ [“GroupWise Objects Are Located in a Separate GroupWise Container” on page 135](#)

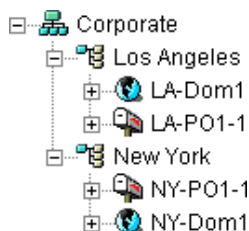
NEW DOMAIN SUMMARY SHEET

Under *Tree Name*, specify the name of the eDirectory tree where you plan to create the new domain.

Under *eDirectory Container*, specify the name of the eDirectory container where you plan to create the new domain.

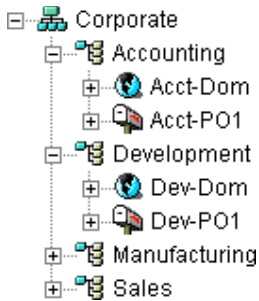
GroupWise Objects Reflect Physical Locations

The GroupWise system below focuses on the physical layout of the company. Because most mail traffic is probably generated by users in the same location, the mail traffic across the WAN is minimized. An organizational unit is created for each site. A domain is created under each organizational unit, corresponding to the city. The sites can be administered centrally or at each site. Administrator rights can be assigned at the domain level.



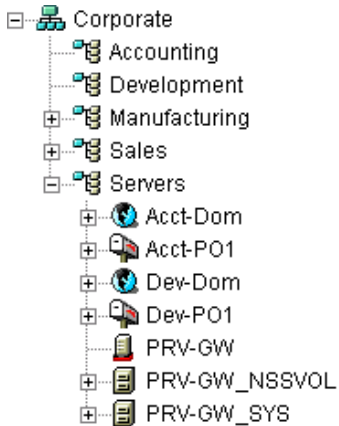
GroupWise Objects Reflect Company Organization

The following GroupWise system focuses on departmental organization, as does the eDirectory tree. GroupWise domains and post offices parallel eDirectory organizational units, placing the domains and post offices within the organizational units containing the users that belong to them.



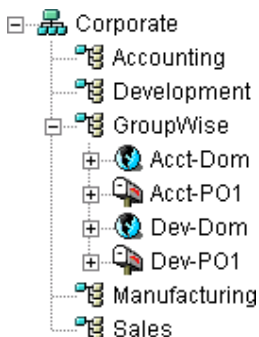
GroupWise Objects Are Grouped with Servers

Because domains and post offices have directory structures on network servers, you could also choose to place the Domain and Post Office objects in the same context as the servers where the directories reside, as shown in the following example.



GroupWise Objects Are Located in a Separate GroupWise Container

Domains and post offices can also be created in their own organizational unit. Administratively, this approach makes it easier to restrict a GroupWise administrator's object and property rights to GroupWise objects only. For information about GroupWise Administrator rights, see [Section 8.2.2, "Deciding Who Will Administer the New Domain,"](#) on page 133.



The GroupWise View in ConsoleOne

Regardless of where you choose to place Domain objects in the eDirectory tree, you can get a consolidated view of your GroupWise system using the GroupWise View in ConsoleOne. For instructions, see [Chapter 3, “GroupWise View,”](#) on page 61.

8.2.5 Choosing the Domain Name

The domain requires a unique name. The name is used as the Domain object’s name in eDirectory. It is also used for addressing and routing purposes in your GroupWise system, and might appear in the GroupWise Address Book.

The domain name can reflect a location, company name or branch name, or some other element that makes sense for your organization. For example, you might want the domain name to be the location (for example, Provo) while the post office name is one of the company’s departments (for example, Research). Name the new domain carefully. After it is created, the name cannot be changed.

The domain name should consist of a single string. Use underscores (_) rather than spaces as separators between words to facilitate addressing across the Internet.

Do not use any of the following invalid characters in the domain name:

ASCII characters 0-31	Comma,
Asterisk *	Double quote “
At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces {}	Period.
Colon:	Slash /

NEW DOMAIN SUMMARY SHEET

Under *Domain Name*, specify the domain name.

Under *Domain Description*, provide a description for the new domain.

8.2.6 Deciding Where to Create the Domain Directory

Logically, the Domain object resides in eDirectory and is administered through ConsoleOne. Physically, the domain has a directory structure for databases, message queues, and other files. The domain directory structure can be created on any of the supported platforms listed in “[GroupWise Administration Requirements](#)” in the [GroupWise 2012 Installation Guide](#). The server where you create the domain directory structure can be in the same tree as the Domain object or in another tree.

Many different configurations are possible. When deciding where to create the domain directory, you should consider the following.

- ♦ **Domain Directory Space Requirements:** The domain directory is not a large consumer of disk space. For guidance on domain directory space requirements, visit the [GroupWise Best Practices Wiki](http://wiki.novell.com/index.php/GroupWise) (<http://wiki.novell.com/index.php/GroupWise>).

- ♦ **Access by the MTA:** For best performance, the MTA should be installed on the same server as the domain directory. This is required on Linux. Remote installation is possible on Windows, but not recommended.
- ♦ **Security from User Access:** Users never need access to the domain directory so you should create it in a location you can easily secure; otherwise, you could have files inadvertently moved or deleted.

Choose an empty directory for the new domain. If you want, the directory can reflect the name of the domain, for example, `Provo1` for one of several domains located in Provo. Use the following platform-specific conventions:

Linux: Use only lowercase characters.

Windows: No limitations.

Choose the name and path carefully. After the domain directory is created, it is difficult to rename it. If the directory you specify does not exist, it can be created when you create the domain. If you create the directory in advance, it is easy to browse to it as you create the domain.

IMPORTANT: Do not create the domain directory under another domain or post office directory.

NEW DOMAIN SUMMARY SHEET

Under *Domain Database Location*, enter the full path for the domain directory.

8.2.7 Deciding Where to Install the Agent Software

You must run a new instance of the MTA for each new domain. To review the functions of the MTA for the domain, see [Section 41.4, “Role of the Message Transfer Agent,” on page 624](#). For complete installation instructions and system requirements, see [“Installing GroupWise Agents” in the *GroupWise 2012 Installation Guide*](#).

You can install the MTA on Linux or Windows. You should install it on the same server where you plan to create the domain directory structure.

NEW DOMAIN SUMMARY SHEET

Under *Agent Platform*, enter the platform of the server where the MTA will run (Linux or Windows).

8.2.8 Deciding How to Link the New Domain

Domain links tell the MTAs how to route messages between domains. Properly configured links optimize message flow throughout your GroupWise system. For a review of link types, see [Section 10.1.1, “Domain-to-Domain Links,” on page 155](#).

When you create the new domain, you link it to one existing domain. By default, this link is a direct link using TCP/IP as the link protocol, which means the new domain’s MTA communicates with the existing domain’s MTA through TCP/IP. This is the recommended configuration, and is required on Linux.

On Windows, you can configure the direct link to use a UNC path or a mapped drive as the link protocol, which means the new domain's MTA transfers information to and from the existing domain by accessing the existing domain's directory, rather than by communicating with the other domain's MTA.

NEW DOMAIN SUMMARY SHEET

Under *Link to Domain*, specify the existing domain that you want to link the new domain to, then specify the link protocol (TCP/IP or UNC path).

After you create the new domain, you can configure links to additional domains as needed. See [Section 10.2, "Using the Link Configuration Tool," on page 161](#).

8.2.9 Selecting the Domain Language

The domain language determines the default sort order for items in the GroupWise Address Book for users in post offices that belong to the domain. For more information, see [Section 11.2.8, "Selecting the Post Office Language," on page 179](#).

NEW DOMAIN SUMMARY SHEET

Under *Domain Language*, specify the domain language.

8.2.10 Selecting the Domain Time Zone

When a message is sent from a user in one time zone to a user in another time zone, GroupWise adjusts the message's time so that it is correct for the recipient's time zone. For example, if a user in New York (GMT -05:00, Eastern Time) schedules a user in Los Angeles (GMT -08:00, Pacific Time) for a conference call at 4:00 p.m. Eastern Time, the appointment is scheduled in the Los Angeles user's calendar at 1:00 p.m. Pacific Time.

The domain time zone becomes the default time zone for each post office in the domain.

NEW DOMAIN SUMMARY SHEET

Under *Domain Time Zone*, enter the time zone.

8.3 Setting Up the New Domain

You should have already reviewed [Section 8.2, "Planning a New Domain," on page 132](#) and filled out the [New Domain Summary Sheet](#). Complete the following tasks to create the new domain:

- ♦ [Section 8.3.1, "Creating the New Domain," on page 139](#)
- ♦ [Section 8.3.2, "Configuring the MTA for the New Domain," on page 141](#)
- ♦ [Section 8.3.3, "Installing and Starting the New MTA," on page 141](#)

8.3.1 Creating the New Domain

- 1 Make sure you are logged in to the tree where you want to create the domain ([Tree Name](#) on the [New Domain Summary Sheet](#)).
- 2 (Conditional) If you are creating the domain on a different machine from where you are running ConsoleOne, make sure that ConsoleOne has write access to the location where you want to create the domain.

Linux: Mount the file system where you want to create the new domain. For assistance, see [Section 2.1, "ConsoleOne on Linux,"](#) on page 39.

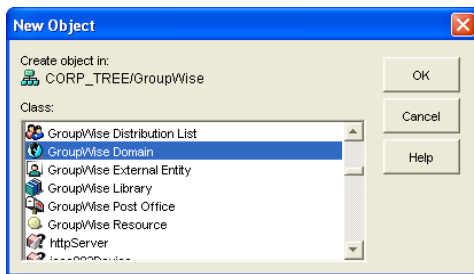
Windows: Map a drive to the location where you want to create the new domain.

- 3 In ConsoleOne, click *Tools > GroupWise Utilities > Check eDirectory Schema* to make sure that the tree's schema has been extended to accommodate GroupWise objects.

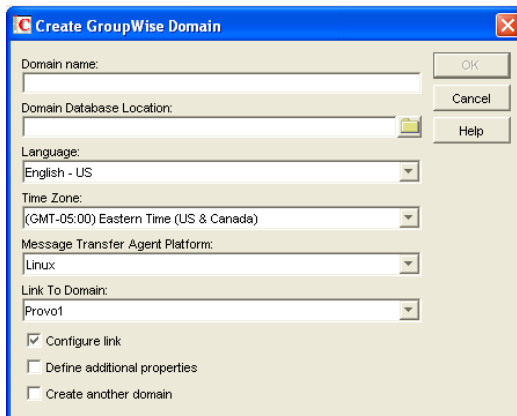
- 4 Connect to the primary domain.

If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, "Select Domain,"](#) on page 69.

- 5 Browse to and right-click the eDirectory container where you want to create the domain ([eDirectory Container](#) on the [New Domain Summary Sheet](#)), then click *New > Object*.



- 6 Double-click *GroupWise Domain*, then fill in the fields in the Create GroupWise Domain dialog box from your [New Domain Summary Sheet](#).



[Domain Name](#)

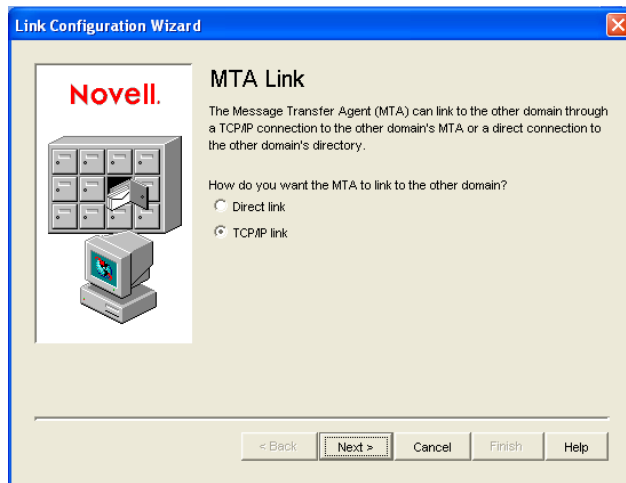
[Domain Database Location](#)

[Domain Language](#)

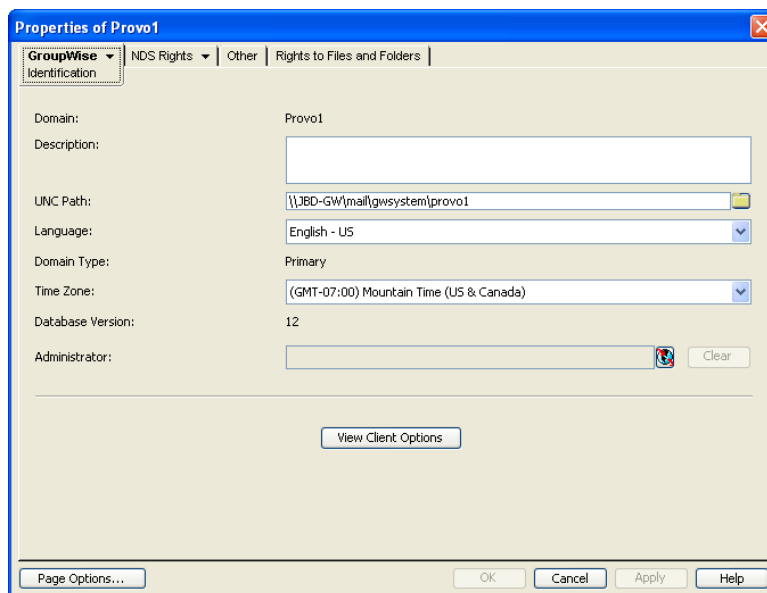
[Domain Time Zone](#)

[Link to Domain](#)

- 7 Make sure the *Configure Links* and *Define Additional Properties* options are selected, then click *OK* to display the Link Configuration Wizard.



- 8 Follow the on-screen instructions to define how the new domain links to the existing domain, listed in the *Link to Domain* field. When you have finished defining the link, ConsoleOne creates the Domain object and displays the domain Identification page.



- 9 Fill in the fields that have not been filled in for you from your [New Domain Summary Sheet](#):

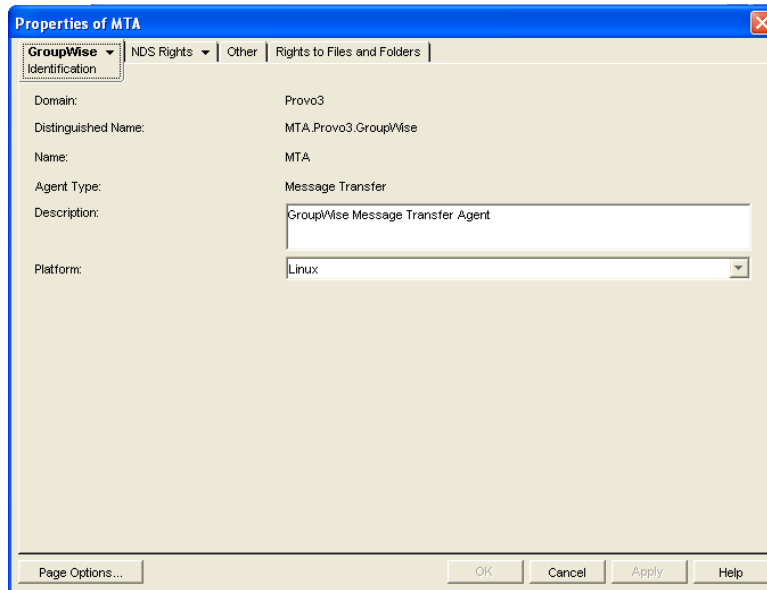
[Domain Description](#)
[Domain Administrator](#)

- 10 Click *OK* to save the domain information.
- 11 Continue with [Configuring the MTA for the New Domain](#).

8.3.2 Configuring the MTA for the New Domain

Although there are many MTA settings, the default settings are sufficient to get your domain operational. However, there are a few important settings that you can conveniently modify before you install the agent software.

- 1 In ConsoleOne, double-click the new Domain object.
- 2 Right-click the MTA object, then click *Properties* to display the MTA Identification page.



- 3 Specify a description for the MTA.
This description displays on the MTA agent console as the MTA runs.
- 4 Select the platform where the MTA will run ([Agent Platform](#) on the [New Domain Summary Sheet](#)).
- 5 (Conditional) If you have multiple domains in your GroupWise system and want to use TCP/IP to link to the other domains ([Link to Domain](#) on the [New Domain Summary Sheet](#)), follow the instructions in [“Using TCP/IP Links between Domains”](#) on page 632.
- 6 (Conditional) If you have created the domain in a clustered environment, follow the instructions in the appropriate section of the [GroupWise 2012 Interoperability Guide](#).
- 7 To ensure that user information in the new domain stays synchronized with user information in eDirectory, follow the instructions in [Section 42.4.1, “Using eDirectory User Synchronization,”](#) on page 652.
- 8 For more MTA configuration options, see [Section 9.7, “Changing the MTA Configuration to Meet Domain Needs,”](#) on page 154.
- 9 Click OK to save the MTA configuration information.
- 10 Continue with [Installing and Starting the New MTA](#)

8.3.3 Installing and Starting the New MTA

- 1 Install and start the MTA for the new domain on the server where you created the domain directory structure.

For instructions, see “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.

2 Continue with [What’s Next](#).

8.4 What’s Next

After you have added the new domain and started its MTA, you are ready to continue to expand and enhance your GroupWise system by:

- ♦ Configuring the Address Book for the new domain.
See “[GroupWise Address Book](#)” on page 105.
- ♦ Adding post offices to the new domain.
See “[Post Offices](#)” on page 171.
- ♦ Configuring the MTA for optimal performance.
See “[Message Transfer Agent](#)” on page 619.
- ♦ Connecting domains and GroupWise systems across the Internet using the GWIA.
See “[Internet Agent](#)” on page 741.
- ♦ Setting up GroupWise Monitor to monitor the GroupWise agents.
See “[Monitor](#)” on page 939.

8.5 New Domain Summary Sheet

Field	Value for Your GroupWise System	Explanation
Tree Name:		Section 8.2.4, “Determining the Context for the Domain Object,” on page 134
eDirectory Container:		Section 8.2.4, “Determining the Context for the Domain Object,” on page 134
Domain Name:		Section 8.2.5, “Choosing the Domain Name,” on page 136
Domain Database Location:		Section 8.2.6, “Deciding Where to Create the Domain Directory,” on page 136
Domain Language:		Section 8.2.9, “Selecting the Domain Language,” on page 138
Domain Time Zone:		Section 8.2.10, “Selecting the Domain Time Zone,” on page 138

Field	Value for Your GroupWise System	Explanation
Link to Domain:		Section 8.2.8, "Deciding How to Link the New Domain," on page 137
Link Protocol:		
<ul style="list-style-type: none"> ◆ TCP/IP 	Address:	
	Port:	
<ul style="list-style-type: none"> ◆ UNC path 		
Domain Description:		Section 8.2.5, "Choosing the Domain Name," on page 136
Domain Administrator:		Section 8.2.2, "Deciding Who Will Administer the New Domain," on page 133
Agent Platform:		Section 8.2.7, "Deciding Where to Install the Agent Software," on page 137
<ul style="list-style-type: none"> ◆ Linux MTA 		
<ul style="list-style-type: none"> ◆ Windows MTA 		

9 Managing Domains

As your GroupWise system grows and evolves, you might need to perform the following maintenance activities on domains:

- ♦ [Section 9.1, “Connecting to a Domain,” on page 145](#)
- ♦ [Section 9.2, “Editing Domain Properties,” on page 146](#)
- ♦ [Section 9.3, “Converting a Secondary Domain to a Primary Domain,” on page 150](#)
- ♦ [Section 9.4, “Replacing the Primary Domain Database with a Secondary Domain Database,” on page 151](#)
- ♦ [Section 9.5, “Moving a Domain,” on page 152](#)
- ♦ [Section 9.6, “Deleting a Domain,” on page 153](#)
- ♦ [Section 9.7, “Changing the MTA Configuration to Meet Domain Needs,” on page 154](#)

See also [Chapter 26, “Maintaining Domain and Post Office Databases,” on page 401](#).

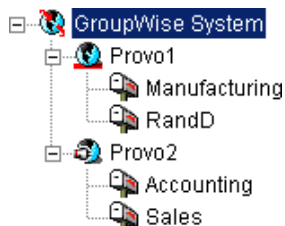
9.1 Connecting to a Domain

Whenever you change domain information, it is efficient to connect directly to the domain before you begin making modifications. This enables ConsoleOne to write directly to the domain database (`wdomain.db`). Performing administrative tasks in a domain while not connected to it increases the amount of administrative message traffic sent between domains.

IMPORTANT: In a large GroupWise system, especially where some domains are on Linux servers and some domains are on Windows servers, and where you might be running ConsoleOne on a different platform from where the domain directory is located, a direct connection might not be convenient. Although they are efficient, direct connections are not required for most GroupWise administration tasks. For more information, see [Section 4.1.2, “Understanding the Need for Domain Connections,” on page 71](#).

To change your domain connection:

- 1 In ConsoleOne in the GroupWise View, right-click the Domain object, then click *Connect*.
The GroupWise View identifies the domain to which you are connected by adding a plug symbol to the domain icon.



The domain marked with the red underscore is the primary domain.

or

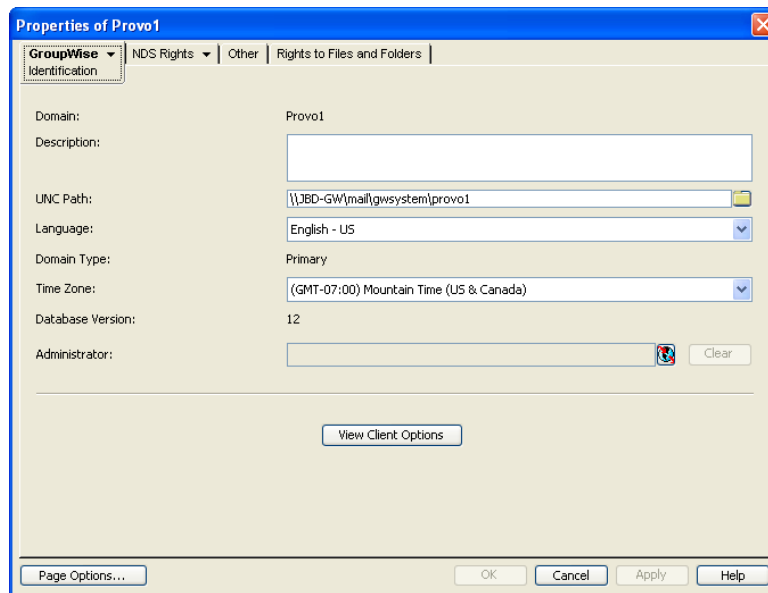
In the Console View, click *Tools > GroupWise System Operations*, click *Select Domain*, browse to and select the domain directory, then click *OK*.

Under certain circumstances, this connection method is required. See [Section 4.1, “Select Domain,”](#) on page 69.

9.2 Editing Domain Properties

After creating a domain, you can change some domain properties. Other domain properties cannot be changed.

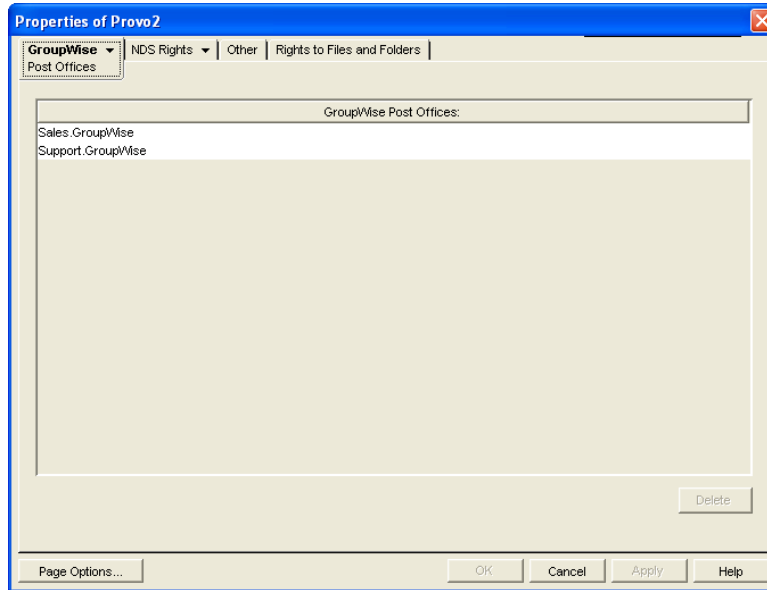
- 1 In ConsoleOne, browse to and right-click a Domain object, then click *Properties* to display the domain Identification page.



- 2 Change editable fields as needed.

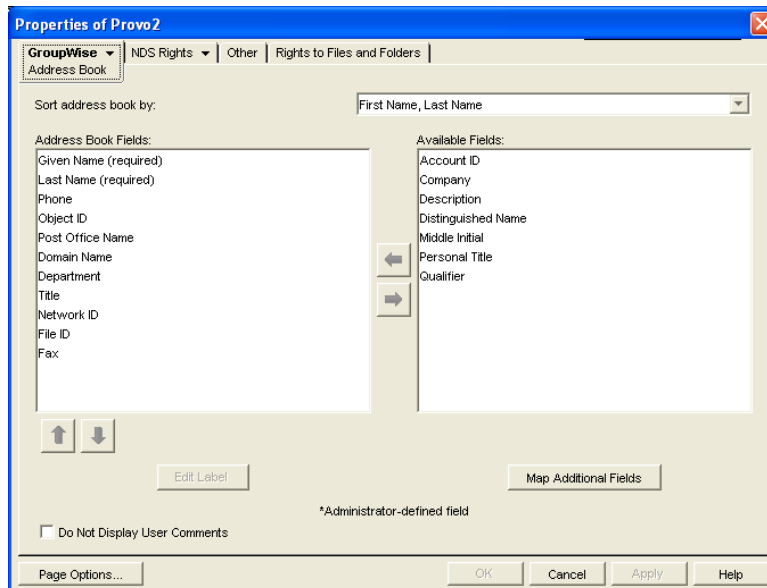
For information about individual fields, see [Section 8.2, “Planning a New Domain,”](#) on page 132 or use online help when editing the domain information.

- 3 Click *GroupWise > Post Offices* to display the Post Offices page.



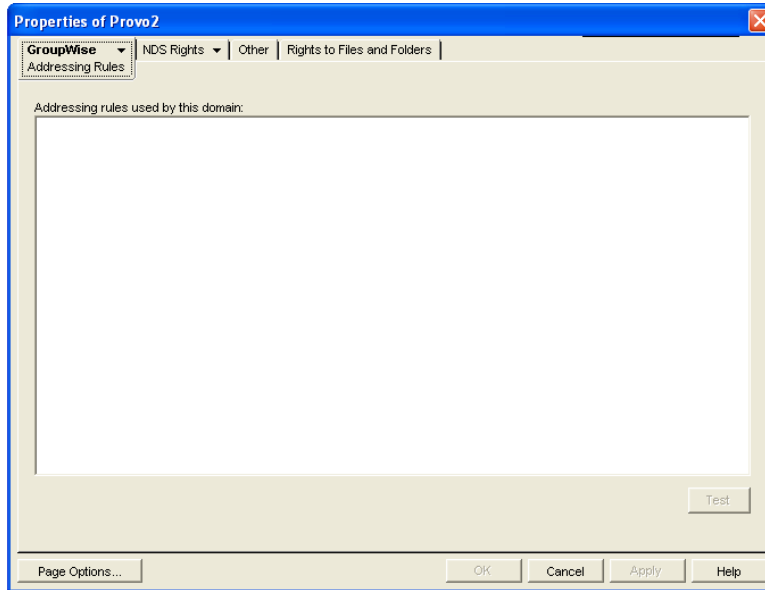
All post offices in the domain are listed, no matter where their Novell eDirectory objects are placed in the tree. This is a convenient place to delete post offices from the domain.

- 4 Click *GroupWise > Address Book* to display the Address Book page.



- 5 Use this page to configure the Address Book to control how it appears to GroupWise client users in all post offices in the domain. See [Section 6.1, "Customizing Address Book Fields," on page 105](#) for more information.

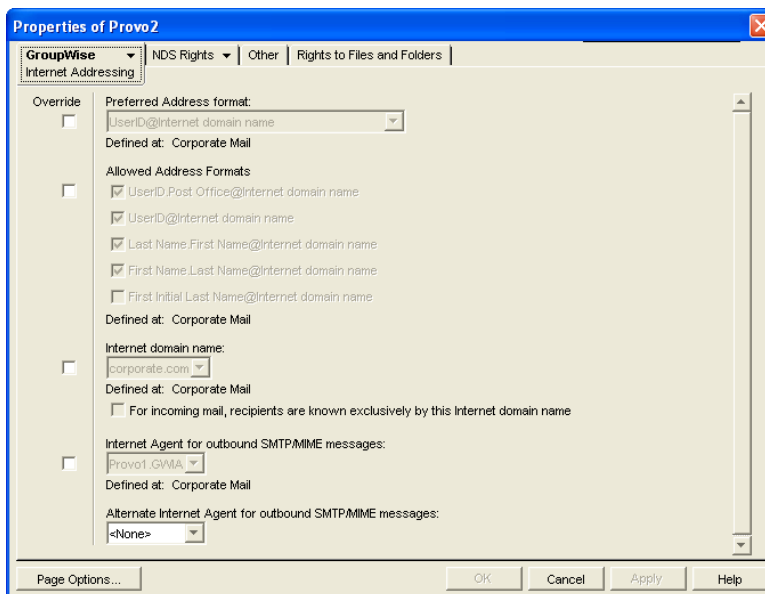
- 6 Click *GroupWise > Addressing Rules* to display the Addressing Rules page.



This page lists all addressing rules that have been set up for the domain. Addressing rules are typically used with GroupWise gateways.

NOTE: GroupWise gateways are legacy products and are not supported with the current GroupWise version.

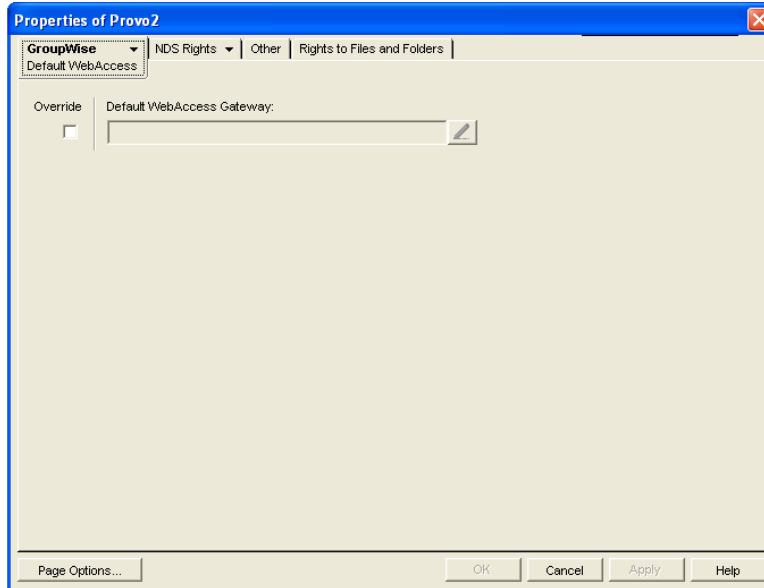
- 7 Click *GroupWise > Internet Addressing* to display the Internet Addressing page.



Use this page to override any Internet addressing settings established at the system level. See [Section 52, “Configuring Internet Addressing,” on page 743](#) for more information.

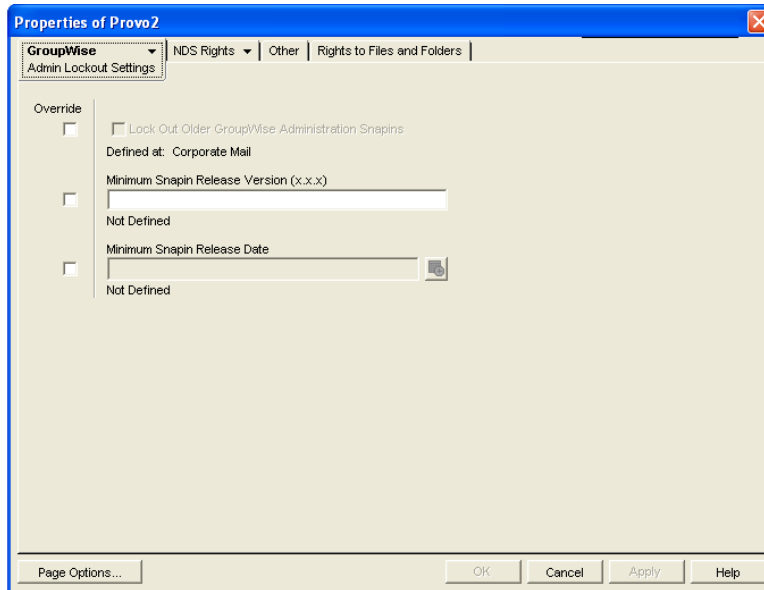
- 8 Click *GroupWise > Default WebAccess* to display the Default WebAccess page.

NOTE: This page applies only to domains that have not yet been updated to GroupWise 2012. GroupWise 2012 does not include the WebAccess Agent.



Use this page to designate the default WebAccess Agent (gateway) for the legacy domain.

- 9 Click *GroupWise > Admin Lockout Settings*.



Use this page to control the version of the GroupWise Administrator snap-ins to ConsoleOne that is allowed to access GroupWise databases. See [Section 4.2.6, "Admin Lockout Settings,"](#) on [page 76](#) for more information.

- 10 Click *OK* to save the new domain settings.

9.3 Converting a Secondary Domain to a Primary Domain

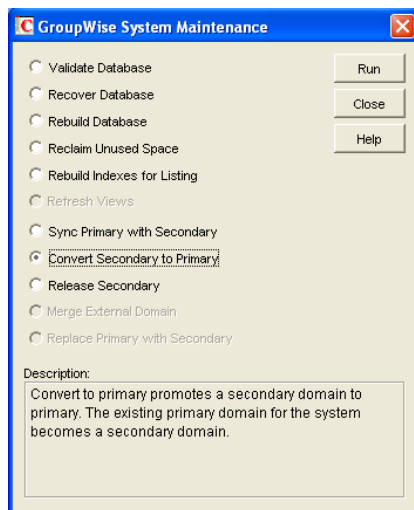
You can change which domain is primary if it becomes more convenient to administer the primary domain from a different location. You can, however, have only one primary domain at a time. When you convert a secondary domain to primary, the old primary domain becomes a secondary domain.

To convert a secondary domain to primary:

- 1 In ConsoleOne, connect to the primary domain.

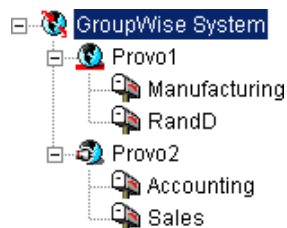
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, "Select Domain,"](#) on page 69.

- 2 Make sure there are no pending operations for the primary domain, as described in [Section 4.5, "Pending Operations,"](#) on page 80.
- 3 Browse to and select the secondary domain you want to convert.
- 4 Click *Tools > GroupWise Utilities > System Maintenance*.



- 5 Click *Convert Secondary to Primary*.
- 6 Specify the path to the secondary domain database, then click *OK*.

The GroupWise View in ConsoleOne displays the primary domain with a red underscore.



9.4 Replacing the Primary Domain Database with a Secondary Domain Database

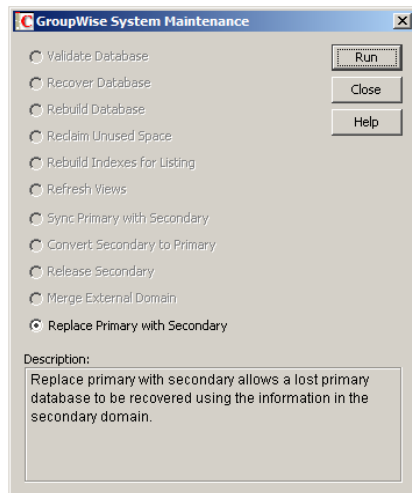
If the primary domain database (`wppdomain.db`) has become so damaged that it cannot be rebuilt, and if you do not have a current backup of it, you can replace the primary domain database with the contents of a secondary domain database. You should only do this if you are confident that the secondary domain database is completely synchronized with current GroupWise domain information.

To replace the primary domain database with the contents of a secondary domain database:

- 1 Make sure you have full administrative rights to the primary domain database directory.
- 2 Stop the MTA for the primary domain.
- 3 In ConsoleOne, connect to the secondary domain where the current database is located.

If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,”](#) on page 69.

- 4 Browse to and select the Domain object for the secondary domain.
- 5 Click *Tools > GroupWise Utilities > System Maintenance*.



- 6 Click *Replace Primary with Secondary > Run*.
- 7 When prompted, make sure the *Path to Database* field displays the path to the primary domain.
- 8 (Conditional) If an incorrect path is displayed, browse to and select the path to the primary domain database, then click *OK*.

ConsoleOne then updates the primary domain database with the current contents of the selected secondary domain database.

- 9 When the primary domain database has been replaced, restart the MTA for the primary domain.

9.5 Moving a Domain

You cannot use ConsoleOne to move a Domain object to a different location in the eDirectory tree because it is a container object. Only leaf objects can be moved. If you need to change the context, graft the GroupWise domain to its corresponding eDirectory object in the new container location. See [Section 5.15, “GW / eDirectory Association,” on page 99](#) for more information about grafting objects.

You can, however, move the domain directory and the domain database ([wpdomain.db](#)) by copying the domain directory structure and all its contents to the new location.

IMPORTANT: These instructions are for moving the domain from one location to another on the same platform. If you want to move a domain from a Windows server to a Linux server, follow the instructions in the [GroupWise Server Migration Guide](#).

- 1 Back up the domain, as described in [Chapter 31, “Backing Up GroupWise Databases,” on page 431](#).
- 2 In ConsoleOne, browse to and right-click the domain to move, then click *Properties* to display the domain Identification page.
- 3 In the *UNC Path* field, change the path to the location where you want to move the domain, then click *OK* to save the new location.

The format of the path in the *UNC Path* field depends on whether you are running Linux ConsoleOne or Windows ConsoleOne, and on whether the domain is on Linux or Windows. Retain the original format of the path in your modified version of the location.

The location change is propagated throughout your GroupWise system.

- 4 Stop the MTA, and if applicable, other agents (Internet Agent and Monitor Agent) that are running for the domain.
- 5 (Conditional) On Linux:
 - 5a In a terminal window, log in as *root*, then provide the *root* password.
 - 5b Use `cp` to copy the domain directory and database to the new location:

```
cp -r domain_directory destination
```

- 6 (Conditional) On Windows:
 - 6a Use `xcopy` with the `/s` and `/e` options to copy the domain directory and database to the new location:

```
xcopy domain_directory /s /e destination
```

These options re-create the same directory structure even if directories are empty.

- 6b Give rights to all objects that need to access the domain database.

For example, if the new location is on a different server, the Windows MTA and GroupWise administrators who run ConsoleOne need adequate rights to the new location, as described in [Chapter 87, “GroupWise Administrator Rights,” on page 1127](#).
- 7 Edit the MTA and other agent startup files to reflect the changes, then restart the MTA and other agents.

See [Section 42.1.7, “Adjusting the MTA for a New Location of a Domain or Post Office,” on page 640](#).
- 8 When you are sure the domain is functioning properly in its new location, delete the original domain directory and its contents.

If you need to move the MTA along with its domain, see [Section 42.1.6, “Moving the MTA to a Different Server,”](#) on page 640.

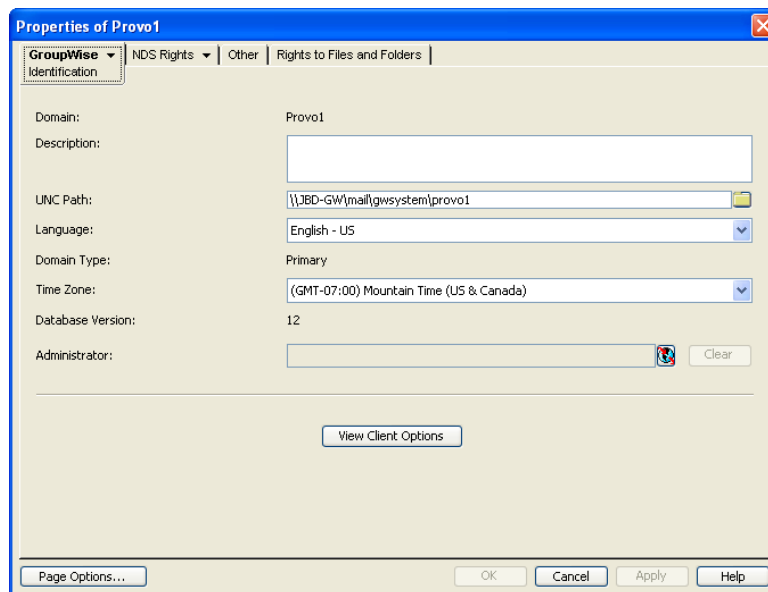
9.6 Deleting a Domain

You can delete a domain only when it no longer owns subordinate GroupWise objects. For example, you cannot delete the primary domain of your GroupWise system if it still owns secondary domains. You cannot delete a secondary domain if it still owns post offices. However, MTA and Gateway objects are automatically deleted along with the Domain object. Keep the MTA running until after you have deleted the domain, so that it can process the object deletion requests.

- 1 In ConsoleOne, connect to the primary domain.

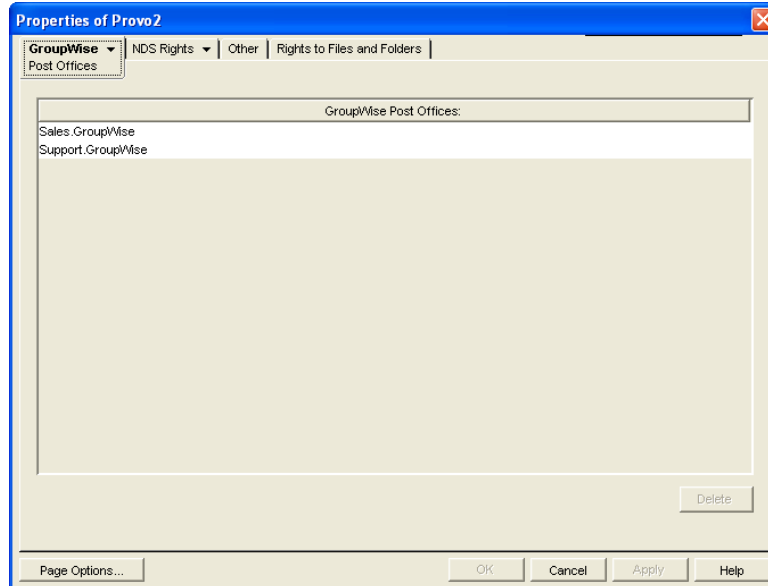
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,”](#) on page 69.

- 2 Browse to and right-click the Domain object you want to delete, then click *Properties* to display the domain Identification page.



- 3 Verify that the current directory path displayed on the domain Identification page is correct.

- 4 Click *Post Offices*, then move or delete any post offices that belong to this domain, as described in Section 12.10, “Moving a Post Office,” on page 212 and Section 12.11, “Deleting a Post Office,” on page 214.



- 5 Right-click the Domain object, then click *Delete* to delete the Domain object from eDirectory.
- 6 When prompted, click *Yes* to delete the corresponding domain directory structure.
- 7 Stop the MTA for the domain, as described in the following sections in the *GroupWise 2012 Installation Guide*:
 - ♦ “Stopping the Linux GroupWise Agents”
 - ♦ “Stopping the Windows GroupWise Agents”
- 8 Uninstall the MTA software if applicable, as described in the following sections in the *GroupWise 2012 Installation Guide*:
 - ♦ “Uninstalling the Linux GroupWise Agents”
 - ♦ “Uninstalling the Windows GroupWise Agents”

9.7 Changing the MTA Configuration to Meet Domain Needs

Because the MTA transfers messages between domains and between post offices in the same domain, it affects the domain itself, local users in post offices belonging to the domain, and users who exchanges messages with local users in the domain. Proper MTA configuration is essential for a smoothly running GroupWise system. Complete details about the MTA are provided in [Part X, “Message Transfer Agent,” on page 619](#). As you create and manage domains, you should keep in mind the following aspects of MTA configuration:

- ♦ [Section 42.2.1, “Restricting Message Size between Domains,” on page 642](#)
- ♦ [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,” on page 643](#)
- ♦ [Section 42.3.2, “Scheduling Direct Domain Links,” on page 647](#)
- ♦ [Section 44.1, “Optimizing TCP/IP Links,” on page 685](#)

10 Managing the Links between Domains and Post Offices

When you create a new secondary domain in your GroupWise system or a new post office in a domain, you configure one direct link to connect the new domain or post office to a domain in your GroupWise system. For simple configurations, this initial link might be adequate. For more complex configurations, you must modify link types and protocols to achieve optimum message flow throughout your GroupWise system.

The following topics help you manage links between domains and post offices:

- ♦ [Section 10.1, “Understanding Link Configuration,” on page 155](#)
- ♦ [Section 10.2, “Using the Link Configuration Tool,” on page 161](#)
- ♦ [Section 10.3, “Interpreting Link Symbols,” on page 168](#)
- ♦ [Section 10.4, “Modifying Links,” on page 169](#)

10.1 Understanding Link Configuration

In GroupWise, a link is defined as the information required to route messages between domains, post offices, and gateways in a GroupWise system. Initial links are created when domains, post offices, and gateways are created. The following topics help you understand link configuration:

- ♦ [Section 10.1.1, “Domain-to-Domain Links,” on page 155](#)
- ♦ [Section 10.1.2, “Domain-to-Post-Office Links,” on page 158](#)
- ♦ [Section 10.1.3, “Link Protocols for Direct Links,” on page 159](#)

10.1.1 Domain-to-Domain Links

The primary role of the MTA is to route messages from one domain to another. Domain links tell the MTA how to route messages between domains. Domain links are stored in the domain database (`wpdomain.db`). There are three types of links between source and destination domains:

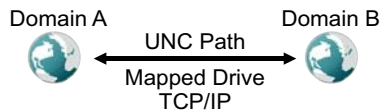
- ♦ [“Direct Links” on page 156](#)
- ♦ [“Indirect Links” on page 156](#)
- ♦ [“Gateway Links” on page 158](#)

As an alternative to configuring individual links between individual domains throughout your GroupWise system, you can establish a system of one or more routing domains. See [Section 42.3.1, “Using Routing Domains,” on page 645](#).

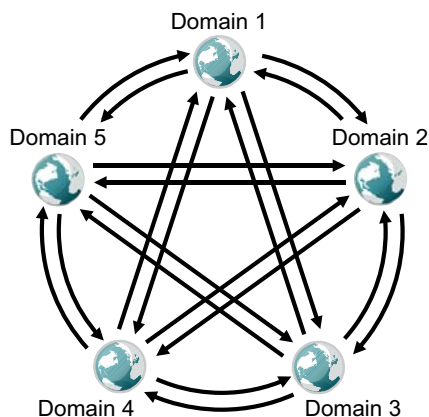
Direct Links

In a direct link between domains, the source domain's MTA communicates directly with the destination domain's MTA. If it is using a TCP/IP link, the source domain MTA communicates messages to the destination domain MTA by way of TCP/IP, which does not require disk access by the source MTA in the destination domain. This is the recommended configuration, and is the only option for domains on Linux.

If a Windows domain is using a mapped or UNC link, the source domain MTA writes message files into the destination domain MTA input queue, which does require disk access by the source MTA in the destination domain. For additional details about the configuration options for direct links, see [Section 10.1.3, "Link Protocols for Direct Links," on page 159](#).



Direct links can be used between all domains. This is a very efficient configuration but might not be practical in a large system.



Indirect Links

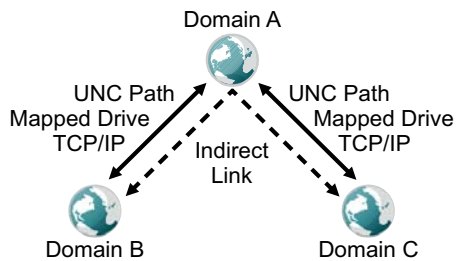
In an indirect link between domains, the source domain's MTA routes messages through one or more intermediate MTAs in other domains to reach the destination domain's MTA. In other words, an indirect link is a series of two or more direct links.

In large systems, direct links between each pair of domains might be impractical, so indirect links can be common. Properly configured links optimize message flow throughout your GroupWise system. A variety of indirect link configurations are possible, including:

- ♦ ["Simple Indirect Links" on page 157](#)
- ♦ ["Star Configuration" on page 157](#)
- ♦ ["Two-Way Ring Configuration" on page 158](#)
- ♦ ["Combination Configuration" on page 158](#)

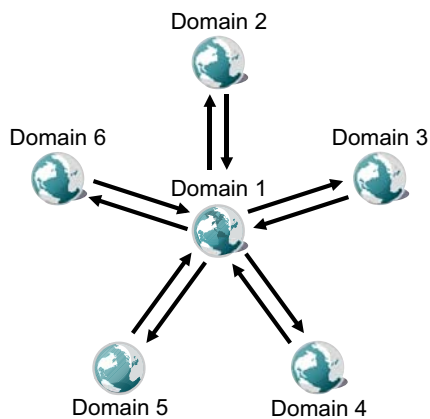
Simple Indirect Links

In simplest form, an indirect link can be used to pass messages between two domains that are not directly linked.



Star Configuration

In a star configuration, one central domain is linked directly to all other domains in the system. All other domains are indirectly linked to each other through the central domain.

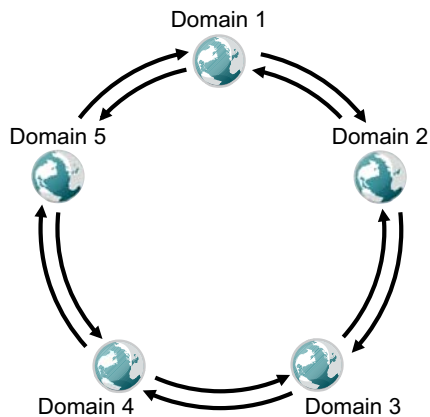


If you have more than ten domains, you might want to designate the central domain as a routing domain. The sole function of a routing domain is to transfer messages between other domains; it has no post offices of its own. See [Section 42.3.1, "Using Routing Domains,"](#) on page 645.

The major drawback of the star configuration is that the central domain is a single point of failure.

Two-Way Ring Configuration

In a two-way ring configuration, each domain is directly linked to the next and previous domains in the ring and indirectly linked to all other domains in the system.



An advantage of the two-way ring configuration is that it has no single point of failure. A disadvantage is that, depending on the size of the system, a message might go through several domains before arriving at its destination. A two-way ring works well in a system with five domains or less because transferring a message never requires more than two hops.

Combination Configuration

These three basic link configurations can be combined in any way to meet the needs of your GroupWise system.

Gateway Links

In a gateway link between domains, the sending domain's MTA must route the message through a gateway to reach its destination. Gateways can be used to:

- ♦ Link domains within your GroupWise system. See ["Using Gateway Links between Domains"](#) on page 636.
- ♦ Link your GroupWise system to another GroupWise system through an external domain. See ["Using Direct Links"](#) in ["Connecting to Other GroupWise Systems"](#) in the *GroupWise 2012 Multi-System Administration Guide*

For more information, see the [GroupWise Gateways Documentation Web site \(http://www.novell.com/documentation/gwgateways\)](http://www.novell.com/documentation/gwgateways).

NOTE: GroupWise gateways are legacy products and are not supported with the current GroupWise version.

You cannot locate a post office across a gateway link from its domain.

10.1.2 Domain-to-Post-Office Links

Between a domain and its post offices, all links must be direct links. There are no alternative link types between a domain and its post offices.

10.1.3 Link Protocols for Direct Links

The link protocol of a direct link between domains determines how the MTAs for the domains communicate with each other across the link. When you create a new domain, you must link it to an existing domain. This creates the initial domain-to-domain link.

Between a domain and a post office, the link protocol determines how the MTA transfers messages to the post office. Messages do not flow directly from one post office to another within a domain. Instead, they are routed through the domain. When you create a new post office, you must specify which domain it belongs to. This creates the initial domain-to-post-office link.

There are three link protocols for direct links between domains and between a domain and its post offices:

- ♦ [“TCP/IP Links” on page 159](#)
- ♦ [“Mapped Links” on page 159](#)
- ♦ [“UNC Links” on page 160](#)

NOTE: On Linux, TCP/IP links are required. On Windows, they are recommended.

TCP/IP Links

- ♦ [“Domain-to-Domain TCP/IP Links” on page 159](#)
- ♦ [“Domain-to-Post-Office TCP/IP Links” on page 159](#)

Domain-to-Domain TCP/IP Links

In a TCP/IP link between domains, the source MTA and the destination MTA communicate by way of TCP/IP rather than by writing message files into queue directories. The source MTA establishes a TCP/IP link with the destination MTA and transmits whatever messages need to go to that domain. The destination MTA receives the messages and routes them on to local post offices or to other domains as needed. During the process, message files are created in the [gwinprog](#) directory for backup purposes and are deleted when the TCP/IP communication process is completed.

Domain-to-Post-Office TCP/IP Links

In a TCP/IP link between a domain and a post office, you must configure both the POA and the MTA for TCP/IP. The source MTA establishes a TCP/IP link with the destination POA and transmits whatever messages need to go to that post office. The destination POA receives the messages and delivers them into mailboxes in the post office. During this process, message files are created in the POA input queue for backup purposes and are deleted when delivery is completed.

Mapped Links

Mapped links apply only to domains on Windows servers.

- ♦ [“Domain-to-Domain Mapped Links” on page 159](#)
- ♦ [“Domain-to-Post-Office Mapped Links” on page 160](#)

Domain-to-Domain Mapped Links

In a mapped link between domains, the location of the destination domain is specified in the following format:

drive:\domain_directory

The source MTA writes message files into its output queue at the following location:

drive:\domain_directory\wpcsin

The files are sent as input for the destination domain's MTA. Because drive mappings are changeable, you can move the domain directory structure, map its new location to the original drive letter, and the domain-to-domain link is still intact.

Domain-to-Post-Office Mapped Links

In a mapped link between a domain and a post office, the location of the post office is specified in the following format:

drive:\post_office_directory

The MTA writes message files into its output queue at the following location:

drive:\post_office_directory\wpcout

The files are sent as input for the post office's POA. Because drive mappings are changeable, you can move the post office directory structure, map its new location to the original drive letter, and the domain-to-post-office link is still intact.

UNC Links

UNC links apply only to domains on Windows servers.

- ♦ [“Domain-to-Domain UNC Links” on page 160](#)
- ♦ [“Domain-to-Post-Office UNC Links” on page 160](#)

Domain-to-Domain UNC Links

In a UNC link between domains, the location of the destination domain is specified in the following format:

\\server\volume\domain_directory

The source MTA writes message files into its output queue at the following location:

\\server\volume\domain_directory\wpcsin

The files are sent as input for the destination domain's MTA. Because UNC paths represent absolute locations on your network, if you move the domain to a new location, you need to edit the link to match.

Domain-to-Post-Office UNC Links

In a UNC link between a domain and a post office, the location of the post office is specified in the following format:

\\server\volume\post_office_directory

The MTA writes message files into its output queue at the following location:

\\server\volume\post_office_directory\wpcout

The files are sent as input for the post office's POA. Because UNC paths represent absolute locations in your network, if you move the post office to a new location, you need to edit the link to match.

10.2 Using the Link Configuration Tool

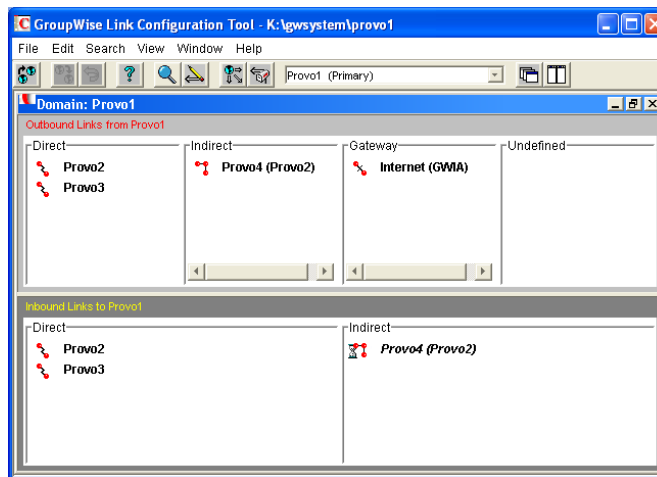
The Link Configuration tool helps you manage the links between the domains and post offices in your GroupWise system. The following topics help you perform basic link management tasks:

- ♦ Section 10.2.1, “Starting the Link Configuration Tool,” on page 161
- ♦ Section 10.2.2, “Editing a Domain Link,” on page 162
- ♦ Section 10.2.3, “Editing Multiple Domain Links,” on page 163
- ♦ Section 10.2.4, “Editing a Post Office Link,” on page 165
- ♦ Section 10.2.5, “Viewing the Path of an Indirect Link between Domains,” on page 165
- ♦ Section 10.2.6, “Viewing the Indirect Links Passing through a Domain,” on page 166
- ♦ Section 10.2.7, “Viewing the Gateway Links Passing through a Gateway,” on page 167
- ♦ Section 10.2.8, “Saving and Synchronizing Link Configuration Information,” on page 168





10.2.1 Starting the Link Configuration Tool





The Link Configuration tool is provided to help you change from default links to whatever link configuration best suits your GroupWise system.

- 1 In ConsoleOne, select the Domain object whose links you want to modify.
- 2 Click *Tools > GroupWise Utilities > Link Configuration* to display the Link Configuration Tool window.



The most frequently used features of the Link Configuration tool are available on the toolbar:

Button	Menu Equivalent	Function
	<i>File > Open</i>	Open a different domain database (wpdomain.db) to modify links in a different domain
	<i>File > Save</i>	Save the current link configuration information to the domain database
	<i>Edit > Undo</i>	Undo your changes to the link configuration (since the last save)
	<i>Help > Help</i>	Display online Help for the Link Configuration tool

Button	Menu Equivalent	Function
	<i>Search > Find</i>	Search for a specified domain
	Double-click object	Display details of the selected object
	<i>View > Domain Links</i>	View domain links for the selected domain
	<i>View > Post Office Links</i>	View post office links for the selected domain

3 Continue with a specific link management task:

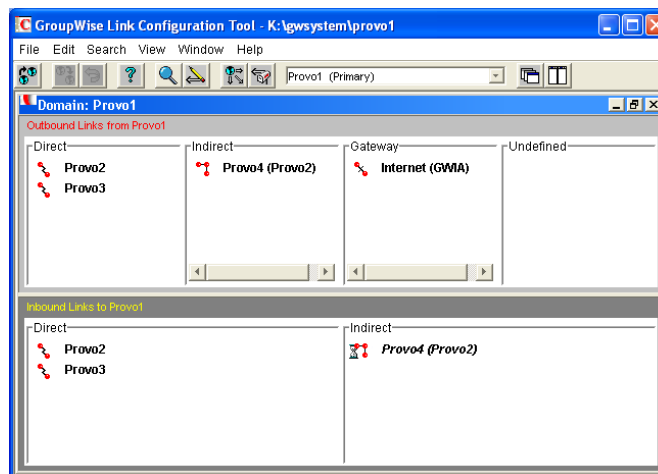
- ◆ [Section 10.2.2, “Editing a Domain Link,” on page 162](#)
- ◆ [Section 10.2.3, “Editing Multiple Domain Links,” on page 163](#)
- ◆ [Section 10.2.4, “Editing a Post Office Link,” on page 165](#)
- ◆ [Section 10.2.5, “Viewing the Path of an Indirect Link between Domains,” on page 165](#)
- ◆ [Section 10.2.6, “Viewing the Indirect Links Passing through a Domain,” on page 166](#)
- ◆ [Section 10.2.7, “Viewing the Gateway Links Passing through a Gateway,” on page 167](#)

10.2.2 Editing a Domain Link

After starting the Link Configuration tool:

- 1 From the drop-down list, select the domain whose links you want to edit.
- 2 Click *View > Domain Links* to display domain links.

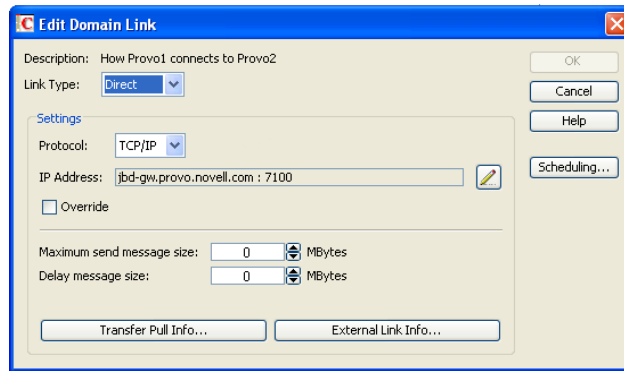
Outbound and inbound links for the selected domain are listed.



- 3 Double-click a domain in the *Outbound* Links list to edit the link to that domain from the selected domain.

or

Double-click a domain in the *Inbound Links* list to edit the link from that domain to the selected domain.



TIP: You can also open the Edit Domain Link dialog box by dragging a domain from one link type to another.

- 4 Select the link type:
 - ◆ “Direct Links” on page 156
 - ◆ “Indirect Links” on page 156
 - ◆ “Gateway Links” on page 158
- 5 For a direct link, select the link protocol:
 - ◆ “Mapped Links” on page 159
 - ◆ “UNC Links” on page 160
 - ◆ “TCP/IP Links” on page 159
- 6 Provide the location of the domain in the format appropriate to the selected protocol.
- 7 Click *OK*.
- 8 Repeat [Step 1](#) through [Step 7](#) for whatever links you need to modify.

As a time-saving measure, you can make a new domain’s links the same as an existing domain’s links. Click *Edit > Default Links*, then click the domain whose links you want to use as a pattern for the new domain. Select *Outbound* and/or *Inbound* as needed, then click *OK*.

To look at the same link information from different points of view, you can start the Link Configuration tool multiple times to open multiple Link Configuration Tool windows.

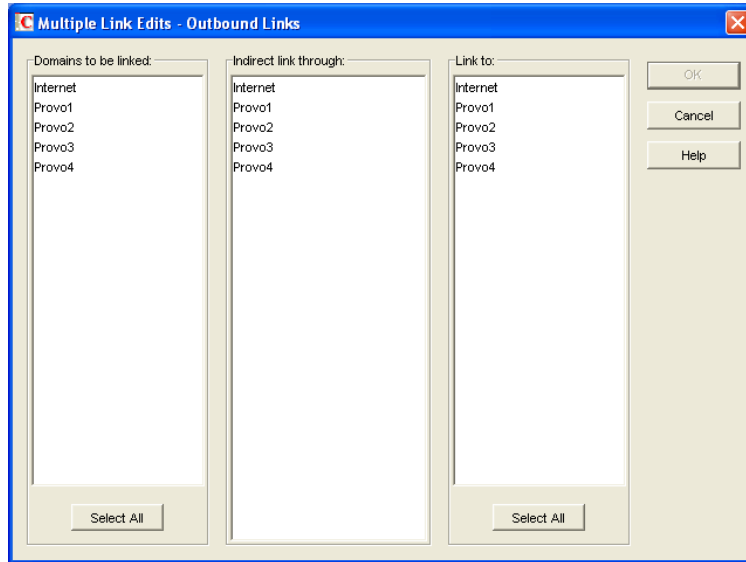
- 9 To exit the Link Configuration Tool and save your changes, click *File > Exit > Yes*.

10.2.3 Editing Multiple Domain Links

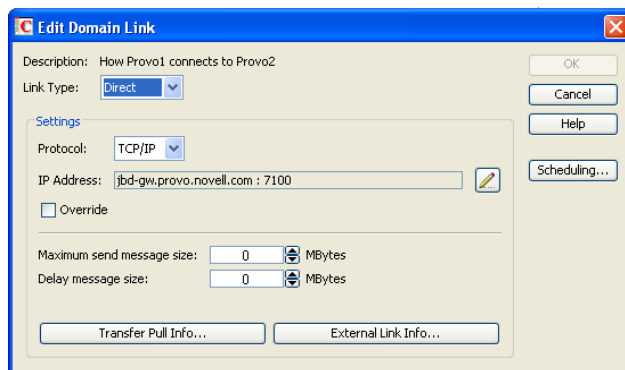
When your GroupWise system includes indirect links, it is not unusual for several domains to link to the same domain. As a time-saving measure, you can create links from multiple domains to the same domain in one operation.

After starting the Link Configuration tool:

- 1 Click *Edit > Multiple Link Edits*.



- 2 In the *Domains to Be Linked* column, select the source domains whose outgoing links you want to modify.
- 3 In the *Indirect Link Through* column, select the intermediate domain through which you want the indirect links to pass.
- 4 In the *Link To* column, select one or more destination domains.
- 5 Click *OK*.
- 6 Fill in the fields in the *Edit Domain Link* dialog box for each direct link between a source domain and the intermediate domain, as described in [Section 10.2.2, "Editing a Domain Link,"](#) on [page 162](#), then click *OK*.



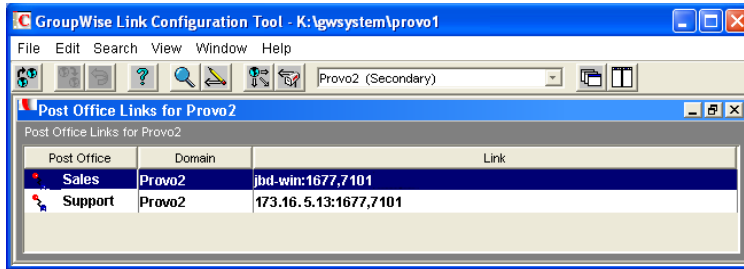
The *Edit Domain Link* dialog box continues to appear until you have defined all the direct links between the source domains and the intermediate domain.

IMPORTANT: After defining links from the source domains to the intermediate domain, make sure the links from the intermediate domain to other domains are set up the way you want them.

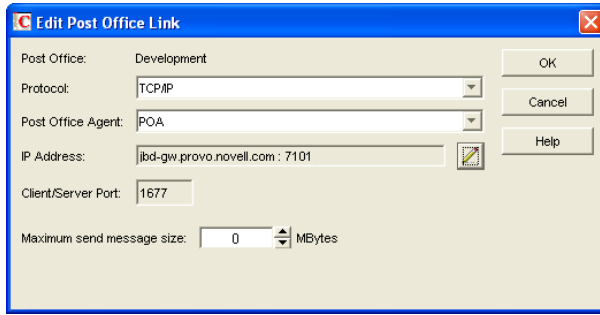
10.2.4 Editing a Post Office Link

After starting the Link Configuration tool:

- 1 From the drop-down list, select the domain whose post office link you want to edit.
- 2 Click *View > Post Office Links* to display post office links.



- 3 Double-click a post office to edit the link from the domain to the post office.



- 4 Select the link protocol for the direct link.
 - ♦ [“Mapped Links” on page 159](#)
 - ♦ [“UNC Links” on page 160](#)
 - ♦ [“TCP/IP Links” on page 159](#)
- 5 Provide the location of the post office in the format appropriate to the selected protocol.
- 6 For a TCP/IP link, provide the message transfer port number where you want the POA to listen for incoming messages from the MTA.

The default message transfer port for the POA is 7101.
- 7 Click OK.
- 8 To exit the Link Configuration tool and save your changes, click *File > Exit > Yes*.

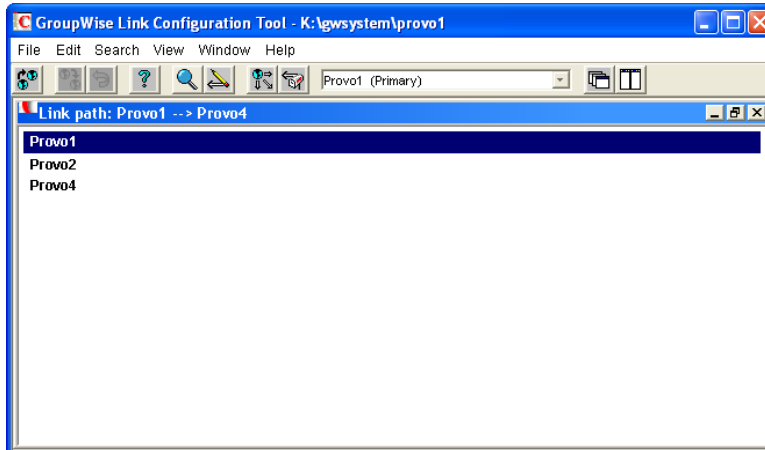
10.2.5 Viewing the Path of an Indirect Link between Domains

The more hops between two indirectly linked domains, the longer it takes a message to travel between them. To make sure the number of hops between two indirectly linked domains is as small as possible, you can list the route a message would take from one domain to the other in ConsoleOne.

After starting the Link Configuration tool:

- 1 Select a domain from the drop-down list.
- 2 Select a domain in the Indirect links list.

- 3 Click *View > Link Path* to see a list of the hops between the two domains.



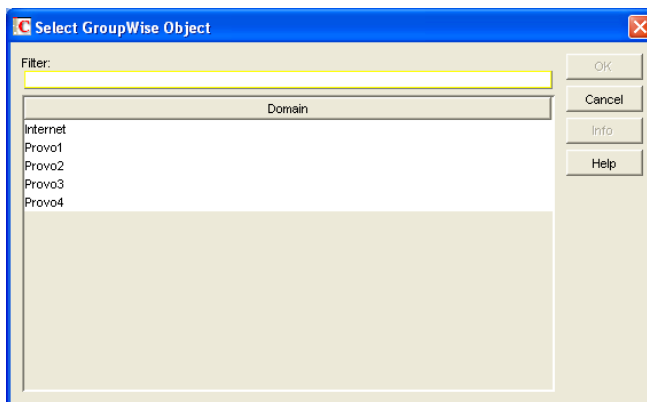
You can also use GroupWise Monitor to trace the path a message would take between two domains. See [Section 71.3.1, “Link Trace Report,”](#) on page 979.

10.2.6 Viewing the Indirect Links Passing through a Domain

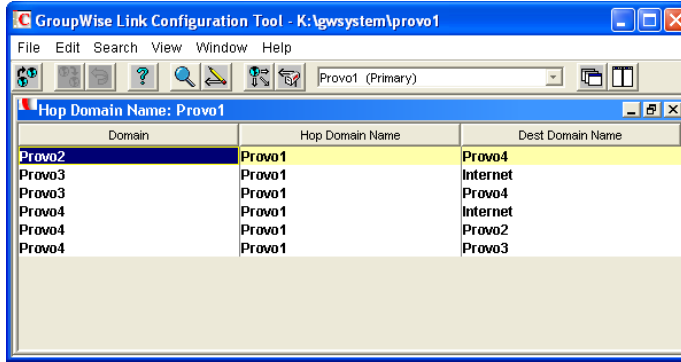
If a domain serves as a hop in an indirect link, making changes to that domain could affect all indirect links passing through that domain. You can list all the indirect links that pass through a domain in ConsoleOne.

After starting the Link Configuration tool:

- 1 Click *View > Link Hop* to list all domains in your system.



- 2 Double-click a domain to list the indirect links passing through it.



- 3 If you need to reroute a link, right-click the link, then click *Edit* to open the Edit Domain Link dialog box and make changes as needed.

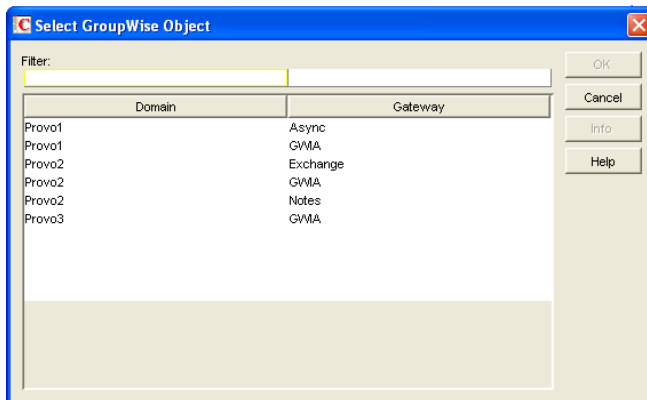
You can also use GroupWise Monitor to check the links passing through a selected domain. See [Section 71.3.2, "Link Configuration Report," on page 980](#). However, you cannot change link information using Monitor.

10.2.7 Viewing the Gateway Links Passing through a Gateway

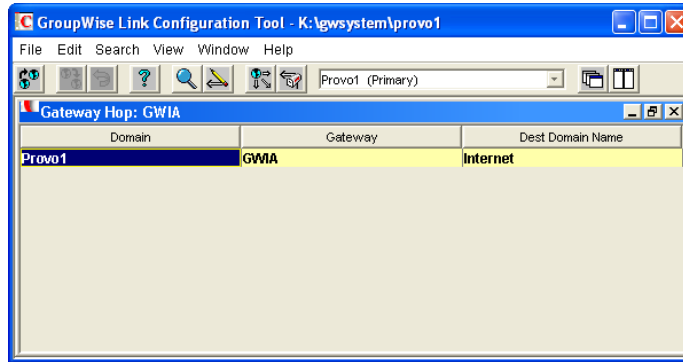
Before making changes to a gateway, you can list all the links that pass through the gateway.

After starting the Link Configuration tool:

- 1 Click *View > Gateway Hop* to list all gateways in your system.



- 2 Double-click a gateway to list the domains linked through that gateway.



- 3 If you need to reroute a link, right-click the link, then click *Edit* to open the Edit Domain Link dialog box and make changes as needed.

10.2.8 Saving and Synchronizing Link Configuration Information

Whenever you modify link configuration information, a cautionary symbol (see [Section 10.3.2, “Link Status Symbols,” on page 169](#)) appears next to the modified link until you save the current link configuration by clicking *Edit > Save*. If you are making extensive changes to link configuration information, you should save regularly. When you save, the information is written out to the domain database (`wdomain.db`) for the domain to which you are currently connected. You can change to a different domain database without exiting the Link Configuration tool by clicking *File > Open*.

The MTA routinely synchronizes the information in the domain databases throughout your GroupWise system. If you are making extensive changes to link configuration information, you can synchronize the information immediately by clicking *Edit > Synchronize*.


10.3 Interpreting Link Symbols

As you modify links, you see symbols that represent the various link types. Along with the link type symbols, you sometimes see link status symbols.





- [Section 10.3.1, “Link Type Symbols,” on page 168](#)
- [Section 10.3.2, “Link Status Symbols,” on page 169](#)

10.3.1 Link Type Symbols

Link Type Symbol	Meaning
	Direct link
	Indirect link
	Gateway link
	TCP/IP link to domain
	TCP/IP link to post office

Link Type Symbol	Meaning
	Undefined link

10.3.2 Link Status Symbols

Link Status Symbol	Meaning
	Link modification not yet saved
	Link modification not yet synchronized
	Insufficient rights to modify link
	Rights not yet checked

10.4 Modifying Links

In [Part IX, “Post Office Agent,” on page 469](#) and [Part X, “Message Transfer Agent,” on page 619](#), detailed instructions for changing link types are provided as outlined below:

Changing the Link Protocol between the Post Office and the Domain

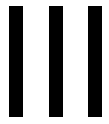
- ♦ [“Using TCP/IP Links between the Post Office and the Domain” on page 487](#)
- ♦ [“Using Mapped or UNC Links between the Post Office and the Domain” on page 489](#)

Changing the Link Protocol between Domains

- ♦ [“Using TCP/IP Links between Domains” on page 632](#)
- ♦ [“Using Mapped or UNC Links between Domains” on page 635](#)
- ♦ [“Using Gateway Links between Domains” on page 636](#)

Customizing Link Configuration

- ♦ [“Using Routing Domains” on page 645](#)
- ♦ [“Scheduling Direct Domain Links” on page 647](#)
- ♦ [“Using a Transfer Pull Configuration \(Windows Only\)” on page 650](#)



Post Offices

- ◆ [Chapter 11, “Creating a New Post Office,” on page 173](#)
- ◆ [Chapter 12, “Managing Post Offices,” on page 189](#)

11 Creating a New Post Office

As your GroupWise system grows, you typically need to add new post offices.

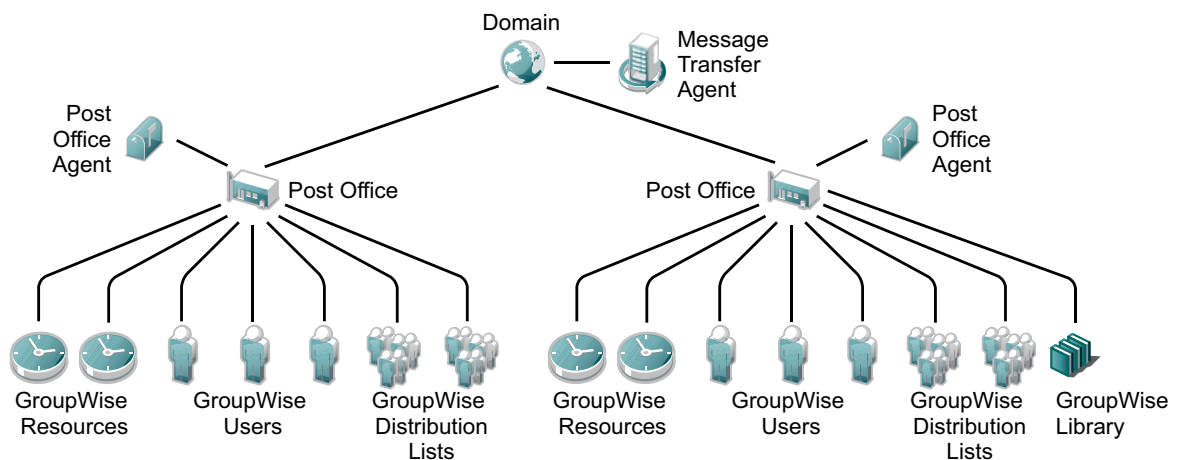
- ♦ Section 11.1, “Understanding the Purpose of Post Offices,” on page 173
- ♦ Section 11.2, “Planning a New Post Office,” on page 174
- ♦ Section 11.3, “Setting Up the New Post Office,” on page 181
- ♦ Section 11.4, “What’s Next,” on page 186
- ♦ Section 11.5, “New Post Office Summary Sheet,” on page 187

IMPORTANT: If you are creating a new post office in a clustered GroupWise system, see the [GroupWise 2012 Interoperability Guide](#) before you create the post office:

11.1 Understanding the Purpose of Post Offices

The post office serves as an administrative unit for a group of users and is used for addressing messages. Each GroupWise user has a unique GroupWise address that consists of a user ID, the user’s post office name, the GroupWise domain name, and, optionally, an Internet domain name.

The following diagram illustrates the logical organization of a GroupWise domain with multiple post offices. The two post offices belong to the domain. All of the objects under each post office belong to that post office.



As illustrated above, each post office must have at least one Post Office Agent (POA) running for it. The POA delivers messages to users’ mailboxes and performs a variety of post office and mailbox maintenance activities.

When you add a new post office, you must link it to a domain. The link defines how messages travel between the post office and its domain. Links are discussed in detail in [Chapter 10, “Managing the Links between Domains and Post Offices,”](#) on page 155.

Physically, a post office consists of a set of directories that house all the information stored in the post office. To view the structure of the post office directory, see [“Post Office Directory”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*. The post office directory contains user mailboxes and messages, as well as other vital information. For an overview, see [Section 35.3, “Information Stored in the Post Office,”](#) on page 472.

11.2 Planning a New Post Office

This section provides the information you need in order to decide when, where, and how to create a new post office. The [“New Post Office Summary Sheet”](#) on page 187 lists all the information you need as you set up your post office. The items in the summary sheet are listed in the order you enter them when setting up your post office. This planning section does not follow the same order as the summary sheet, but all summary sheet items are covered. You should print the summary sheet and fill it out as you complete the tasks listed below.

- ◆ [Section 11.2.1, “Determining When to Add a Post Office,”](#) on page 174
- ◆ [Section 11.2.2, “Selecting the Domain That the Post Office Belongs To,”](#) on page 176
- ◆ [Section 11.2.3, “Determining the Context for the Post Office Object,”](#) on page 176
- ◆ [Section 11.2.4, “Choosing the Post Office Name,”](#) on page 176
- ◆ [Section 11.2.5, “Deciding Where to Create the Post Office Directory,”](#) on page 177
- ◆ [Section 11.2.6, “Deciding Where to Install the Agent Software,”](#) on page 178
- ◆ [Section 11.2.7, “Deciding How to Link the New Post Office,”](#) on page 178
- ◆ [Section 11.2.8, “Selecting the Post Office Language,”](#) on page 179
- ◆ [Section 11.2.9, “Selecting the Post Office Time Zone,”](#) on page 179
- ◆ [Section 11.2.10, “Selecting a Software Distribution Directory,”](#) on page 179
- ◆ [Section 11.2.11, “Selecting a Post Office Security Level,”](#) on page 180
- ◆ [Section 11.2.12, “Deciding if You Want to Create a Library for the New Post Office,”](#) on page 180

After you have completed the tasks and filled out the [“New Post Office Summary Sheet”](#) on page 187, you are ready to continue with [Section 11.3, “Setting Up the New Post Office,”](#) on page 181.

11.2.1 Determining When to Add a Post Office

After you have your basic GroupWise system up and running, you can expand it to accommodate additional users. How do you know when you should add a post office? The answer to this depends on your company organization, the number of users on your network, and the physical limitations of your network servers.

- ◆ **Physical Organization:** If your network spans several sites, you might want to create post offices (if not domains) at each physical location. This reduces the demands on long distance network links.
- ◆ **Logical Organization:** Processing messages within a post office is faster and typically generates less network traffic than messages traveling between different post offices. As you expand GroupWise, you might find it useful to add post offices in order to group users who frequently send mail to each other.

Grouping users into post offices, based upon company organization or job function, makes administrative tasks, such as creating distribution lists, limiting Address Book visibility, and distributing shared folders, easier. For example, some employees might work in corporate functions like accounting and human resources. Other employees might be involved in sales and marketing and frequently attend meetings together, requiring frequent busy searches. Some areas, for example the production floor, might not need a workstation or user account for each individual.

- ◆ **Number of Users:** A GroupWise post office can support more than 10,000 users. However, the number of users that a single post office can support effectively is influenced by many factors, including:
 - ◆ **User activity level**

A post office where most users send and receive a large number of messages would support fewer users effectively than would a post office where users send messages only occasionally.
 - ◆ **User access methods**

A post office where most users use the Windows client in Online mode would support fewer users effectively than would a post office where most users use Caching mode.

Users who synchronize their mobile devices with their GroupWise mailboxes also increase the load on the post office.
 - ◆ **Server disk speed/throughput**

The POA's activities are very disk intensive. A post office on a very high-speed server or SAN can support more users effectively than a post office on slower hardware.
 - ◆ **Number of post offices on a single server**

Having only one post office on a server is highly recommended. If hardware constraints require multiple post offices on a single server, each post office would effectively support fewer users than if the post office was located on its own server.
 - ◆ **Number of users affected by a down server or POA**

If a problem occurs with a server or POA, fewer users are affected when the post office is smaller.
 - ◆ **Maintenance time requirements**

The time required to perform post office and mailbox maintenance activities including backups can become excessive for a very large post office.
 - ◆ **Room for growth**

The ideal size for a new post office allows room to grow while maintaining optimal performance.
- ◆ **Demand on the POA:** The POA is a very flexible component of your GroupWise system. Many aspects of its functioning are configurable, to meet the particular needs of the post office it services, no matter what the size. See [Chapter 36, "Configuring the POA," on page 481](#) and [Chapter 38, "Optimizing the POA," on page 559](#).

In addition, you can choose to run multiple POAs for the same post office, in order to specialize its functioning, as described in:

- ◆ [Section 38.1.3, "Configuring a Dedicated Client/Server POA \(Windows Only\)," on page 562](#)
- ◆ [Section 38.2.2, "Configuring a Dedicated Message File Processing POA \(Windows Only\)," on page 565](#)
- ◆ [Section 39.5, "Configuring a Dedicated Indexing POA \(Windows Only\)," on page 577](#)
- ◆ [Section 38.4.2, "Configuring a Dedicated Database Maintenance POA \(Windows Only\)," on page 568](#)

As a result, the choice is up to you whether you prefer a single, large post office, perhaps with multiple POAs, or multiple smaller post offices, each with its own POA. For additional guidance with determining post office size, visit the [GroupWise Best Practices Wiki \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

11.2.2 Selecting the Domain That the Post Office Belongs To

A post office is associated with a specific domain, even though it might reside in a different organizational unit in the eDirectory tree. If you have just one domain, the new post office will belong to it. If you want to create a new domain as well as a new post office, see [Chapter 8, “Creating a New Domain,” on page 131](#).

Domains function as the main administration units for the GroupWise system. Post office information is stored in the domain database, as well as in the post office database. Changes are distributed to each post office database from the domain.

NEW POST OFFICE SUMMARY SHEET

Under *GroupWise Domain*, specify the GroupWise domain that the new post office will belong to.

11.2.3 Determining the Context for the Post Office Object

The eDirectory context of the Post Office object determines how you administer the post office. The post office can be created in any Organization or Organizational Unit container in any context as long as it is in the same tree as the domain. The same principles apply to placing Post Office objects in the eDirectory tree as apply for Domain objects. Review [Section 8.2.4, “Determining the Context for the Domain Object,” on page 134](#) to help you plan the context for the Post Office object.

NEW POST OFFICE SUMMARY SHEET

Under *Tree Name*, specify the name of the eDirectory tree of the domain that will own the new post office.

Under *eDirectory Container*, specify the name of the eDirectory container where you want to create the new post office.

11.2.4 Choosing the Post Office Name

The post office must be given a unique name. The name is used for addressing and routing purposes within GroupWise, and might appear in the GroupWise Address Book.

The post office name can reflect a location, organization, department, and so on. For example, you might want the domain name to be the location (for example, Provo) while the post office name is one of the company’s departments (for example, Research). Name the new post office carefully. After it is created, the name cannot be changed.

The post office name should consist of a single string. Use underscores (_) rather than spaces as separators between words to facilitate addressing across the Internet.

Do not use any of the following invalid characters in the post office name:

- | | |
|-----------------------|----------------|
| ASCII characters 0-31 | Comma , |
| Asterisk * | Double quote " |

At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

NEW POST OFFICE SUMMARY SHEET

Under *Post Office Name*, specify the post office name.

Under *Post Office Description*, provide a description for the post office to help you identify its function in the system.

11.2.5 Deciding Where to Create the Post Office Directory

Logically, the Post Office object resides in eDirectory and is administered through ConsoleOne. Physically, the post office has a directory structure for databases, message queues, and other files. The post office directory structure can be created on any of the supported platforms listed in “[GroupWise Administration Requirements](#)” in the *GroupWise 2012 Installation Guide*. The server where you create the post office directory structure can be in the same tree as the Post Office object or in another tree.

When you are planning the post office directory location and which users will belong to the post office, consider the following:

- ◆ **Post Office Directory Space Requirements:** The post office directory can be a large consumer of disk space. The amount of disk space required is influenced by many factors, including:
 - ◆ Number of users in the post office
 - ◆ Activity level of users
 - ◆ Number and typical size of attachments
 - ◆ Online mode vs. Caching mode for Windows client users
 - ◆ Archive and deletion policies
 - ◆ Libraries and document storage

For guidance on post office directory space requirements, visit the [GroupWise Best Practices Wiki](http://wiki.novell.com/index.php/GroupWise) (<http://wiki.novell.com/index.php/GroupWise>).

For details about managing post office disk space, see [Section 12.3, “Managing Disk Space Usage in the Post Office,”](#) on page 196.

- ◆ **Access by the POA:** For best performance, the POA should be installed on the same server as the post office directory. This is required on Linux. Remote installation is possible on Windows, but not recommended.
- ◆ **Security from User Access:** Users typically access their mailboxes through a TCP/IP connection to the POA. Therefore, users do not need access to the post office directory. You should create it in a location you can easily secure; otherwise, you could have files inadvertently moved or deleted.

Choose an empty directory for the new post office. If you want, the directory can reflect the name of the post office, for example research for the Research post office. Use the following platform-specific conventions:

Linux: Use only lowercase characters.

Windows: No limitations.

Choose the name and path carefully. After the post office directory is created, it is difficult to rename it. If the directory you specify does not exist, it is created when you create the post office. If you create the directory in advance, it is easy to browse to it as you create the post office.

IMPORTANT: Do not create the post office directory under domain directory or another post office directory.

NEW POST OFFICE SUMMARY SHEET

Under *Post Office Database Location*, specify the full path for the post office directory.

11.2.6 Deciding Where to Install the Agent Software

You must run a new instance of the POA for each new post office. To review the functions of the POA for the post office, see [Section 35.5, “Role of the Post Office Agent,” on page 477](#). For complete POA installation instructions and system requirements, see “[Installing GroupWise Agents](#)” in the [GroupWise 2012 Installation Guide](#).

You can install the POA on Linux or Windows. You should install it on the same server where you plan to create the post office directory structure.

NEW POST OFFICE SUMMARY SHEET

Under *Agent Platform*, specify the platform where the POA will run (Linux or Windows).

11.2.7 Deciding How to Link the New Post Office

When you create a new post office, you have the opportunity to choose the type of link to use between the new post office and its domain. For a review of link types, see [Section 10.1.2, “Domain-to-Post-Office Links,” on page 158](#).

When you create the new post, you link it to its domain. By default, this link is a direct link using TCP/IP as the link protocol, which means the new post office’s POA communicates with the domain’s MTA through TCP/IP. This is the recommended configuration, and is required on Linux.

On Windows, you can configure the direct link to use a UNC path or a mapped drive as the link protocol, which means the new post office’s POA transfers information to and from the existing domain by accessing the existing domain’s directory, rather than by communicating with the other domain’s MTA.

NEW POST OFFICE SUMMARY SHEET

Under *Link to Domain*, indicate the type of link you plan to set up between the new post office and its domain.

11.2.8 Selecting the Post Office Language

The post office language determines the sort order for items in the GroupWise Address Book.

The post office defaults to the same language as its domain unless you specify otherwise. For example, if you set the domain and post office language to English-US, the Address Book items are sorted according to English-US sort order rules. This is true even if some users in the post office are running non-English GroupWise clients such as German or Japanese. Their client interface and Help files are in German or Japanese, but the Address Book sort order is according to English-US standards. Time, date, and number formats for the non-English clients defaults to the workstation language.

NEW POST OFFICE SUMMARY SHEET

Under *Post Office Language*, specify the post office language.

11.2.9 Selecting the Post Office Time Zone

When a message is sent from a user in one time zone to a user in another time zone, GroupWise adjusts the message's time so that it is correct for the recipient's time zone. For example, if a user in New York (GMT -05:00, Eastern Time) schedules a user in Los Angeles (GMT -08:00, Pacific Time) for a conference call at 4:00 p.m. Eastern Time, the appointment is scheduled in the Los Angeles user's calendar at 1:00 p.m. Pacific Time.

The post office defaults to the same time zone as its domain unless you specify otherwise.

NEW POST OFFICE SUMMARY SHEET

Under *Time Zone*, specify the time zone for the new post office.

11.2.10 Selecting a Software Distribution Directory

An initial software distribution directory was created when your GroupWise system was first set up, as described in "[GroupWise Software Distribution Directory](#)" in "[Installing a Basic GroupWise System](#)" in the *GroupWise 2012 Installation Guide*.

The software distribution directory contains files that users need in order to set up the GroupWise Windows client on their workstations. Additional software distribution directories might have been created since that time to accommodate users in various locations, as described in [Section 4.9, "Software Directory Management,"](#) on page 84.

You can select the most convenient software distribution directory for the new post office.

NEW POST OFFICE SUMMARY SHEET

Under *Software Distribution Directory*, specify the name of the software distribution directory from which users in the new post office will install the GroupWise client software on their Windows workstations.

11.2.11 Selecting a Post Office Security Level

Post office security settings affect two types of GroupWise users:

- ♦ Users who do not have personal GroupWise passwords set on their mailboxes
- ♦ Users who use LDAP passwords (that is, passwords required to log in to the network through an LDAP server) instead of personal GroupWise passwords to access their mailboxes

After a user sets a personal GroupWise password on his or her mailbox, the post office security level no longer applies. The user is always prompted for the GroupWise password unless the administrator has set certain client options in ConsoleOne to prevent the password prompt, as described in [Section 82.1.3, “Managing GroupWise Passwords,”](#) on page 1100.

In the absence of personal GroupWise passwords on user mailboxes, the post office security level takes effect. By default, a new post office is created with High Security, which provides protection to GroupWise mailboxes through types of authentication other than personal GroupWise passwords. In a High Security post office, you can choose between eDirectory authentication and LDAP authentication:

- ♦ **eDirectory Authentication:** If you use eDirectory authentication for a post office, users must be logged in to the network through eDirectory in order to access their GroupWise mailboxes.
- ♦ **LDAP Authentication:** If you use LDAP authentication for a post office, users must successfully authenticate to an LDAP server, such as for network login, in order to access their GroupWise mailboxes.

For more information, see [Section 36.3, “Configuring Post Office Security,”](#) on page 505 and [Section 82.1, “Mailbox Passwords,”](#) on page 1099.

IMPORTANT: In a Low Security post office, mailboxes are completely unprotected. Without a personal GroupWise password, any user’s mailbox could be accessed by another user who knows how to use the `@u-userID` startup switch. This security level is not recommended.

NEW POST OFFICE SUMMARY SHEET

Under *Post Office Security Level*, mark the security level for the post office. If you choose High Security, indicate the type of authentication you plan to use.

11.2.12 Deciding if You Want to Create a Library for the New Post Office

If you anticipate that users on this post office will require document management services, you can create a library at the same time you create the post office. The library is created with all of the default library options including Store Documents at Post Office. Using a document storage area is preferable to storing documents at the post office because a document storage area can be moved. You should appropriately configure the library immediately after it is created, before users begin to store documents there.

NEW POST OFFICE SUMMARY SHEET

Under *Create Library*, indicate whether or not you want to immediately create a library for the new post office. You can always add a library to the post office at a later time.

If you decide to create a library for the post office, see [Part VII, “Libraries and Documents,”](#) on page 313 for instructions on configuring the library.

11.3 Setting Up the New Post Office

You should have already reviewed [Section 11.2, “Planning a New Post Office,”](#) on page 174 and filled out the [New Post Office Summary Sheet](#). Complete the following tasks to create a new post office.

- ♦ [Section 11.3.1, “Creating the New Post Office,”](#) on page 181
- ♦ [Section 11.3.2, “Configuring the POA for the New Post Office,”](#) on page 185
- ♦ [Section 11.3.3, “Installing and Starting the New POA,”](#) on page 186
- ♦ [Section 11.3.4, “Setting Up User Access to the New Post Office,”](#) on page 186

11.3.1 Creating the New Post Office

- 1 Make sure that you are logged in to the tree where you want to create the post office.

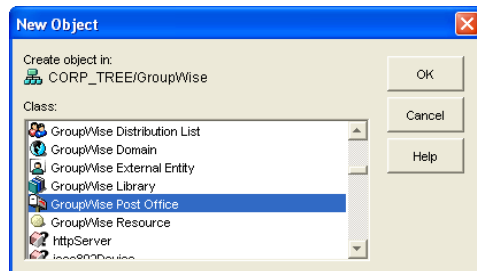
This must be the same tree as the domain that the post office belongs to (*Tree Name* on the [New Post Office Summary Sheet](#)).

- 2 (Conditional) If you are creating the post office on a different machine from where you are running ConsoleOne, make sure that ConsoleOne has write access to the location where you want to create the post office.

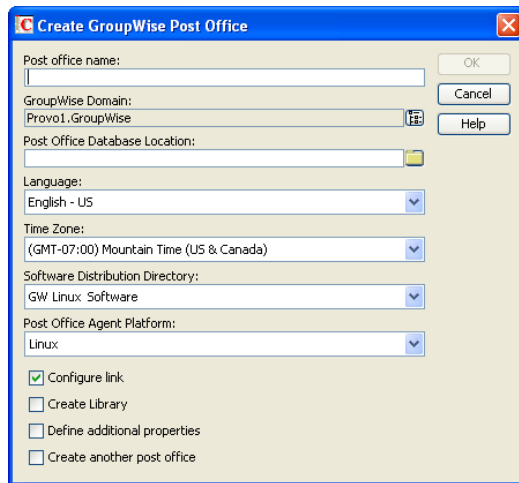
Linux: Mount the file system where you want to create the new post office. For assistance, see [Section 2.1, “ConsoleOne on Linux,”](#) on page 39.

Windows: Map a drive to the location where you want to create the new post office.

- 3 In ConsoleOne, browse to and right-click the eDirectory container where you want to create the post office (*eDirectory Container* on the [New Post Office Summary Sheet](#)), then click *New > Object*.

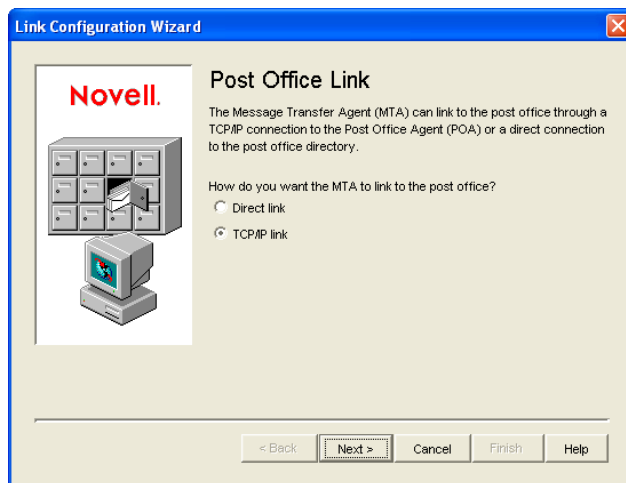


- 4 Double-click GroupWise Post Office, then fill in the fields in the Create GroupWise Post Office dialog box from your [New Post Office Summary Sheet](#).



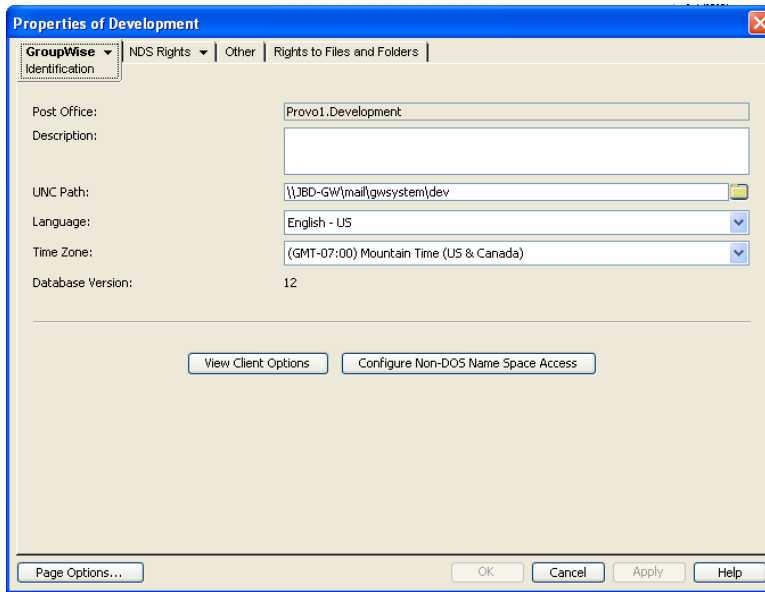
[Post Office Name](#)
[GroupWise Domain](#)
[Post Office Database Location](#)
[Post Office Language](#)
[Post Office Time Zone](#)
[Software Distribution Directory](#)
[Create Library](#)

- 5 Make sure the *Configure Links* and *Define Additional Properties* options are selected, then click *OK* to display the Link Configuration Wizard.

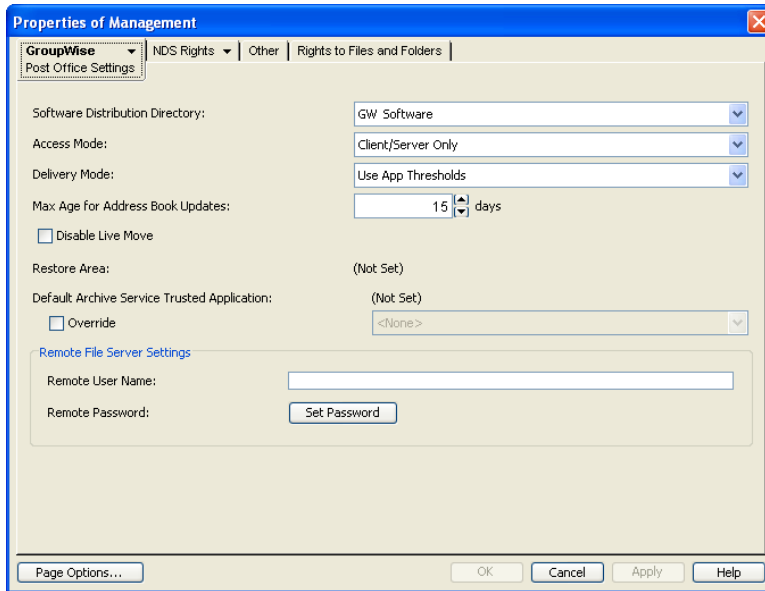


- 6 Follow the on-screen instructions to define how the post office links to its domain ([Link to Domain](#) on the [New Post Office Summary Sheet](#)).

When you finish defining the link, ConsoleOne creates the Post Office object and displays the post office Identification page.

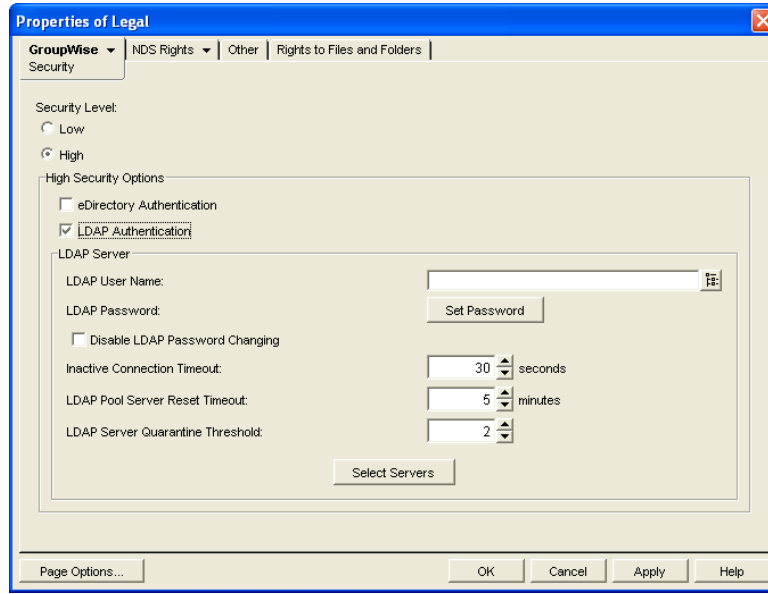


- 7 Provide a description for the new post office ([Description](#) on the [New Post Office Summary Sheet](#)).
- 8 Click *GroupWise > Post Office Settings* to display the Post Office Settings page.



- 9 Select the software distribution directory for the post office ([Software Distribution Directory](#) on the [New Post Office Summary Sheet](#)).

10 Click *GroupWise > Security* to display the Security page.



11 Provide the post office security level and authentication type for the post office ([Post Office Security Level](#) on the [New Post Office Summary Sheet](#)).

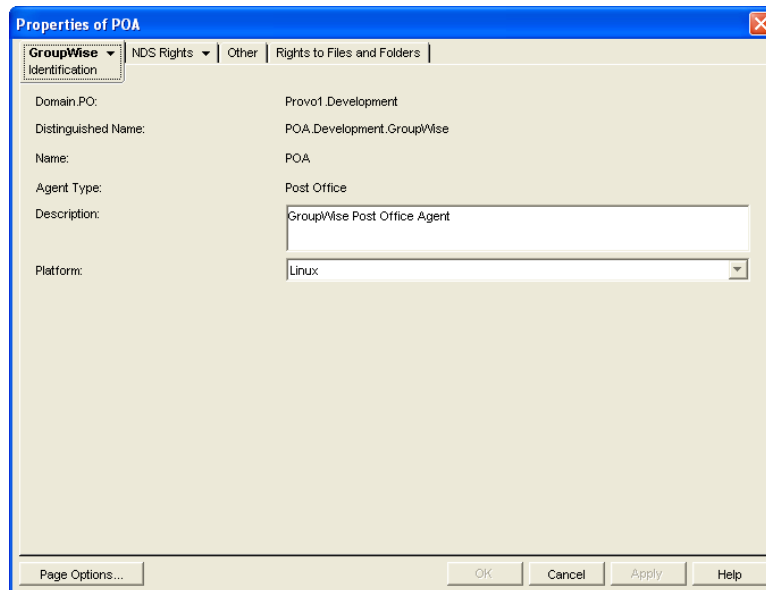
12 Click *OK* to save the post office information.

13 Continue with [Configuring the POA for the New Post Office](#).

11.3.2 Configuring the POA for the New Post Office

Although there are many POA settings, the default settings are sufficient to get your post office operational. However, there are a few important settings that you can conveniently modify before you install the agent software.

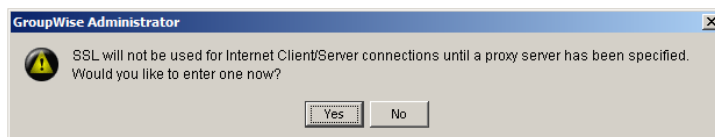
- 1 In ConsoleOne, double-click the new Post Office object.
- 2 Right-click the POA object, then click *Properties* to display the POA Identification page.



- 3 Provide a description for the POA.
The description displays on the POA agent console as the POA runs.
- 4 Select the platform where the POA will run ([Agent Platform](#) on the [New Post Office Summary Sheet](#)).
- 5 (Conditional) If you have created the post office in a clustered environment, follow the instructions in the appropriate section of the [GroupWise 2012 Interoperability Guide](#).
- 6 Click *OK* to save the POA configuration information.

For more POA configuration options, see [Section 12.12, "Changing POA Configuration to Meet Post Office Needs,"](#) on page 215.

Because the security of POA connections with the GroupWise Windows client is vital to the security of your GroupWise system, the following message appears:



- 7 (Optional) Click *Yes* to open the *Network Address* tab of the POA so that you can enable SSL for the POA, as described in [Section 36.3.3, "Securing the Post Office with SSL Connections to the POA,"](#) on page 508, and to set up an external IP address for it, as described in [Section 36.3.1, "Securing Client/Server Access through an External Proxy Server,"](#) on page 506.

or

Click *No* to configure SSL later.

You continue to receive this message each time you modify the properties of the POA object until you configure SSL and an external address for the POA. However, you can continue with installing and starting the new POA without immediately establishing the recommended security configuration.

- 8 Continue with [Installing and Starting the New POA](#).

11.3.3 Installing and Starting the New POA

- 1 Install and start the POA for the new post office on the server where you created the post office directory structure.

For instructions, see “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.

- 2 Continue with [Setting Up User Access to the New Post Office](#).

11.3.4 Setting Up User Access to the New Post Office

The post office Access Mode determines how GroupWise client users access their mailboxes. By default, the GroupWise Windows client use Client/Server Access Mode to the post office. Client/Server Access Mode provides the following benefits:

- ◆ Client/server access provides the greatest level of security. Users do not need rights to the post office directory because the GroupWise client does not write directly to databases in the post office. All database updates are performed by the POA.
- ◆ Client/server access eliminates the need for separate network logins and passwords. This avoids problems with login restrictions, changing passwords, and insufficient network rights.
- ◆ Client/server access allows the GroupWise client to maintain multiple simultaneous connections to the post office.
- ◆ With client/server access mode, proxy rights can be granted to any user visible in the Address Book.

Historical Note: In GroupWise 5.x, the GroupWise client allowed the user to enter a path to the post office directory during login to facilitate Direct Access mode. The GroupWise 6.x and later Windows client no longer offers that login option. However, you can force the GroupWise 6.x and later Windows client to use Direct Access mode by starting it with the `/ph` switch and providing the path to the post office directory. However, this access mode is not recommended.

If you have not already done so, establish the recommended security configuration for the POA by following the instructions in:

- ◆ [Section 36.3.1, “Securing Client/Server Access through an External Proxy Server,”](#) on page 506
- ◆ [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508

11.4 What’s Next

After you have created the new post office and started its POA, you are ready to expand the post office by:

- ◆ Adding users to the post office.
See “[Users](#)” on page 217.
- ◆ Defining groups of users (distribution lists) that GroupWise users can select when addressing messages.

- See [“Distribution Lists, Groups, and Organizational Roles”](#) on page 279.
- ♦ Defining resources (for example, conference rooms or company cars) that users can schedule.
See [“Resources”](#) on page 263.
 - ♦ Defining libraries and setting up Document Management Services.
See [“Libraries and Documents”](#) on page 313.
 - ♦ Setting up the GroupWise Windows client software so that GroupWise users can run the client from Windows workstations.
See [“Client”](#) on page 1013.
 - ♦ Configuring the POA for optimal performance and security.
See [“Post Office Agent”](#) on page 469.

11.5 New Post Office Summary Sheet

Item	Value for Your GroupWise System	Explanation
Tree Name:		Section 11.2.3, “Determining the Context for the Post Office Object,” on page 176
eDirectory Container:		Section 11.2.3, “Determining the Context for the Post Office Object,” on page 176
Post Office Name:		Section 11.2.4, “Choosing the Post Office Name,” on page 176
GroupWise Domain:		Section 11.2.2, “Selecting the Domain That the Post Office Belongs To,” on page 176
Post Office Database Location:		Section 11.2.5, “Deciding Where to Create the Post Office Directory,” on page 177
Post Office Language:		Section 11.2.8, “Selecting the Post Office Language,” on page 179
Post Office Time Zone:		Section 11.2.9, “Selecting the Post Office Time Zone,” on page 179
Software Distribution Directory:		Section 11.2.10, “Selecting a Software Distribution Directory,” on page 179
Create Library:		Section 11.2.12, “Deciding if You Want to Create a Library for the New Post Office,” on page 180
	<ul style="list-style-type: none"> ♦ No ♦ Yes 	
Post Office Description:		Section 11.2.4, “Choosing the Post Office Name,” on page 176

Item	Value for Your GroupWise System	Explanation
Post Office Security Level:	<ul style="list-style-type: none"> ◆ Low ◆ High <ul style="list-style-type: none"> ◆ eDirectory authentication ◆ LDAP authentication 	Section 11.2.11, "Selecting a Post Office Security Level," on page 180
Agent Platform:	<ul style="list-style-type: none"> ◆ Linux POA ◆ Windows POA 	Section 11.2.6, "Deciding Where to Install the Agent Software," on page 178
Link to Domain:	<ul style="list-style-type: none"> ◆ TCP/IP ◆ Mapped ◆ UNC 	Section 11.2.7, "Deciding How to Link the New Post Office," on page 178

12 Managing Post Offices

As your GroupWise system grows and evolves, you might need to perform the following maintenance activities on post offices:

- ♦ [Section 12.1, “Connecting to the Domain That Owns a Post Office,”](#) on page 189
- ♦ [Section 12.2, “Editing Post Office Properties,”](#) on page 190
- ♦ [Section 12.3, “Managing Disk Space Usage in the Post Office,”](#) on page 196
- ♦ [Section 12.4, “Auditing Mailbox License Usage in the Post Office,”](#) on page 207
- ♦ [Section 12.5, “Viewing Current Client Usage in the Post Office,”](#) on page 209
- ♦ [Section 12.6, “Tracking and Restricting Client Access to the Post Office,”](#) on page 209
- ♦ [Section 12.7, “Securing the Post Office with LDAP Authentication,”](#) on page 211
- ♦ [Section 12.8, “Refreshing the Client View Files in the Post Office,”](#) on page 211
- ♦ [Section 12.9, “Disabling a Post Office,”](#) on page 212
- ♦ [Section 12.10, “Moving a Post Office,”](#) on page 212
- ♦ [Section 12.11, “Deleting a Post Office,”](#) on page 214
- ♦ [Section 12.12, “Changing POA Configuration to Meet Post Office Needs,”](#) on page 215

See also [Section 26, “Maintaining Domain and Post Office Databases,”](#) on page 401 and [Section 31, “Backing Up GroupWise Databases,”](#) on page 431.

Proper database maintenance and backups allow recovery from accidental deletions, as described in [Section 32.5, “Restoring Deleted Mailbox Items,”](#) on page 435 and [Section 32.6, “Recovering Deleted GroupWise Accounts,”](#) on page 438.

12.1 Connecting to the Domain That Owns a Post Office

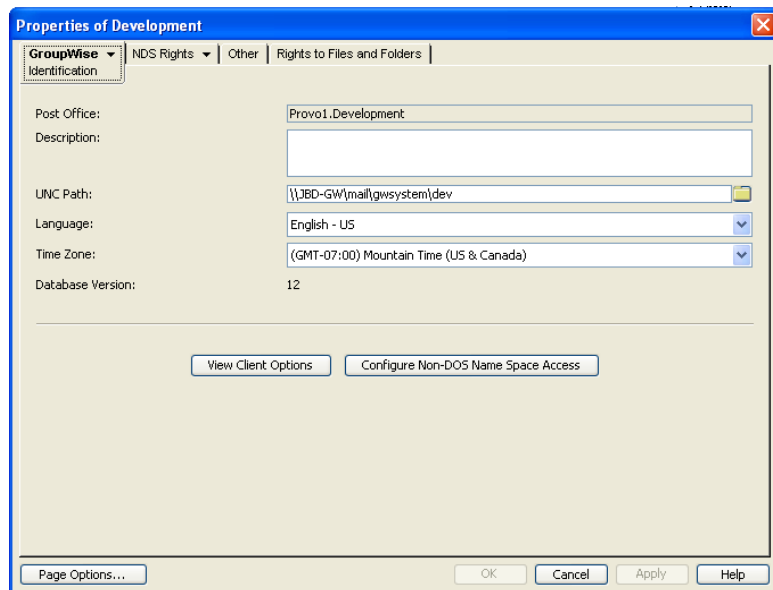
Whenever you change post office information, it is most efficient to connect directly to the domain that the post office belongs to before you begin making modifications. Performing administrative tasks in a post office while not connected to the post office’s domain increases the amount of administrative message traffic sent between domains.

For instructions, see [Section 9.1, “Connecting to a Domain,”](#) on page 145.

12.2 Editing Post Office Properties

After creating a post office, you can change some post office properties. Other post office properties cannot be changed.

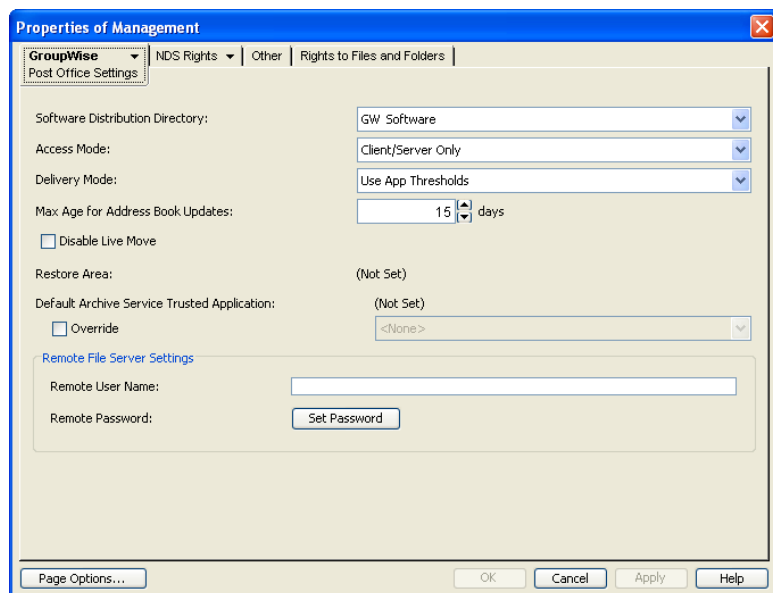
- 1 In ConsoleOne, browse to and right-click the Post Office object, then click *Properties* to display the post office Identification page.



- 2 Change editable fields as needed.

For information about individual fields, see [Section 11.3, "Setting Up the New Post Office,"](#) on [page 181](#) or use online help when editing the post office.

- 3 Click *GroupWise > Post Office Settings* to display the Post Office Settings page.



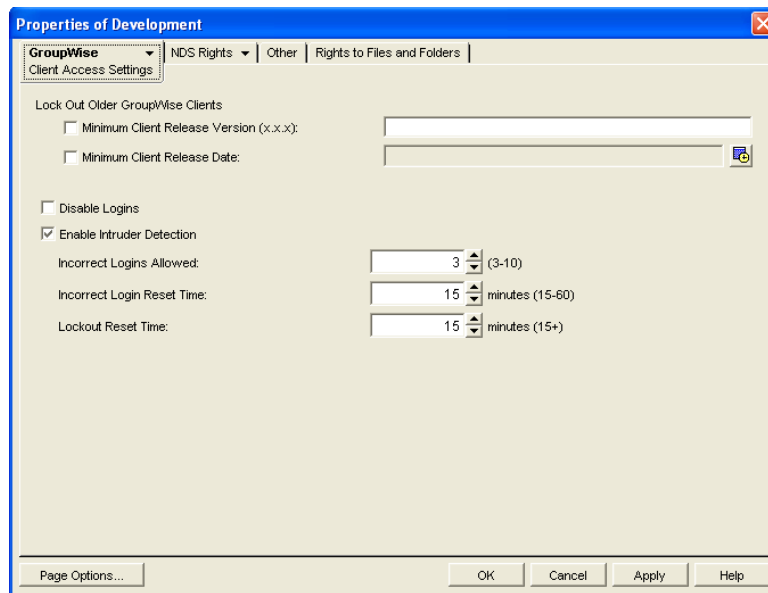
Basic post office settings are discussed in the following sections:

- ◆ [Section 11.2.10, “Selecting a Software Distribution Directory,”](#) on page 179
- ◆ [Section 11.3.4, “Setting Up User Access to the New Post Office,”](#) on page 186

More advanced post office settings are discussed in the following sections:

- ◆ [Section 6.5, “Controlling Address Book Synchronization for Caching and Remote Client Users,”](#) on page 112
- ◆ [Section 14.4, “Moving GroupWise Accounts,”](#) on page 234
- ◆ [Section 32.5, “Restoring Deleted Mailbox Items,”](#) on page 435
- ◆ [Section 4.2.7, “Archive Service Settings,”](#) on page 77
- ◆ [Section 36.1.7, “Configuring the POA for Remote Server Login \(Windows Only\),”](#) on page 492

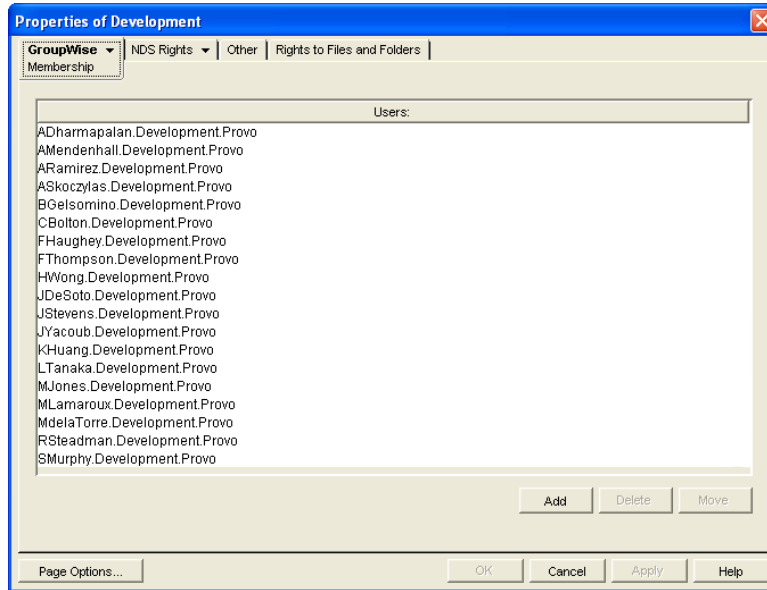
4 Click *GroupWise > Client Access Settings* to display the Client Access Settings page.



The client access settings are discussed in the following sections:

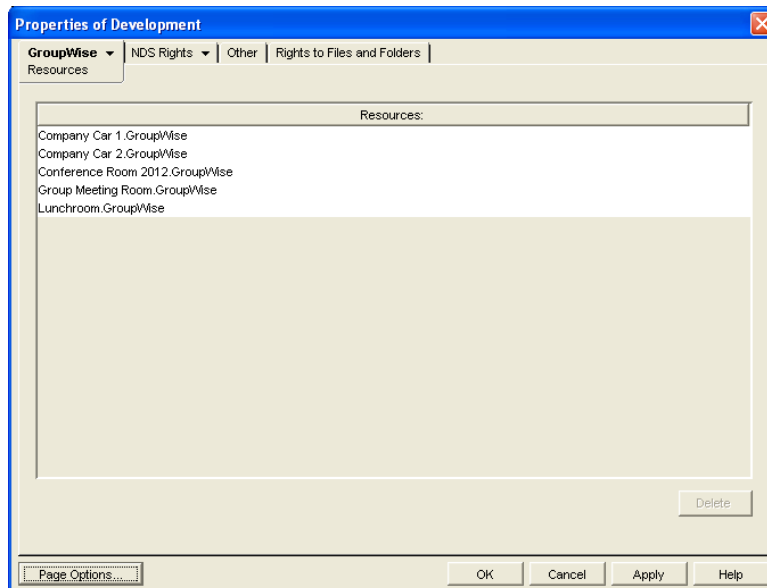
- ◆ [Section 12.6, “Tracking and Restricting Client Access to the Post Office,”](#) on page 209
- ◆ [Section 12.9, “Disabling a Post Office,”](#) on page 212
- ◆ [Section 36.3.5, “Enabling Intruder Detection,”](#) on page 516

5 Click *GroupWise > Membership* to display the Membership page.



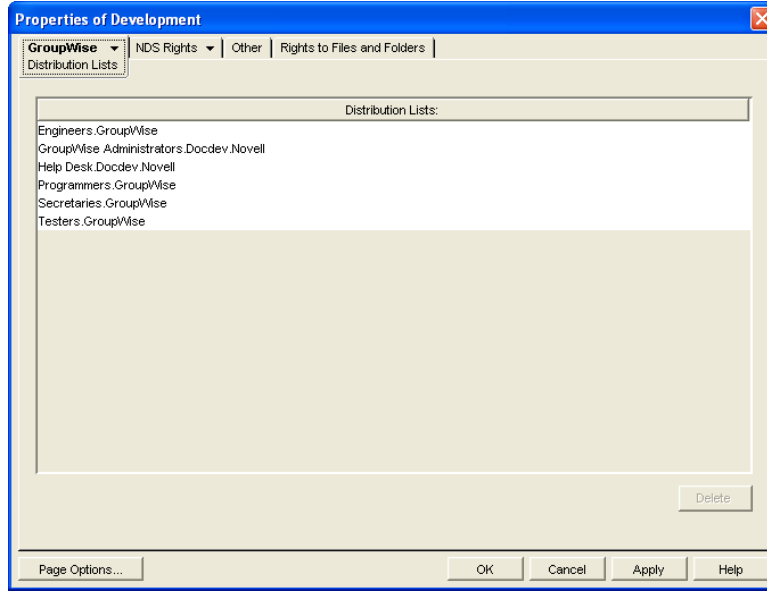
All users in the post office are listed, no matter where their Novell eDirectory objects are located in the tree. Here you can add, delete, and move users in the post office. See [“Users” on page 217](#).

6 Click *GroupWise > Resources* to display the Resources page.



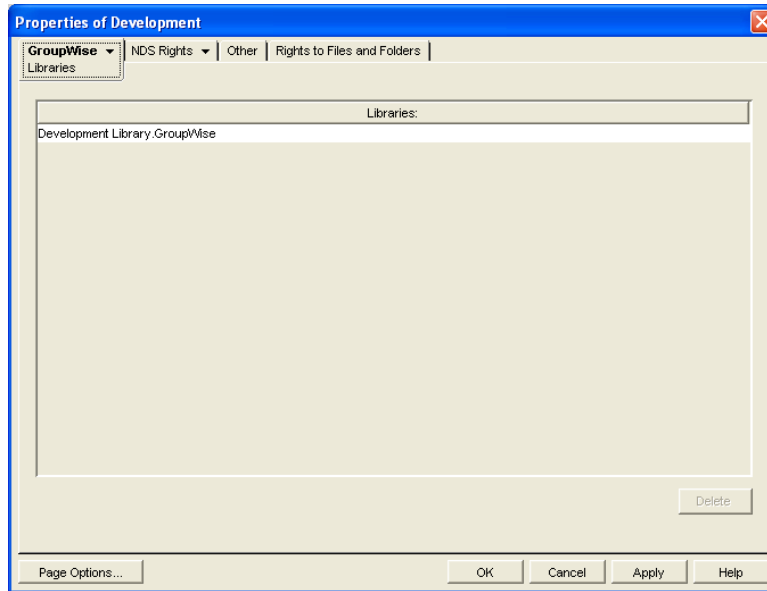
All resources in the post office are listed, no matter where their eDirectory objects are located in the tree. This is a convenient place to delete resources from the post office. See [“Resources” on page 263](#)

7 Click *GroupWise > Distribution Lists* to display the Distribution Lists page.



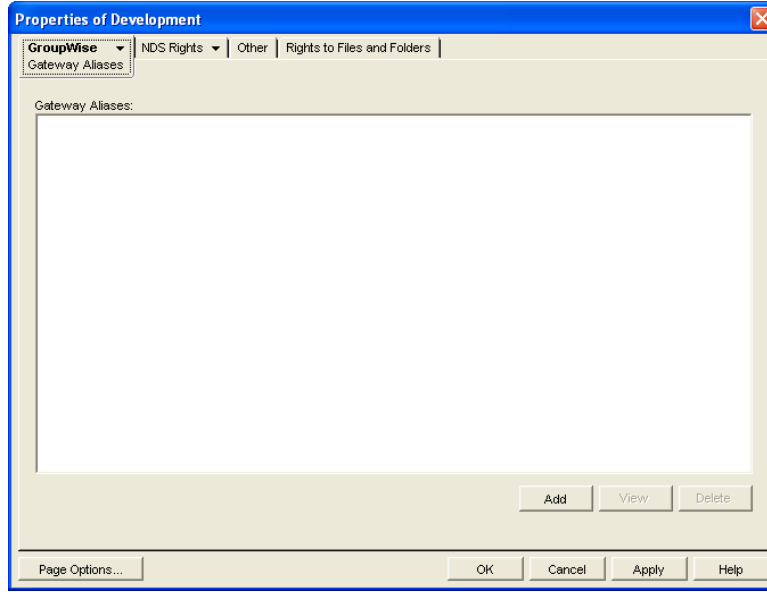
All distribution lists in the post office are listed, no matter where their eDirectory objects are located in the tree. This is a convenient place to delete distribution lists from the post office. See [“Distribution Lists, Groups, and Organizational Roles”](#) on page 279.

8 Click *GroupWise > Libraries* to display the Libraries page.



All libraries belonging to the post office are listed, no matter where their eDirectory objects are located in the tree. This is a convenient place to delete libraries. See [Part VII, “Libraries and Documents,”](#) on page 313.

- 9 Click *GroupWise > Gateway Aliases* to display the Aliases page.

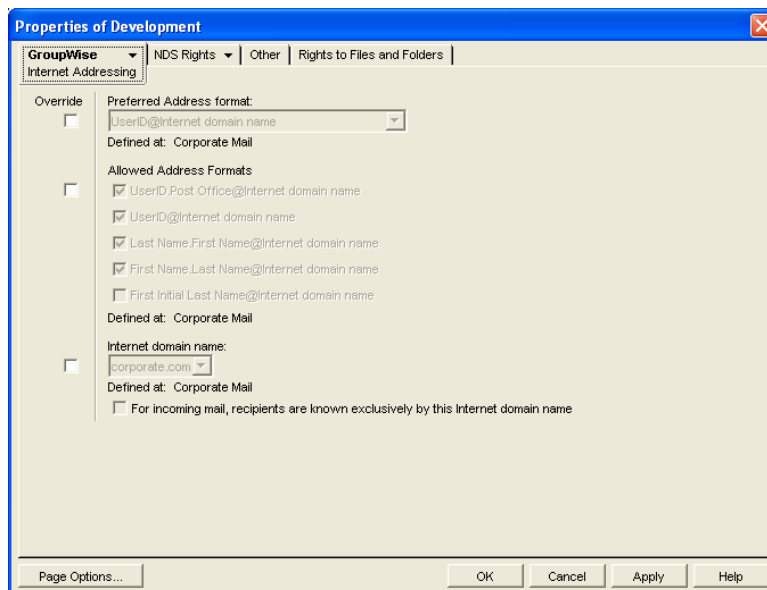


Many non-GroupWise systems do not use the same address syntax as GroupWise. Or, in some cases, they might not support the same address characters or address length. A gateway alias is simply an alternate address that conforms to the format requirements of the non-GroupWise system that the gateway connects to. An alias might be required in order to exchange messages with the non-GroupWise system, or it might be required when synchronizing directory (user) information between the two systems.

Alias requirements vary depending on the non-GroupWise system to which your gateway connects. For alias information specific to your gateway, see the GroupWise guide for that gateway on the [GroupWise Gateways Documentation Web site \(http://www.novell.com/documentation/gwgateways\)](http://www.novell.com/documentation/gwgateways).

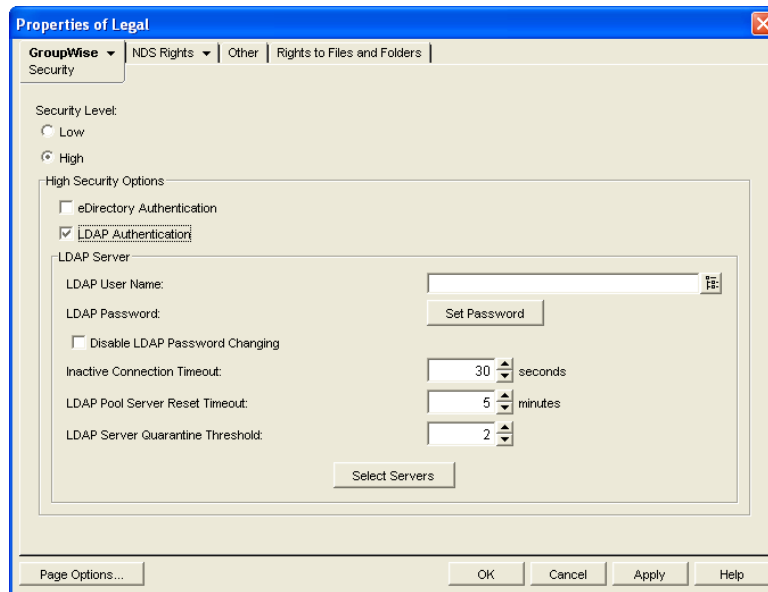
For more information about gateway aliases, see [Section 52.3, "Transitioning from SMTP Gateway Aliases to Internet Addressing,"](#) on page 754.

- 10 Click *GroupWise > Internet Addressing* to display the Internet Addressing page.



Here you provide information used to determine the Internet addressing settings for the post office. See [Section 52, “Configuring Internet Addressing,”](#) on page 743 for more information.

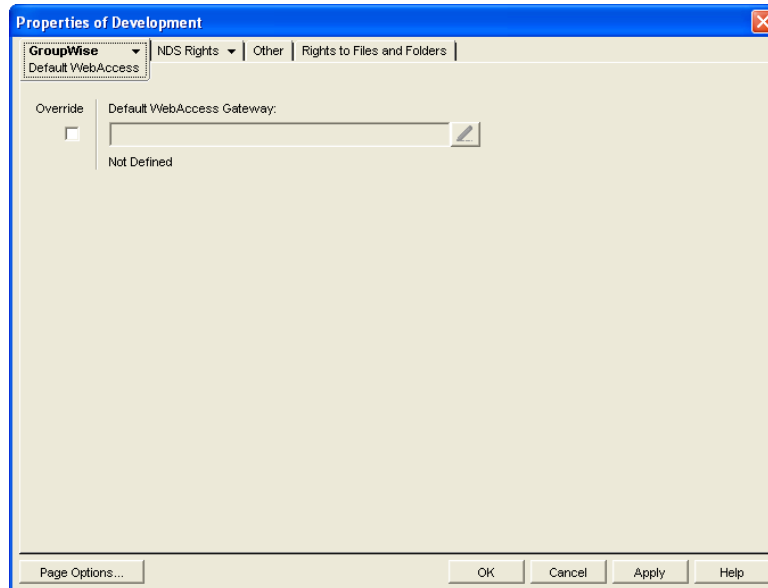
- 11 Click *GroupWise > Security* to display the Security page.



For instructions on setting the security level for the post office, see [Section 11.2.11, “Selecting a Post Office Security Level,”](#) on page 180.

- 12 Click *GroupWise > Default WebAccess* to display the Default WebAccess page.

NOTE: This page applies only to post offices that have not yet been updated to GroupWise 2012. GroupWise 2012 does not include the WebAccess Agent.



Use this page to designate the default WebAccess gateway for the legacy post office.

- 13 Click *OK* to save changes to the post office properties.

12.3 Managing Disk Space Usage in the Post Office

Many users are prone to save every message and attachment they ever receive. You can moderate this behavior by implementing disk space management:

- ♦ [Section 12.3.1, “Understanding Disk Space Usage and Mailbox Size Limits,” on page 196](#)
- ♦ [Section 12.3.2, “Preparing to Implement Disk Space Management,” on page 197](#)
- ♦ [Section 12.3.3, “Setting Mailbox Size Limits,” on page 198](#)
- ♦ [Section 12.3.4, “Enforcing Mailbox Size Limits,” on page 200](#)
- ♦ [Section 12.3.5, “Restricting the Size of Messages That Users Can Send,” on page 201](#)
- ♦ [Section 12.3.6, “Preventing the Post Office from Running Out of Disk Space,” on page 203](#)
- ♦ [Section 12.3.7, “An Alternative to Disk Space Management in the Post Office,” on page 206](#)
- ♦ [Section 12.3.8, “Forcing Caching Mode,” on page 206](#)

12.3.1 Understanding Disk Space Usage and Mailbox Size Limits

The concept of mailbox size is different for Windows client users than it is for you as an administrator. Users are most interested in the functional size of their mailboxes; that is, the number of items that they can store in their mailboxes. Administrators are usually more concerned about the physical disk space that mailboxes occupy.

Functional mailbox size is computed by adding the bytes occupied by individual messages. Users are notified when they exceed the functional mailbox size limit that you have set for them. Users can then identify items to delete or archive.

- ♦ Windows client users can use *Tools > Check Mailbox Size* to list items in the Trash folder, the Sent Items folder, the Mailbox folder, the Work in Progress folder, and any posted items. Item size is displayed in bytes and the list is sorted from largest to smallest, to easily identify candidates for deletion or archiving.
- ♦ WebAccess users always have the *Size* column visible.

When users have deleted or archived sufficient items, their functional mailbox size limit problem is resolved.

As an administrator, you want to set functional mailbox size limits that are reasonable for users and that make efficient use of the physical disk space that you have available. You are more concerned about physical disk space usage in the post office. Physical disk space usage is much more complex than counting the bytes occupied by individual messages.

The following factors influence physical disk space usage:

- ♦ In a typical post office, 85% of disk space is occupied by attachments in the [offiles](#) directory structure. Attachments are compressed by 40% to allow more data to be stored in less space.
- ♦ A large message sent to multiple users in the same post office is only stored on disk once, but counts against mailbox size for all recipients. If it is sent to multiple post offices, a copy is stored in each post office
- ♦ A large distribution list can cause even a small message to take up substantial disk space. If all recipients are in the same post office, only one copy is stored, but if there are recipients in multiple post offices, a copy is stored in each post office
- ♦ User databases ([userxxx.db](#) files) might contain large numbers of contacts and folders. Contacts and folders affect the size of the user databases, which have a maximum size of 4 GB, but do not count against the mailbox size for users.

- ♦ Shared folders count only against the owner’s mailbox size, even though sharing with users in other post offices uses disk space in those post offices as well.
- ♦ A message is stored until the last recipient deletes and empties it. As a result, you might attempt to reduce post office disk space usage by reducing certain users’ mailboxes, but disk space usage does not change. This can occur because large messages eliminated from the reduced mailboxes still exist in other mailboxes.

Because of the complexity of these factors, you might consider a progressive strategy to determine the appropriate functional mailbox limits for your users.

For a new post office, you could check the physical disk space occupied by the post office before users start accumulating email and initially set no functional mailbox limits. After a period of time (for example, a month), see how much the post office has grown. Run a report, as described in [Section 30.1, “Gathering Mailbox Statistics,” on page 423](#), to assess the rate of mailbox growth, then start setting functional mailbox limits based on user needs and available physical disk space. To set mailbox limits, skip to [Section 12.3.3, “Setting Mailbox Size Limits,” on page 198](#).

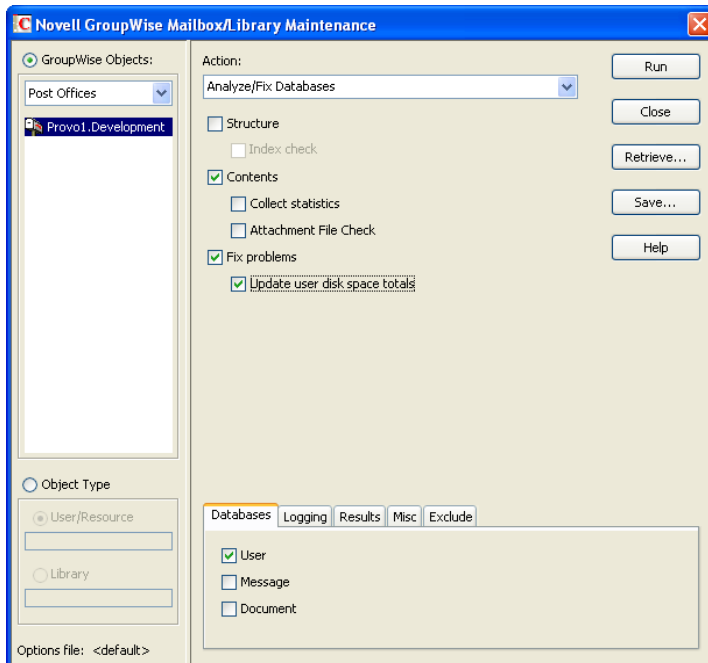
For an existing post office, where users have never had functional mailbox limits set in the past, continue with [Preparing to Implement Disk Space Management](#).

12.3.2 Preparing to Implement Disk Space Management

If you are implementing disk space management in an existing GroupWise system, you must begin by setting the initial size information on all users’ mailboxes.

To establish current mailbox size:

- 1 In ConsoleOne, browse to and select a Post Office object.
- 2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



- 3 In the *GroupWise Objects* field, select *Post Offices*.
- 4 In the *Action* field, select *Analyze/Fix Databases*.
- 5 As options to the action, select *Contents*, *Fix Problems*, and *Update User Disk Space Totals*.

Make sure all other options are deselected.

- 6 On the *Databases* tab, select *User*.

Make sure all other types of databases are deselected.

- 7 Click *Run*, then click *OK* to acknowledge that the Mailbox/Library Maintenance task has been sent to the POA.

After the POA has performed the task, current mailbox size information becomes available on each user's mailbox. The information is updated regularly as the user receives and deletes messages.

- 8 To generate a report of current mailbox information, follow the instructions in [Section 30.1, "Gathering Mailbox Statistics,"](#) on page 423.
- 9 Repeat [Step 1](#) through [Step 8](#) for each post office where you want to implement disk space management.
- 10 Continue with [Setting Mailbox Size Limits](#).

12.3.3 Setting Mailbox Size Limits

After initial size information is recorded on each user's mailbox, you can establish a limit on the amount of disk space each user's mailbox is allowed to occupy. You can set a single limit for an entire domain. You can set different limits for each post office. You can even set individual user limits if necessary.

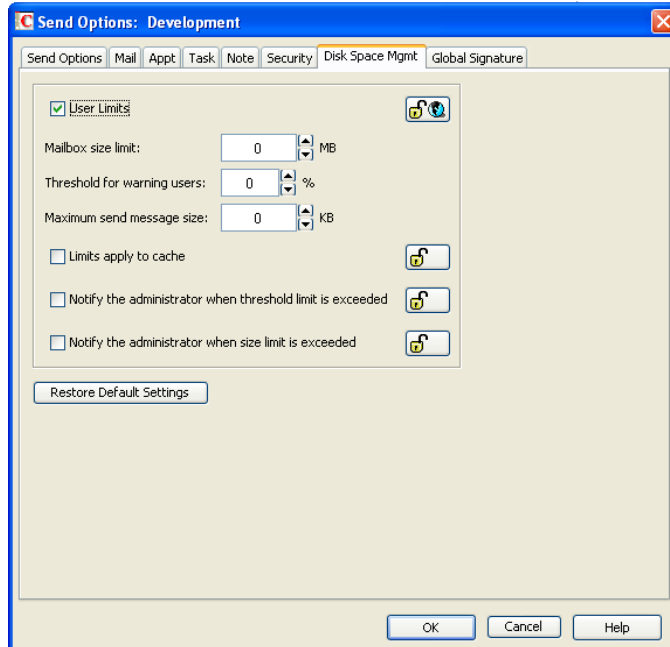
If you are implementing disk space management in an existing GroupWise system where users are accustomed to unlimited disk space, you should warn them about the coming change. After you establish the mailbox size limits as described in this section, users whose mailboxes exceed the established limit cannot send messages until the size of their mailboxes is reduced. Users might want to manually delete and archive items in advance in order to avoid this interruption in their use of GroupWise.

To establish mailbox size limits:

- 1 In ConsoleOne, browse to and select a Domain, Post Office, or User object.
- 2 Click *Tools > GroupWise Utilities > Client Options*.



3 Click *Send > Disk Space Management*.



4 Select *User Limits*.

5 Specify the maximum number of megabytes allowed for each user's mailbox.

For guidance in setting mailbox size limits, visit the [GroupWise Best Practices Wiki \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

The maximum size limit that you can set for mailboxes is 4 TB.

6 Specify as a percentage the point where you want to warn users that their mailboxes are getting full.

After users receive a warning message, they can continue to send messages until the size limit is reached. After the size limit is reached, users must reduce the size of their mailboxes in order to send additional messages.

7 (Optional) Specify in kilobytes the largest message that users can send.

IMPORTANT: By restricting message size, you can influence how fast users' mailboxes fill up. However, if users have valid reasons for sending messages that exceed this limit, the limit can become a hindrance to users getting their work done.

8 Click *OK > Close* to save the disk space management settings.

9 (Conditional) If you are adding disk space management to an existing GroupWise system where users' mailboxes are already over the desired size limit, continue with [Enforcing Mailbox Size Limits](#).

or

(Conditional) If you are implementing disk space management in a new system where users have not yet begun to use their mailboxes, see "Using Mailbox Storage Size Information" in "Maintaining GroupWise" in the *GroupWise 2012 Windows Client User Guide* to see how setting a mailbox size limit affects users' activities in the GroupWise client.

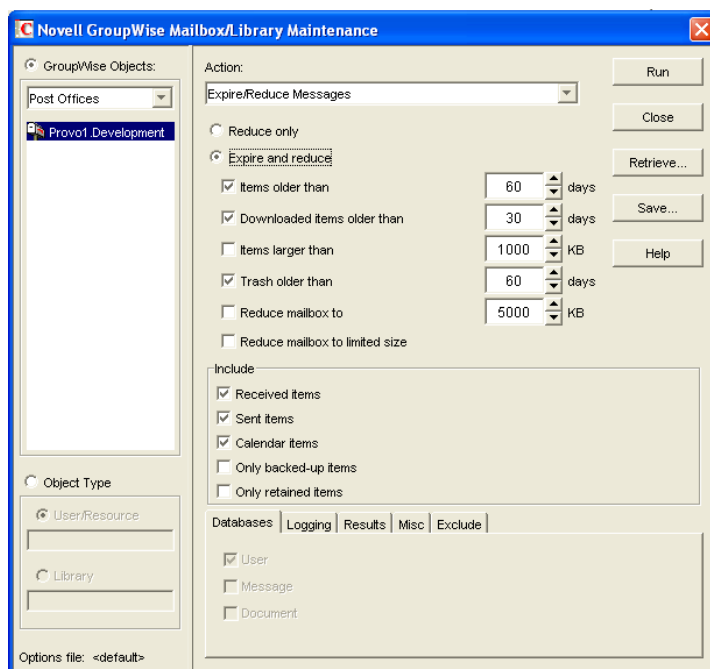
12.3.4 Enforcing Mailbox Size Limits

If existing GroupWise users are having difficulty fitting their mailboxes into the established mailbox size limits, you can assist them by reducing the size of their mailboxes for them.

When users archive and empty messages in their mailboxes, the messages are marked for removal from the database (“expired”), but the disk space that the expired messages occupied in the databases is retained and used again for new messages. As a result, archiving and deleting messages does not affect the overall size of the databases.

The Expire/Reduce Messages option of Mailbox/Library Maintenance enables you to expire additional messages and reduce the size of the databases by reclaiming the free space in the databases that is created when messages are expired. You should inform users before you run this process so they have a chance to archive or delete messages. Unread messages are not expired.

- 1 In ConsoleOne, browse to and select a Post Office object.
- 2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



- 3 In the *Action* field, select *Expire/Reduce*.
- 4 Set the *Expire* and *Reduce* options as desired, making sure that *Reduce Mailbox to Limited Size* is selected.
- 5 Click *Run*, then click *OK* to acknowledge that the Mailbox/Library Maintenance task has been sent to the POA.

After the POA has performed the task, users mailboxes fit within the mailbox size limit you have established.

- 6 Repeat [Step 1](#) through [Step 5](#) for each post office where you want to reduce user mailboxes to the established mailbox size limit.

To see how setting a mailbox size limit affects user activities in the GroupWise client, see “[Using Mailbox Storage Size Information](#)” in “[Maintaining GroupWise](#)” in the *GroupWise 2012 Windows Client User Guide*.

12.3.5 Restricting the Size of Messages That Users Can Send

By restricting message size, you can influence how fast user mailboxes fill up. However, if users have valid reasons for sending messages that exceed this limit, the limit can become a hindrance to users getting their work done.

For HTML-formatted messages, the MIME portion of the message counts in the message size. MIME files can be large. If a user cannot send an HTML-formatted message, he or she could use plain text instead, in order to decrease the size of the message so that it falls within the message size restriction.

There are four levels at which you can restrict message size:

- ♦ [“Within the Post Office” on page 201](#)
- ♦ [“Between Post Offices” on page 202](#)
- ♦ [“Between Domains” on page 202](#)
- ♦ [“Between Your GroupWise System and the Internet” on page 202](#)

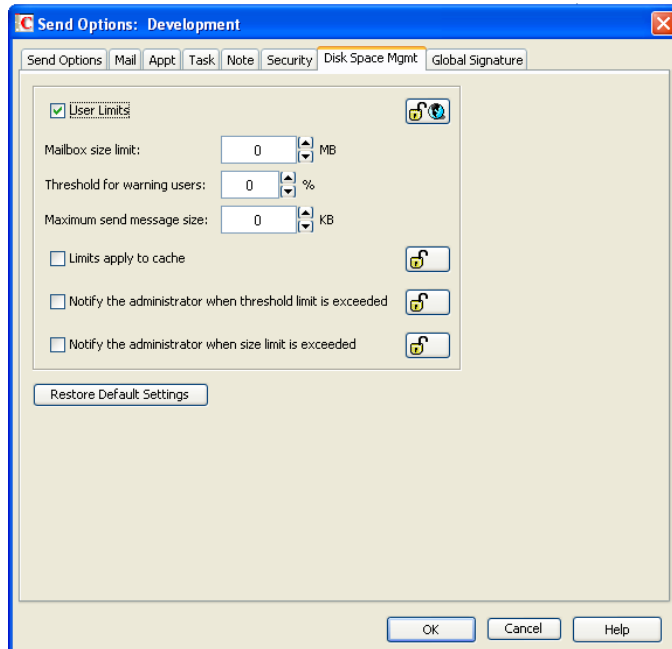
Within the Post Office

You can use Client Options to restrict the size of messages that users can send within their local post office.

- 1 In ConsoleOne, browse to and select a Domain, Post Office, or User object.
- 2 Click *Tools > GroupWise Utilities > Client Options*.



3 Click *Send > Disk Space Management*.



4 Select *User Limits*.

5 Specify in kilobytes the largest message that users can send.

6 Click *OK*, then click *Close* to save the maximum message size setting.

Between Post Offices

You can configure the POA to restrict the size of messages that it allows to pass outside the local post office. See [Section 36.2.7, “Restricting Message Size between Post Offices,”](#) on page 504 for setup instructions.

Between Domains

You can configure the MTA to restrict the size of messages that it allows to pass outside the local domain. See [Section 42.2.1, “Restricting Message Size between Domains,”](#) on page 642 for setup instructions.

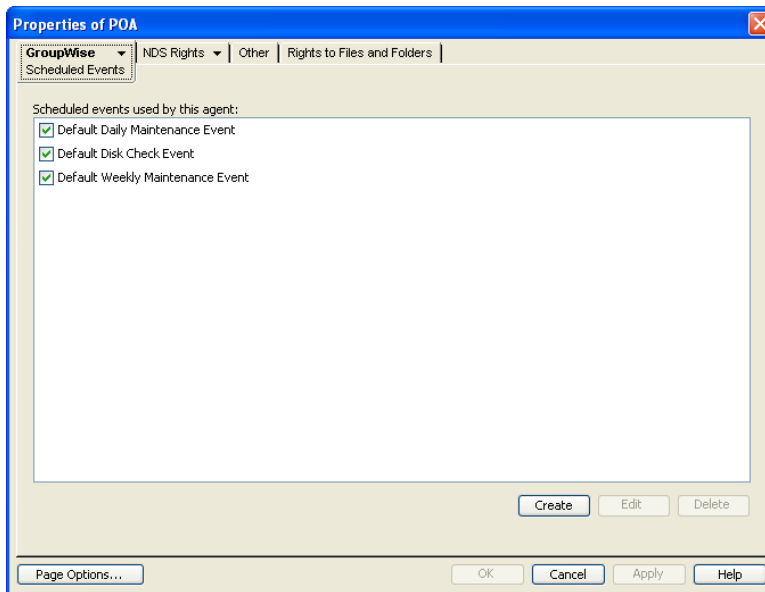
Between Your GroupWise System and the Internet

You can configure the Internet Agent (GWIA) to restrict the size of messages that it allows to pass to and from your GroupWise system by setting the size limits in a customized class of service. See [Section 54.1, “Controlling User Access to the Internet,”](#) on page 787 for setup instructions.

12.3.6 Preventing the Post Office from Running Out of Disk Space

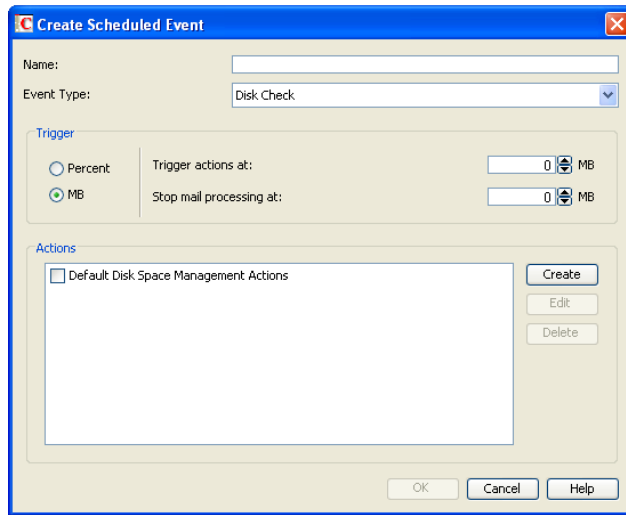
In spite of the best disk space management plans, it is still possible that some unforeseen situation could result in a post office running out of disk space. To prevent this occurrence, you can configure the POA to stop processing messages, so that disk space usage in the post office cannot increase until the disk space problem is resolved.

- 1 In ConsoleOne, browse to and select a Post Office object, right-click its POA object, then click *Properties*.
- 2 Click *GroupWise > Maintenance*, then adjust the settings in the *Disk Check Interval* and *Disk Check Delay* fields as described in [Section 36.4.2, “Scheduling Disk Space Management,”](#) on page 520.
- 3 Click *GroupWise > Scheduled Events*.

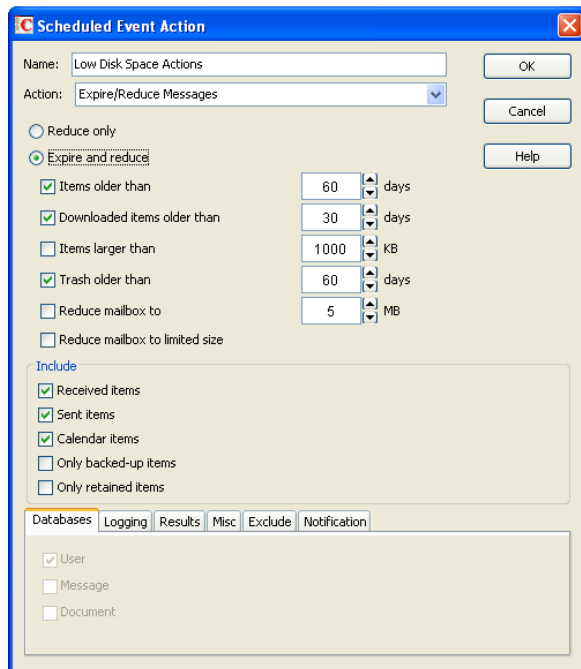


The Default Disk Space Management Actions trigger a Reduce on user and message databases at 4 GB and stop mail processing at 200 MB. You can edit the Default Disk Space Management Actions so that all post offices are affected, or you can create a new set of Disk Space Management actions to assign to specific post offices.

- 4 Click *Create* to create a new scheduled event to handle an unacceptably low disk space condition.

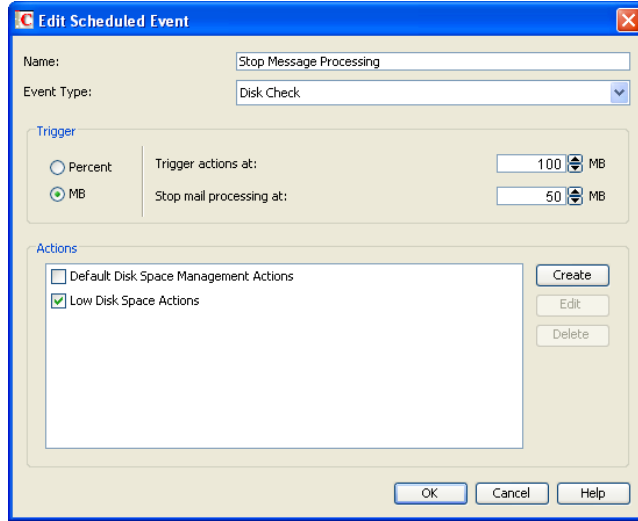


- 5 Type a unique name for the new scheduled event, then select *Disk Check* as the event type.
- 6 In the *Trigger Actions At* field, specify the amount of free post office disk space at which to take preventive measures.
- 7 Click *Create* to define your own disk check actions, then give the new action a unique name.

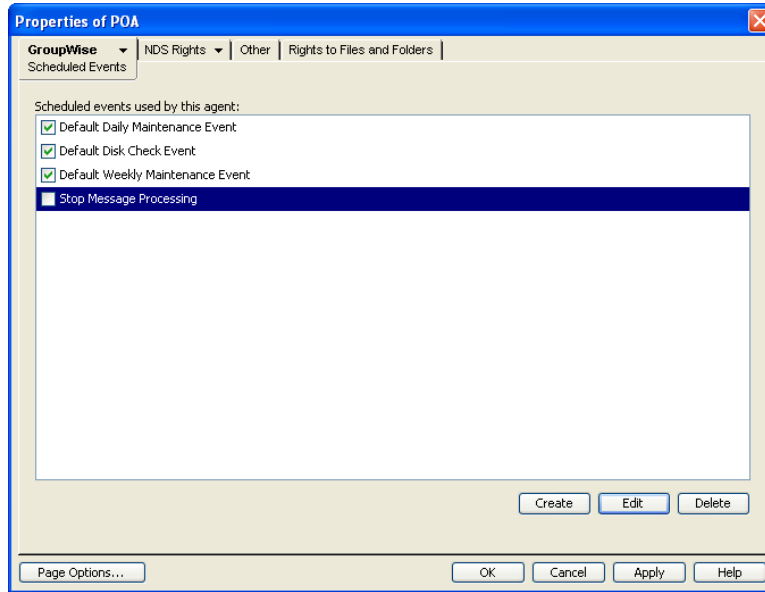


- 8 Configure the actions for the POA to take in order to relieve the low disk space condition. Use the *Results* or *Notification* tab if you want to receive notification about the POA's response to the low disk space condition.

- 9 Click *OK* to return to the *Create Scheduled Event* dialog box.



- 10 In the *Stop Mail Processing At* field, specify the amount of free post office disk space at which you want the POA to stop processing messages.
- 11 Click *OK* to create the new disk space management event and return to the *Scheduled Events* page.



- 12 Select the new disk space management event.
- 13 Click *OK* to close the Scheduled Events page.

ConsoleOne then notifies the POA to restart so the new disk space management event can be put into effect.

For additional instructions, see [Section 36.4.2, “Scheduling Disk Space Management,”](#) on page 520.

12.3.7 An Alternative to Disk Space Management in the Post Office

If you want to place more responsibility for disk space management onto GroupWise client users, you can require that they run the client in Caching mode, where all messages can be stored on user workstations, or other personal locations, rather than in the post office. For an overview of Caching mode, see “Using Caching Mode” in the *GroupWise 2012 Windows Client User Guide*.

IMPORTANT: Do not force Caching mode for a post office that supports Outlook clients along with GroupWise clients.

12.3.8 Forcing Caching Mode

You can force Caching mode for an entire domain, for specific post offices, or for individual users as necessary.

When you initially force caching mode, users’ Caching mailboxes are identical with their Online mailboxes. However, as you employ disk space management processes in the post office and reduce the size of users’ Online mailboxes, more and more of the users’ mailbox items exist only in their Caching mailboxes.

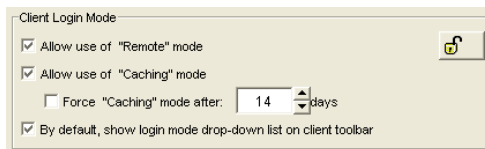
IMPORTANT: Make sure that users understand their responsibilities to back up their Caching mailboxes, as described in “Backing Up Email” in “Maintaining GroupWise” in the *GroupWise 2012 Windows Client User Guide*.

To force Caching mode:

- 1 In ConsoleOne, browse to and select a Domain, Post Office, or User object.
- 2 Click *Tools > GroupWise Utilities > Client Options*.



- 3 Click *Environment > Client Access*.



- 4 In the *Client Login Mode* box, select *Force Use of Caching Mode*.
- 5 Click *OK*, then click *Close* to save the Caching mode setting.

If you are helping existing users, who might have sizeable mailboxes, to start using Caching mode exclusively, you can configure the POA to respond efficiently when multiple users need to download their entire mailboxes for the first time. See [Section 36.2.6, “Supporting Forced Mailbox Caching,”](#) on [page 503](#) for setup instructions.

12.4 Auditing Mailbox License Usage in the Post Office

You can run an audit report in a post office to see:

- ♦ Which mailboxes have been accessed using full client licenses
- ♦ Which mailboxes have been accessed using limited client licenses
- ♦ Which mailboxes are active (have been accessed at least one time)
- ♦ Which mailboxes have never been active
- ♦ Which mailboxes have been inactive for a specified period of time

A mailbox requires a full client license (and is marked as a full client license mailbox) if it has been accessed by any of the following:

- ♦ The GroupWise Windows client (`grpwise.exe`)
- ♦ GroupWise Notify (`notify.exe`) or GroupWise Address Book (`addrbook.exe`)
- ♦ A third-party plug-in to the GroupWise client API

A mailbox requires a limited client license only (and is marked as a limited client license mailbox) if access to it has been limited to the following:

- ♦ GroupWise WebAccess (including mobile devices)
- ♦ GroupWise Windows client or WebAccess via the Proxy feature
- ♦ GroupWise Windows client or WebAccess via the Busy Search feature
- ♦ A mobile device that is synchronizing GroupWise data by using Novell Data Synchronizer
- ♦ A POP client
- ♦ An IMAP client
- ♦ A SOAP client or a third-party plug-in to the GroupWise SOAP protocol

A mailbox is considered active for licensing purposes if its owner has performed at least one of the following actions in the mailbox:

- ♦ Sending a message
- ♦ Opening a message
- ♦ Deleting a message
- ♦ Accessing the mailbox from a non-GroupWise client (for example, a POP3 email client) through the Internet Agent (GWIA)

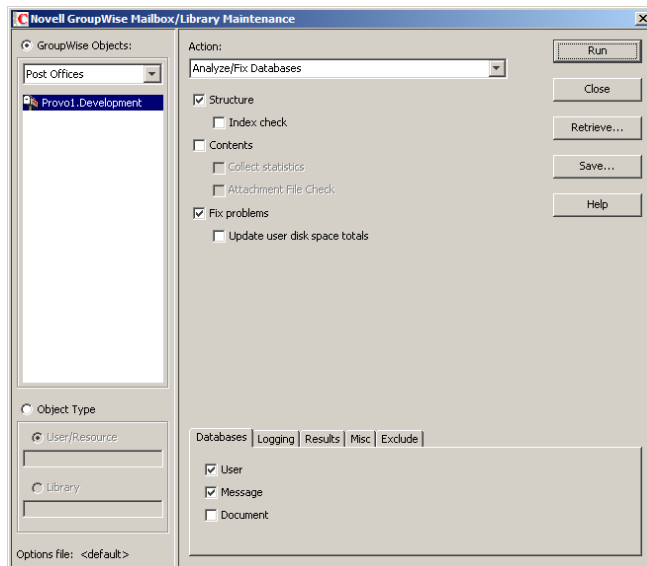
A mailbox is considered inactive for licensing purposes even if its owner has performed one or more of the following actions (or similar actions):

- ♦ Starting and stopping the GroupWise client without doing anything in the mailbox
- ♦ Making changes under *Tools > Options*
- ♦ Creating, modifying, or deleting rules
- ♦ Granting proxy access so that a user other than the mailbox owner is performing tasks that would otherwise indicate an active mailbox

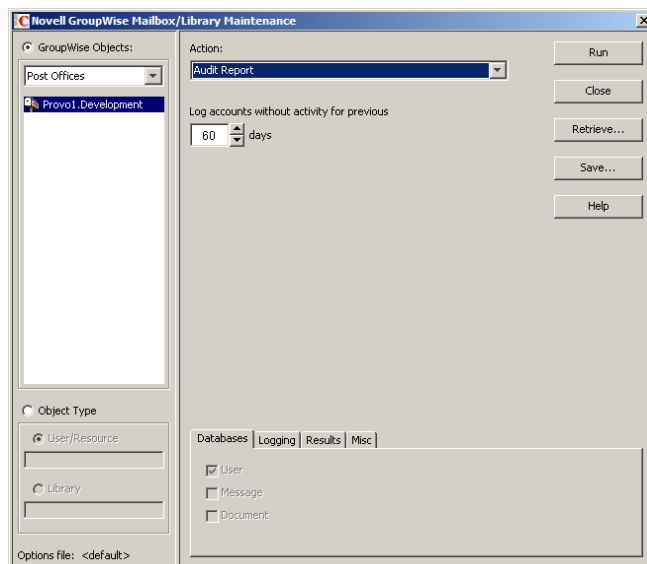
The mailboxes of GroupWise users and external entities require full client licenses.

To generate an audit report for the post office:

- 1 In ConsoleOne, browse to and select the Post Office object.
- 2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



- 3 In the *Action* field, select *Audit Report*.



- 4 In the *Log Accounts without Activity for nn Days* field, select the number of days you want to use for the inactivity report.

The Mailbox/Library Maintenance feature uses the default setting (60 days) to flag all mailboxes that have not had any activity within the last 60 days. Select a different number to change the time period of the log you generate for the audit report. For example, you could generate a log report for the last 30 days. However, if you view the audit information by using *Tools > GroupWise Diagnostics > Information* on a System, Domain, or Post Office object, the information is always listed for the 60-day default time period.

- 5 (Conditional) If you want write the report to a log file, click the *Logging* tab, then specify a name for the log file.
By default, the results are sent as an email message to the domain's GroupWise administrator.
- 6 (Conditional) If you want to send the results to additional users:
 - 6a Click the *Results* tab.
 - 6b Specify the users' email addresses as a comma-delimited list in the *CC* field.
 - 6c Click *Message* to add personalized text to the message, then click *OK*.
- 7 Click *Run*, then click *OK* to acknowledge that the Mailbox/Library Maintenance task has been sent to the POA.

After the POA has performed the task, the audit report is generated in the format (log file or email message) you specified. The audit report lists all users who are currently considered inactive and flags those that have been inactive for longer than the number of days specified in the *Log Accounts without Activity for nn Days* field.

Audit reports are stored as part of the information available on Post Office and Domain objects in ConsoleOne. Right-click a Domain or Post Office object, then click *Tools > GroupWise Diagnostics > Information*. The information stored on the Domain object is cumulative for all post office in the domain for which audit reports have been run.

Audit reports can also be scheduled to run on a regular basis by properly configuring the POA to perform a Mailbox/Library Maintenance event. See [Section 36.4.1, "Scheduling Database Maintenance," on page 517](#).

12.5 Viewing Current Client Usage in the Post Office

ConsoleOne can display the number of users who are using the Windows client. The client version is also displayed.

- 1 In ConsoleOne, select a Post Office object, a Domain object, or the GroupWise System object.
- 2 Click *Tools > Diagnostics > Information* to display the client statistics for the selected object.
- 3 Click *Close* when you are finished.

12.6 Tracking and Restricting Client Access to the Post Office

By default, the post office allows multiple versions of the GroupWise Windows client to access it. Using the Web console available for the post office's POA, you can see the version number of each GroupWise client that logs in to the post office in client/server access mode (TCP/IP to the POA). This information is displayed on the POA Web console's *C/S Users* page. For more information, see [Section 37.2, "Using the POA Web Console," on page 539](#).

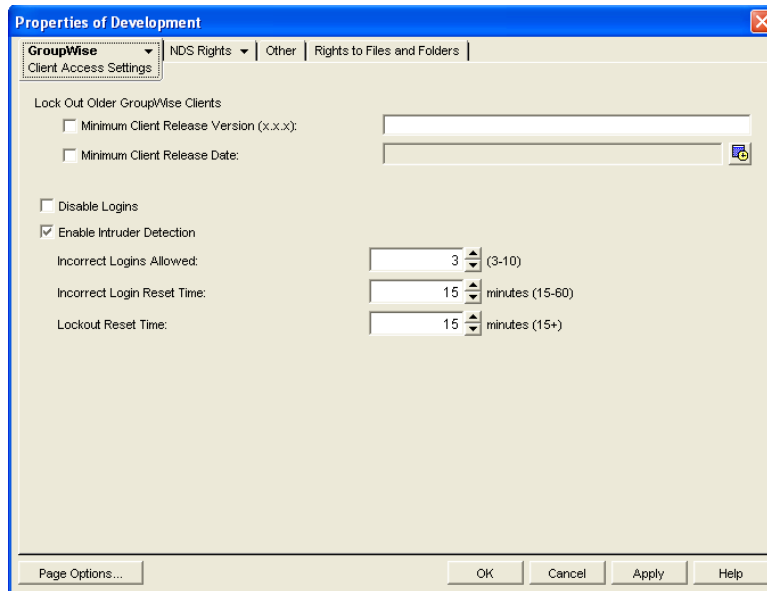
IMPORTANT: Because the POA provides the version tracking and enforces the client lockout, this functionality applies only to GroupWise clients that are accessing the post office in Client/Server Access Mode (not Direct Access Mode).

To help you better monitor and track which versions of the GroupWise client are being used to access the post office, you can specify a preferred GroupWise client version for the post office. Any version that does not match the preferred version is highlighted on the POA Web console's *C/S Users* page. Older versions are shown in red, and newer versions are shown in blue.

In addition, to restrict which versions of the GroupWise client can access the post office, you can choose to lock out any GroupWise clients that are older than the preferred version. If you want to lock out all GroupWise clients (for example, to rebuild the post office database), see [Section 12.9, “Disabling a Post Office,”](#) on page 212.

To specify a preferred GroupWise client version for the post office and to enable the POA to lock out specific GroupWise client versions:

- 1 In ConsoleOne, browse to and right-click the Post Office object, then click *Properties*.
- 2 Click *GroupWise > Client Access Settings* to display the Client Access Settings page.



- 3 Fill in the following fields:

Minimum Client Release Version: Specify the version to use as the post office’s preferred GroupWise client version. Any version that does not match the preferred version is highlighted on the POA Web console’s C/S Users page. Older versions are shown in red, and newer versions are shown in blue. The version number syntax should match what is displayed in the GroupWise client’s About GroupWise dialog box.

For GroupWise 2012, specify 12.

Minimum Client Release Date: This field is available only if you specify a release version. You can use this field to associate an expected release date with the release version. The C/S Users page highlights any dates that do not match the one entered here.

Lock Out Older GroupWise Clients: Select this option for either or both of the above options to lock out any GroupWise clients (Client/Server Access Mode only) that are older than the version and/or date specified in the *Release Version* and *Release Date* fields. For example, if you entered 8.0.0 in the *Release Version* field and October 24, 2008 12:00 AM in the *Release Date* field and selected this option for both, any GroupWise client that is older than version 8.0 or is dated before October 24, 2008 12:00 AM is not allowed access to the post office.

The date for GroupWise 2012 is January 17, 2012.

- 4 Click OK to save the changes.

12.7 Securing the Post Office with LDAP Authentication

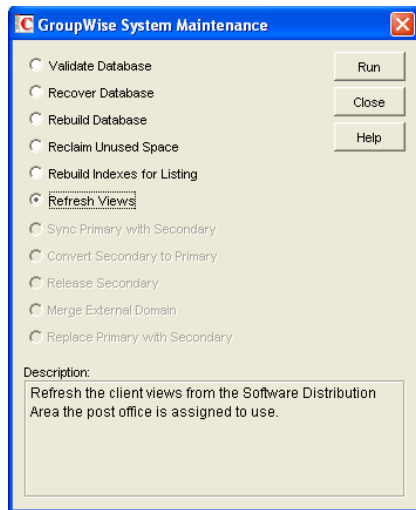
For user convenience, you can configure the post office for LDAP authentication, which enables users to use their LDAP (network) passwords to access their GroupWise mailboxes, rather than having separate GroupWise passwords. The POA performs the LDAP authentication for users in the post office. For setup instructions, see [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,”](#) on page 510.

12.8 Refreshing the Client View Files in the Post Office

The GroupWise Windows client software includes view files that control the appearance of the client interface. When you copy the client software to a software distribution directory, the view files are included. A copy of the view files is also stored in each post office.

When you use AutoUpdate to force Windows client software updates, as described in [Section 77.1, “Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client,”](#) on page 1069, the AutoUpdate process makes one attempt to update the view files in the post office based on the latest client software in the software distribution directory. If that attempt fails, the problem is recorded in the POA log file and you can then manually update the view files in the post office.

- 1 In ConsoleOne, browse to and select the Post Office object whose view files you want to update, then click *Tools > GroupWise Utilities > System Maintenance*.



- 2 Select *Refresh Views*, click *Run*, click *Yes*, then click *OK*.

The POA then retrieves the latest view files from the software distribution directory associated with the selected post office.

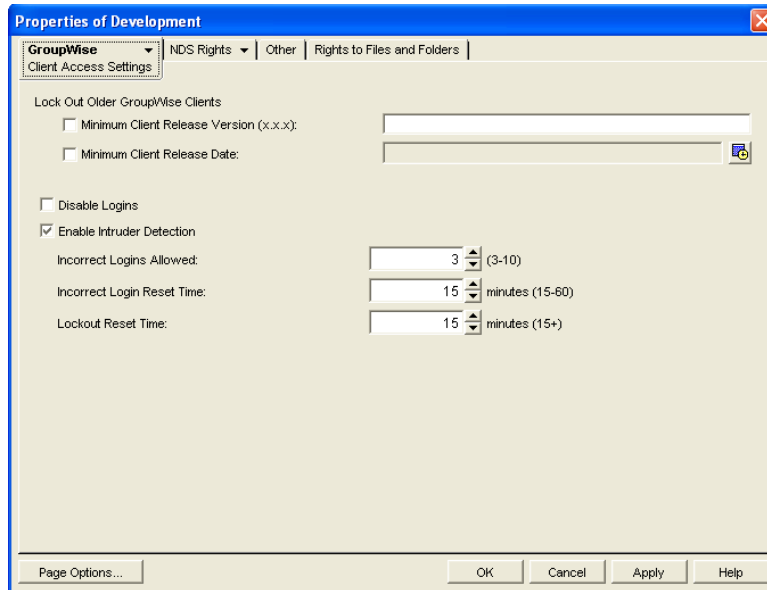
IMPORTANT: If you have created custom view files with the same names as standard view files, they will be overwritten when the post office view files are refreshed from the software distribution directory. If you have such customized view files, you must back them up and then restore them so that your customizations are not lost because of the refresh.

12.9 Disabling a Post Office

Disabling a post office restricts users from starting the GroupWise Windows client and accessing the post office. However, users who are already running the GroupWise client can continue to access the post office; after they exit, they cannot access the post office again until the post office is enabled.

A post office must be disabled if you are rebuilding the post office database ([wphost.db](#)). You might also want to disable a post office when you are doing a complete GroupWise system backup. That ensures that all data is consistent at the time of the backup.

- 1 In ConsoleOne, browse to and right-click the Post Office object, then click *Properties*.
- 2 Click *GroupWise > Client Access Settings* to display the Client Access Settings page.



- 3 Select *Disable Logins*, then click *OK* to disable the post office.
- 4 (Conditional) To re-enable logins and make the post office available again, deselect *Disable Logins*.

12.10 Moving a Post Office

You cannot move a Post Office object in ConsoleOne because it is a container object. Only leaf objects can be moved. If you need to change the context, graft the GroupWise post office to its corresponding eDirectory object in the new container location. See [Section 5.15, "GW / eDirectory Association,"](#) on [page 99](#) for more information on grafting objects.

You can, however, move the post office directory, the post office database ([wphost.db](#)), and the other databases that reside in the post office by copying the post office directory structure and all its contents to the new location.

IMPORTANT: These instructions are for moving the post office from one location to another on the same platform. If you want to move a post office from a Windows server to a Linux server, follow the instructions in the [GroupWise Server Migration Guide](#).

To move a post office directory structure and all its contents:

- 1 Make sure all users are out of the post office, then disable logins to the post office. See [Section 12.9, “Disabling a Post Office,”](#) on page 212.
- 2 Back up the post office. See [Chapter 31, “Backing Up GroupWise Databases,”](#) on page 431.
- 3 In ConsoleOne, display the Identification page of the post office to move.
- 4 In the *UNC Path* field, change the UNC path to the location where you want to move the post office, then click *OK* to save the new location.

The format of the path in the *UNC Path* field depends on whether you are running Linux ConsoleOne or Windows ConsoleOne, and on whether the post office is on Linux or Windows. Retain the original format of the path in your modified version of the location.

The location change is then propagated up to the domain.

- 5 Stop the POA for the post office.

- 6 (Conditional) On Linux:

6a In a terminal window, log in as *root*, then provide the *root* password.

6b Use *cp* to copy the post office directory and database to the new location:

```
cp -r post_office_directory destination
```

- 7 (Conditional) On Windows:

7a Use *xcopy* with the */s* and */e* options to move the post office directory and its contents:

```
xcopy post_office_directory /s /e destination
```

These options re-create the same directory structure even if directories are empty.

7b Give rights to objects that need to access the post office database.

For example, if the new location is on a different server, the POA and the GroupWise administrators who run ConsoleOne need adequate rights to the new location, as described in [Chapter 87, “GroupWise Administrator Rights,”](#) on page 1127.

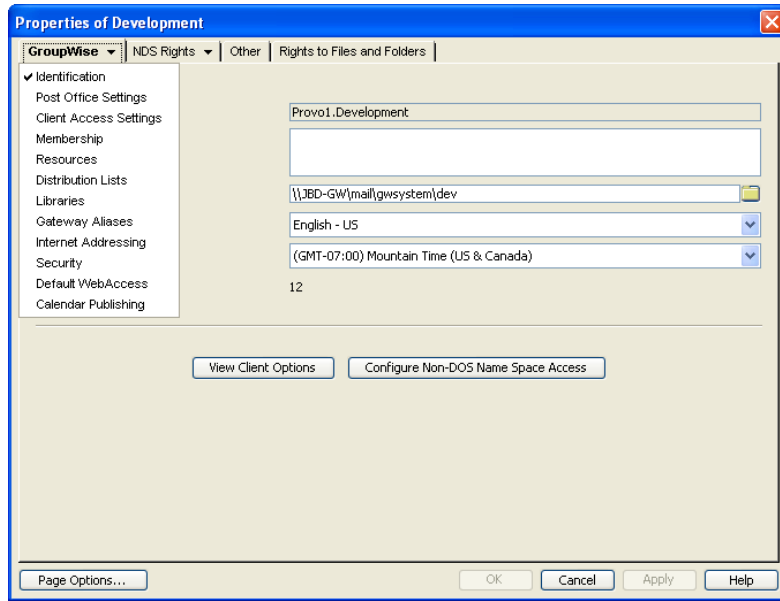
- 8 Edit the POA startup file by changing the setting of the */home* switch, then restart the POA. See [Section 36.1.6, “Adjusting the POA for a New Post Office Location,”](#) on page 491.
- 9 When you are sure the post office is functioning properly, delete the original post office directories.

If you need to move the POA along with its post office, see [Section 36.1.5, “Moving the POA to a Different Server,”](#) on page 490.

12.11 Deleting a Post Office

You cannot delete a post office until you have deleted or moved all objects that belong to it. Keep the POA running until after you have deleted the post office, so that it can process the object deletion requests.

- 1 In ConsoleOne, browse to and right-click the Post Office object to delete, then click *Properties*.



- 2 Click *GroupWise > Resources*, then delete any resources that still belong to the post office.
See [Section 16.6, "Deleting a Resource,"](#) on page 274. You must delete resources before users, because users who own resources cannot be deleted without assigning a new owner in the same post office.
- 3 Click *GroupWise > Membership*, then delete or move any users that still belong to the post office.
See [Section 14.11, "Removing GroupWise Accounts,"](#) on page 255 and [Section 14.4, "Moving GroupWise Accounts,"](#) on page 234.
- 4 Click *GroupWise > Distribution Lists*, then delete any distribution lists that still belong to the post office.
See [Section 18.8, "Deleting a Distribution List,"](#) on page 294.
- 5 Click *GroupWise > Libraries*, then delete any libraries that still belong to the post office.
See [Section 22.6.7, "Deleting a Library,"](#) on page 354.
- 6 Click *OK* to perform the deletions.
As an alternative, it is very easy to perform such deletions in the GroupWise View. Select the Post Office object in the GroupWise View, then use the drop-down list of objects to display objects of each type that still belong to the post office. Delete any residual objects in the Console View.
- 7 In ConsoleOne, browse to and right-click the Domain object that owns the post office to delete, then click *Properties*.
- 8 Click *GroupWise > Post Offices*, select the post office to delete, then click *Delete*.
- 9 Stop the POA for the post office.

- 10** Uninstall the POA software if applicable, as described in the following sections in the *GroupWise 2012 Installation Guide*:
- ♦ “Uninstalling the Linux GroupWise Agents”
 - ♦ “Uninstalling the Windows GroupWise Agents”

12.12 Changing POA Configuration to Meet Post Office Needs

Because the POA delivers messages to mailboxes, responds in real time to client/server users, and maintains all databases located in the post office, its functioning affects the post office and all users who belong to the post office. Proper POA configuration is essential for a smoothly running GroupWise system. Complete details about the POA are provided in [Part IX, “Post Office Agent,” on page 469](#). As you create and manage post offices, you should keep in mind the following aspects of POA configuration:

- ♦ [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,” on page 508](#)
- ♦ [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510](#)
- ♦ [Section 36.3.5, “Enabling Intruder Detection,” on page 516](#)
- ♦ [Section 36.2.3, “Supporting IMAP Clients,” on page 498](#)
- ♦ [Section 36.2.4, “Supporting SOAP Clients,” on page 499](#)
- ♦ [Section 38.1, “Optimizing Client/Server Processing,” on page 559](#)
- ♦ [Section 36.4.1, “Scheduling Database Maintenance,” on page 517](#)
- ♦ [Section 36.4.3, “Performing Nightly User Upkeep,” on page 523](#)
- ♦ [Section 36.2.7, “Restricting Message Size between Post Offices,” on page 504](#)

IV Users

- ♦ [Chapter 13, “Creating GroupWise Accounts,” on page 219](#)
- ♦ [Chapter 14, “Managing GroupWise Accounts and Users,” on page 229](#)

13 Creating GroupWise Accounts

For users to be able to use GroupWise, you must give them GroupWise accounts. A GroupWise account defines the user in the GroupWise system by providing the user with a GroupWise user ID and GroupWise mailbox.

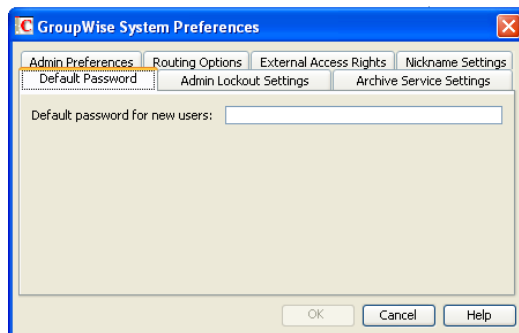
You can give GroupWise accounts to Novell eDirectory users during or after their creation in eDirectory. You can also give GroupWise accounts to users who do not have eDirectory accounts. Refer to the following sections for details:

- [Section 13.1, “Establishing a Default Password for All New GroupWise Accounts,”](#) on page 219
- [Section 13.2, “Creating GroupWise Accounts for eDirectory Users,”](#) on page 220
- [Section 13.3, “Creating GroupWise Accounts for Non-eDirectory Users,”](#) on page 224
- [Section 13.4, “Educating Your New Users,”](#) on page 226

13.1 Establishing a Default Password for All New GroupWise Accounts

To save time and energy when you are creating new GroupWise accounts, you can establish a default password to use for all new accounts.

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > System Preferences > Default Password*.



- 2 Type the password you want to use as the default, then click *OK*.
- 3 Explain to users how to set their own passwords in GroupWise, as described in:
 - [“Assigning a Password to Your Mailbox”](#) in the *GroupWise 2012 Windows Client User Guide*
 - [“Changing Your Password”](#) in the *GroupWise 2012 WebAccess User Guide*

Users cannot change their passwords using GroupWise WebAccess Mobile on tablet devices.

13.2 Creating GroupWise Accounts for eDirectory Users

Depending on your needs, you can choose from the following methods to create GroupWise accounts for eDirectory users:

- ♦ **Creating a Single GroupWise Account:** You can create a GroupWise account for a single eDirectory user by editing the GroupWise information on his or her User object. This method lets you create the GroupWise account on any post office, select the GroupWise user ID, and configure optional GroupWise information. It provides the most flexibility in creating a user's GroupWise account.
- ♦ **Creating Multiple GroupWise Accounts:** You can create GroupWise accounts for multiple eDirectory users by editing the membership information on a Post Office object. This method allows you to quickly add multiple users to the same post office at one time. However, you cannot select the user's GroupWise user ID; instead, the user's eDirectory user name is automatically used as his or her GroupWise user ID. In addition, to configure other optional GroupWise information for a user, you need to modify each User object.

13.2.1 Creating a Single GroupWise Account

To create a GroupWise account for an eDirectory user:

- 1 In ConsoleOne, right-click the User object, then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page.

- 3 Fill in the following fields:

Post Office: Select the post office where you want the user's mailbox created.

Mailbox ID: The mailbox ID (also referred to as the GroupWise user ID or user name) defaults to the eDirectory user name. You can change it if necessary.

Do not use any of the following invalid characters in the mailbox ID:

ASCII characters 0-31	Comma ,
Asterisk *	Double quote “
At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

IMPORTANT: Each user’s mailbox ID becomes part of the user’s email address. Characters that are valid and even desirable in a mailbox ID, such as accented characters, might not be valid in an email address. For some users, you might need to set up a preferred email ID in order to ensure that they have a valid email address. For instructions, see [Section 14.7.2, “Changing a User’s Internet Addressing Settings,”](#) on page 249.

4 Click *Apply* to create the account.

You must create the account by clicking *Apply* (or *OK*) before you can modify any of the other fields, including the GroupWise password.

5 If desired, modify any of the following optional fields:

Visibility: Select the level at which you want the user to be visible in the Address Book. System enables the user to be visible to all users in your GroupWise system. *Domain* enables the user to be visible to all users in the same domain as the user. *Post Office* enables the user to be visible to all users on the same post office as the user. Setting the visibility level to *None* means that no users can see the user in the Address Book. However, even if the user is not displayed in the Address Book, other users can send messages to the user by typing the user’s ID (mailbox ID) in a message’s *To* field.

External Sync Override: This option applies only if your GroupWise system links to and synchronizes with an external system, as described in [“Connecting to Other GroupWise Systems”](#) in the *GroupWise 2012 Multi-System Administration Guide*.

- ◆ **Synchronize According to Visibility:** The user information is synchronized to external systems only if visibility is set to *System*.
- ◆ **Synchronize Regardless of Visibility:** The user information is synchronized to external systems regardless of the object visibility.
- ◆ **Don’t Synchronize Regardless of Visibility** The user information is not synchronized to external systems.

Account ID: This option applies only if you have a GroupWise gateway that supports accounting. For more information about gateway accounting, see your [GroupWise gateway documentation \(http://www.novell.com/documentation/gwgateways\)](#).

File ID: This three-letter ID is randomly generated and is non-editable. It is used for various internal purposes within the GroupWise system, including ensuring that files associated with the user have unique names.

Expiration Date: If you want the user’s GroupWise account to no longer work after a certain date, specify the expiration date. This date applies to the user’s GroupWise account only; it is independent of the eDirectory account expiration date (User object > *Restrictions* > *Login Restrictions*). For more information, see [Section 14.11.2, “Expiring a GroupWise Account,”](#) on page 257.

Gateway Access: This option applies only if you have GroupWise gateways that support access restrictions. For more information, see your [GroupWise gateway documentation \(http://www.novell.com/documentation/gwgateways\)](http://www.novell.com/documentation/gwgateways).

Disable Logins: Select this option to prevent the user from accessing his or her GroupWise mailbox. For more information, see [Section 14.9, “Disabling and Enabling GroupWise Accounts,”](#) on page 254.

LDAP Authentication: This option applies only if you are using LDAP to authenticate users to GroupWise, as described in [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,”](#) on page 510, and if the LDAP server is not a Novell LDAP server. If this is the case, specify the user’s LDAP authentication ID.

Restore Area: This field applies only if you are using the GroupWise backup and restore features. If so, this field indicates the location where the user’s mailbox is being backed up. For details, see [Chapter 32, “Restoring GroupWise Databases from Backup,”](#) on page 433.

View Client Options: Click *View Client Options* as a convenient shortcut for *Tools > GroupWise Utilities > Client Options* in order to modify client options for the currently selected user. For more information, see [Chapter 76, “Setting Defaults for the GroupWise Client Options,”](#) on page 1025.

Change GroupWise Password: Click this option to assign a password to the user’s GroupWise account or change the current password. The user is prompted for this password each time he or she logs in to GroupWise.

To be able to skip this option by setting a default password, see [Section 13.1, “Establishing a Default Password for All New GroupWise Accounts,”](#) on page 219.

Delete GroupWise Account: Click this option to delete the user’s GroupWise account. This includes the user’s mailbox and all items in the mailbox. The user’s eDirectory account is not affected. For more information, see [Section 14.11, “Removing GroupWise Accounts,”](#) on page 255

E-Mail Address: Displays the default email address for the user. Click the drop-down list to specify a custom email address.

GroupWise Resource objects and Distribution List objects have this field on their Identification page. User objects have this GroupWise field on their General page along with other eDirectory user information.

6 Click *Apply* to save the changes.

7 Click *GroupWise > General > Identification* to display the user’s current eDirectory information.

This information appears in the GroupWise Address Book, as described in [Chapter 6, “GroupWise Address Book,”](#) on page 105. If you keep private information in the *Description* field of the User object, you can prevent this information from appearing the GroupWise Address Book. See [Section 6.1.6, “Preventing the User Description Field from Displaying in the Address Book,”](#) on page 109.

8 Make sure that the user’s eDirectory information is current, then click *OK*.

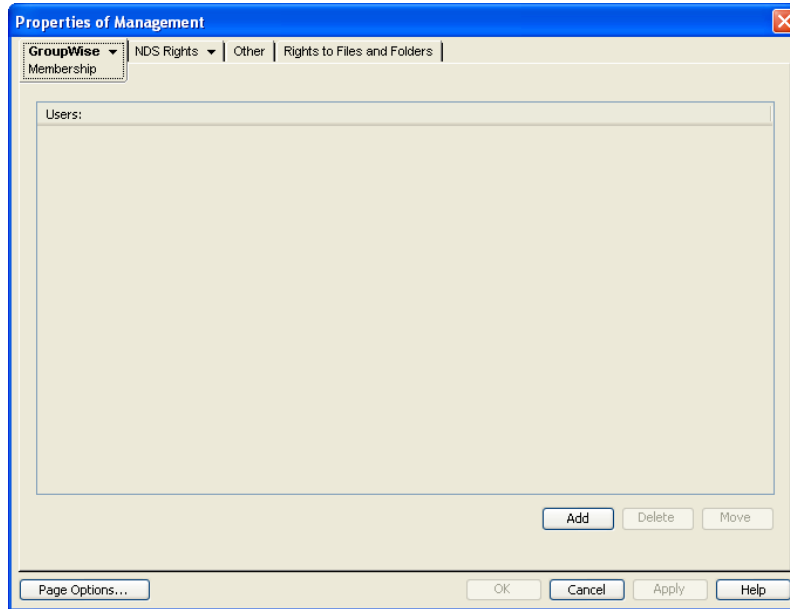
13.2.2 Creating Multiple GroupWise Accounts

If you have multiple eDirectory users who will have GroupWise accounts on the same post office, you can use the Post Office object’s Membership page to quickly add the users and create their accounts. Each user’s GroupWise user ID will be the same as his or her eDirectory user name.

To create GroupWise accounts for multiple eDirectory users:

1 In ConsoleOne, right-click the Post Office object, then click *Properties*.

- 2 Click *GroupWise > Membership* to display the Membership page.



- 3 Click *Add*, select the eDirectory user you want to add to the post office, then click *OK* to add the user to the post office's membership list.

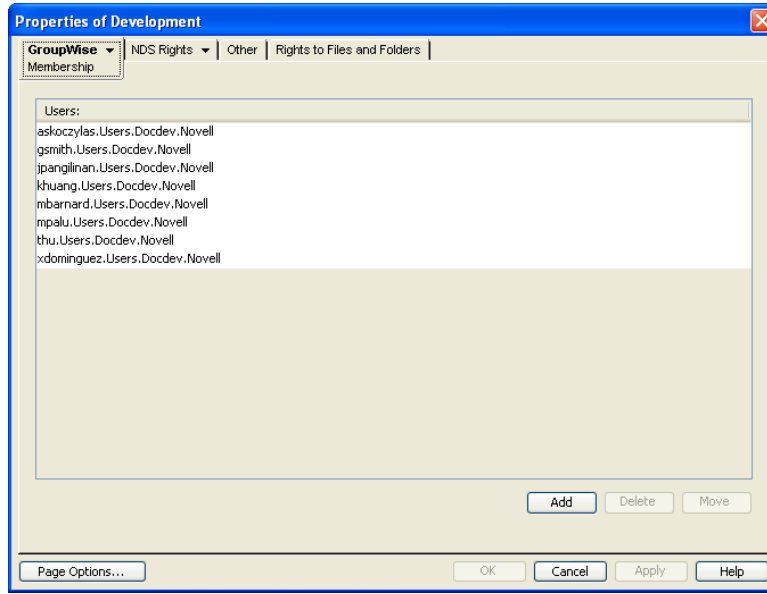
By default, the user's eDirectory user name is used as the GroupWise ID.

A GroupWise user ID cannot contain any of the following invalid characters:

ASCII characters 0-31	Comma ,
Asterisk *	Double quote "
At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

IMPORTANT: Each user's GroupWise ID becomes part of the user's email address. Characters that are valid and even desirable in a GroupWise ID, such as accented characters, might not be valid in an email address. For some users, you might need to set up a preferred email ID in order to ensure that they have a valid email address. For instructions, see [Section 14.7.2, "Changing a User's Internet Addressing Settings,"](#) on page 249.

- Repeat [Step 3](#) to create additional GroupWise accounts in the post office.



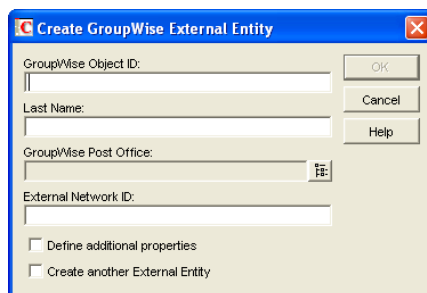
- When you are finished, click *OK* to save the changes.

13.3 Creating GroupWise Accounts for Non-eDirectory Users

If you have users who do not have eDirectory accounts, you can still assign them GroupWise accounts by defining them as GroupWise external entities in eDirectory. Defining a user as a GroupWise external entity provides the user with access to GroupWise only; it does not enable the user to log in to eDirectory. External entities have eDirectory objects, but they are not considered eDirectory users for licensing purposes.

To create a GroupWise account for a non-eDirectory user:

- In ConsoleOne, right-click the eDirectory container where you want to create the user's GroupWise External Entity object, then click *New > Object* to display the New Object dialog box.
- Select *GroupWise External Entity*, then click *OK* to display the Create GroupWise External Entity dialog box.



- Fill in the following fields:

GroupWise Object ID: Specify the user's GroupWise ID. The user's ID along with the user's post office and domain, provide the user with a unique name within the GroupWise system (*userID.po.domain*).

Do not use any of the following invalid characters in the GroupWise object ID:

ASCII characters 0-31	Comma ,
Asterisk *	Double quote "
At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

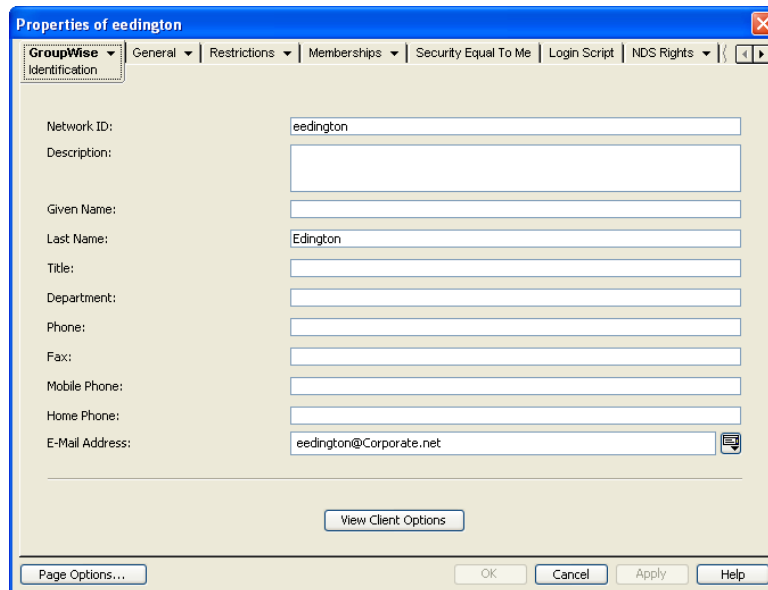
IMPORTANT: Each user's GroupWise ID becomes part of the user's email address. Characters that are valid and even desirable in a GroupWise ID, such as accented characters, might not be valid in an email address. For some users, you might need to set up a preferred email ID in order to ensure that they have a valid email address. For instructions, see [Section 14.7.2, "Changing a User's Internet Addressing Settings,"](#) on page 249.

Last Name: Specify the user's last name.

GroupWise Post Office: Select the post office where you want the user's mailbox.

External Network ID: Specify the user's network ID for the network that he or she logs in to.

- 4 Select *Define Additional Properties*, then click *OK* to display the GroupWise Identification page.



The screenshot shows a dialog box titled "Properties of eedington" with a "GroupWise Identification" tab selected. The dialog has several tabs: "General", "Restrictions", "Memberships", "Security Equal To Me", "Login Script", and "NDS Rights". The "Identification" tab contains the following fields:

- Network ID: eedington
- Description: (empty)
- Given Name: (empty)
- Last Name: Edington
- Title: (empty)
- Department: (empty)
- Phone: (empty)
- Fax: (empty)
- Mobile Phone: (empty)
- Home Phone: (empty)
- E-Mail Address: eedington@Corporate.net

At the bottom of the dialog, there is a "View Client Options" button and a standard Windows dialog footer with "Page Options...", "OK", "Cancel", "Apply", and "Help" buttons.

- 5 If desired, fill in any of the fields on the Identification page.

This information appears in the GroupWise Address Book, as described in [Section 6.1, "Customizing Address Book Fields,"](#) on page 105. If you want to keep private information in the Description field, you can prevent this information from appearing in the GroupWise Address Book. See [Section 6.1.6, "Preventing the User Description Field from Displaying in the Address Book,"](#) on page 109.

- 6 If you want the external entity user to be able to access his or her GroupWise mailbox using LDAP authentication, as described in [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510](#), click *GroupWise > Account*, then provide the fully distinguished name of the user’s External Entity object in LDAP format (for example, `cn=user_id,ou=orgunit,o=organization`).
- 7 Click *OK* to save the information.

The user is given a GroupWise mailbox in the post office you selected and can access his or her mailbox through the GroupWise client.

13.4 Educating Your New Users

After users can log in to their GroupWise accounts, all of the GroupWise client’s features are at their fingertips, but some new users do not know how to get started. You can give your users the following suggestions to encourage them to explore GroupWise.

- ♦ [Section 13.4.1, “GroupWise Windows Client,” on page 226](#)
- ♦ [Section 13.4.2, “GroupWise WebAccess,” on page 227](#)
- ♦ [Section 13.4.3, “GroupWise WebAccess Mobile,” on page 227](#)

You can also provide users with *Quick Starts* that cover specialized GroupWise functionality:

- ♦ *Calendar Publishing Quick Start* (http://www.novell.com/documentation/groupwise2012/pdfdoc/gw2012_qs_calpubuser/gw2012_qs_calpubuser.pdf)
- ♦ *GroupWise and Skype Quick Start* (http://www.novell.com/documentation/groupwise2012/pdfdoc/gw2012_qs_skype/gw2012_qs_skype.pdf)
- ♦ *GroupWise and Messenger Quick Start* (http://www.novell.com/documentation/groupwise2012/pdfdoc/gw2012_qs_messenger22/gw2012_qs_messenger22.pdf)
- ♦ *GroupWise and Vibe Quick Start* (http://www.novell.com/documentation/groupwise2012/pdfdoc/gw2012_qs_vibe/gw2012_qs_vibe.pdf)
- ♦ *WebAccess Basic Interface Quick Start* (http://www.novell.com/documentation/groupwise2012/pdfdoc/gw2012_qs_webaccbasic/gw2012_qs_webaccbasic.pdf) for mobile device users

You can also refer users to the [GroupWise 2012 User Frequently Asked Questions](http://www.novell.com/documentation/groupwise2012/gw2012_guide_userfaq/data/gw2012_guide_userfaq.html) (http://www.novell.com/documentation/groupwise2012/gw2012_guide_userfaq/data/gw2012_guide_userfaq.html).

NOTE: For convenience in printing, all GroupWise User Guides are available in PDF format at the [GroupWise 2012 Documentation Web site](http://www.novell.com/documentation/groupwise2012) (<http://www.novell.com/documentation/groupwise2012>).

13.4.1 GroupWise Windows Client

In the GroupWise Windows client:

- ♦ Click *Help > Help Topics* to learn to perform common GroupWise tasks.
- ♦ Click *Help > What’s New* to learn about the latest new GroupWise features.
- ♦ Click *Help > Training and Tutorials* to display the BrainStorm, Inc. [QuickHelp for GroupWise 2012](http://www.brainstorminc.com/landing/product-integration/novell/gw-2012-quickhelp.aspx) (<http://www.brainstorminc.com/landing/product-integration/novell/gw-2012-quickhelp.aspx>) or customized training materials provided for your users.

Use ConsoleOne to change the URL that displays when users click *Help > Training and Tutorials*. In ConsoleOne, use *Client Options > Environment > Tutorial* to specify the URL for your customized training materials.

- ◆ Click *Help > User Guide* to view the [GroupWise 2012 Windows Client User Guide](#) in HTML format. The guide includes more background information on GroupWise features than the Help does.

13.4.2 GroupWise WebAccess

In GroupWise WebAccess:

- ◆ Click *Help* to learn to perform common GroupWise tasks.
- ◆ Click *Help > What's New in GroupWise 2012* to learn about the latest new GroupWise features.
- ◆ Click *Help > Novell GroupWise 2012 Documentation Web Site* to access the [GroupWise 2012 WebAccess Mobile User Guide](#). The guide includes more background information on GroupWise features than the Help does.

13.4.3 GroupWise WebAccess Mobile

In GroupWise WebAccess Mobile:

- ◆ Click *Help* to learn to perform common GroupWise tasks.
- ◆ Click *Help > What's New in GroupWise 2012* to learn about the latest new GroupWise features.
- ◆ Click *Help > Novell GroupWise 2012 Documentation Web Site* to access the [GroupWise 2012 WebAccess User Guide](#). The guide includes more background information on GroupWise features than the Help does.

14 Managing GroupWise Accounts and Users

As your GroupWise system grows, you will need to add users and manage their GroupWise accounts.

- ♦ [Section 14.1, “Adding a User to a Distribution List,” on page 229](#)
- ♦ [Section 14.2, “Allowing Users to Modify Distribution Lists,” on page 230](#)
- ♦ [Section 14.3, “Adding a Global Signature to Users’ Messages,” on page 231](#)
- ♦ [Section 14.4, “Moving GroupWise Accounts,” on page 234](#)
- ♦ [Section 14.5, “Renaming Users and Their GroupWise Accounts,” on page 242](#)
- ♦ [Section 14.6, “Managing Mailbox Passwords,” on page 243](#)
- ♦ [Section 14.7, “Managing User Email Addresses,” on page 247](#)
- ♦ [Section 14.8, “Checking GroupWise Account Usage,” on page 253](#)
- ♦ [Section 14.9, “Disabling and Enabling GroupWise Accounts,” on page 254](#)
- ♦ [Section 14.10, “Unlocking GroupWise Accounts,” on page 254](#)
- ♦ [Section 14.11, “Removing GroupWise Accounts,” on page 255](#)

See also:

- ♦ [Chapter 26, “Maintaining Domain and Post Office Databases,” on page 401](#)
- ♦ [Chapter 27, “Maintaining User/Resource and Message Databases,” on page 409](#)
- ♦ [Chapter 31, “Backing Up GroupWise Databases,” on page 431](#)

Proper database maintenance and backups allow recovery from accidental deletions, as described in the following sections:

- ♦ [Section 32.5, “Restoring Deleted Mailbox Items,” on page 435](#)
- ♦ [Section 32.6, “Recovering Deleted GroupWise Accounts,” on page 438](#)

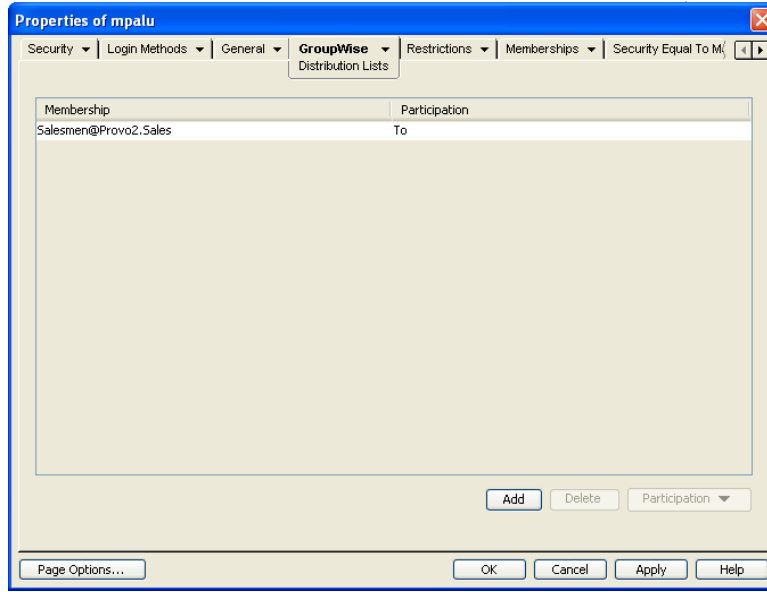
14.1 Adding a User to a Distribution List

GroupWise distribution lists are sets of users and resources that can be addressed as a single entity. When a GroupWise user addresses an item (message, appointment, task, or note) to a distribution list, each user or resource that is a member receives a copy of the item.

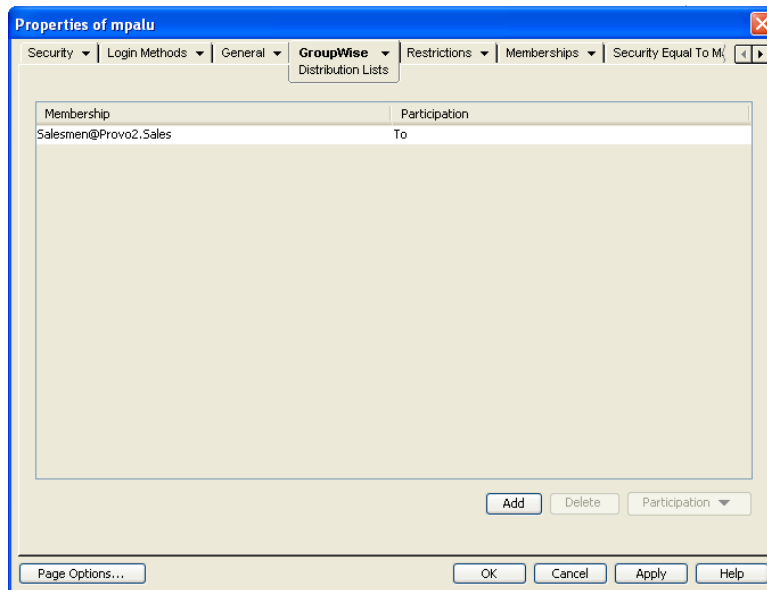
To add a user to a distribution list:

- 1 In ConsoleOne, right-click the User object, then click *Properties*.

- 2 Click *GroupWise > Distribution Lists* to display the Distribution Lists page.



- 3 Click *Add*, select the distribution list that you want to add the user to, then click *OK*.



By default, the user is added as a primary recipient (*To* recipient).

- 4 If you want to change the resource's recipient type, select the distribution list, click *Participation*, then click *To*, *CC*, or *BC*.
- 5 Click *OK* to save your changes.

14.2 Allowing Users to Modify Distribution Lists

Because distribution lists are created in ConsoleOne, users by default cannot modify them. However, in ConsoleOne, you can grant rights to selected users to modify specific distribution lists. For setup instructions, see [Section 18.6, "Enabling Users to Modify a Distribution List,"](#) on page 291.

14.3 Adding a Global Signature to Users' Messages

You can build a list of globally available signatures to be automatically appended to messages sent by GroupWise client users. Global signatures are created in HTML format. For users who prefer the Plain Text compose view in the GroupWise client, a plain text version of the signature is appended instead of the HTML version. When this occurs, HTML formatting and embedded images are lost, but you can customize the plain text version as needed to compensate for the loss of HTML formatting.

For Windows client users, the global signature is appended by the client to messages after any personal signatures that users create for themselves. It is appended after the user clicks *Send*. If S/MIME encryption is enabled, the global signature is encrypted along with the rest of the message. Windows client users can choose whether global signatures are appended only for recipients outside the local GroupWise system or for all recipients, local as well as external. For Windows client users, you can assign a global signature based on users, resources, post offices, and domains.

For all client users, the Internet Agent (GWIA) can append global signatures to the end of messages for recipients outside the local GroupWise system. However, the GWIA does not append global signatures to S/MIME-encoded messages, nor does it duplicate global signatures already appended by the Windows client. You can assign a default global signature for all users in your system and then override that default by editing the properties of each GWIA object

- ◆ [Section 14.3.1, “Creating Global Signatures,” on page 231](#)
- ◆ [Section 14.3.2, “Selecting a Default Global Signature for All Outgoing Messages,” on page 232](#)
- ◆ [Section 14.3.3, “Assigning Global Signatures to GWIAs,” on page 233](#)
- ◆ [Section 14.3.4, “Assigning Global Signatures to Windows Client Users,” on page 233](#)
- ◆ [Section 14.3.5, “Excluding Global Signatures,” on page 234](#)

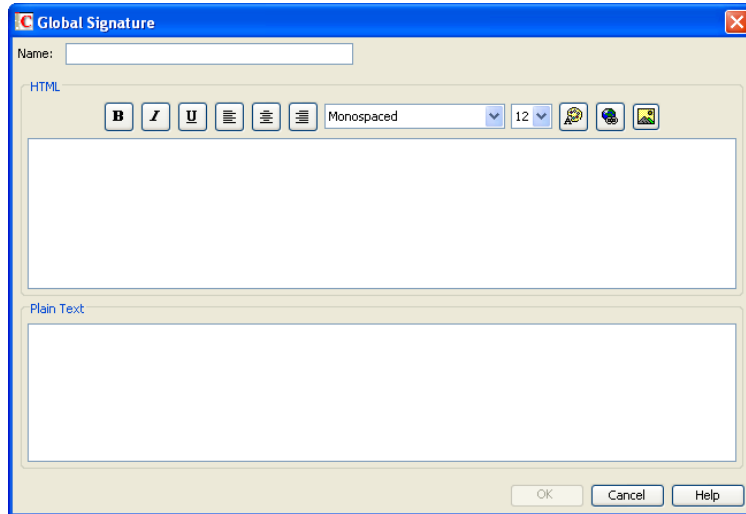
NOTE: If a user sends an external message with a subject only (no message body), a global signature is not appended. This is working as designed. The presence of a global signature on an external message with an empty message body would prevent the GWIA `/flatfwd` switch from functioning correctly.

14.3.1 Creating Global Signatures

- 1 Click *Tools > GroupWise System Operations > Global Signatures*.



- 2 Click *Create* to create a new global signature.

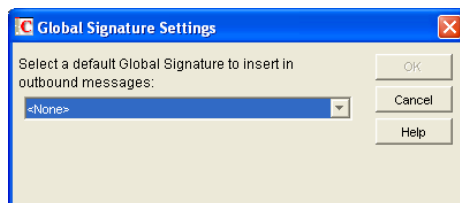


- 3 Specify a descriptive name for the signature.
- 4 Compose the signature using the basic HTML editing tools provided, then click *OK* to add the new signature to the list in the Global Signatures dialog box.
- 5 If you want to check or edit the text version of the signature that was automatically generated:
 - 5a Select the new signature, then click *Edit*.
 - 5b Modify the text version of the signature as needed, then click *OK*.
- 6 Click *OK* in the Global Signatures list dialog box to save the list.

14.3.2 Selecting a Default Global Signature for All Outgoing Messages

If you want the GWIA to append a global signature to all outgoing messages:

- 1 Click *Tools > GroupWise System Operations > Global Signatures*.
- 2 Click *Settings*.

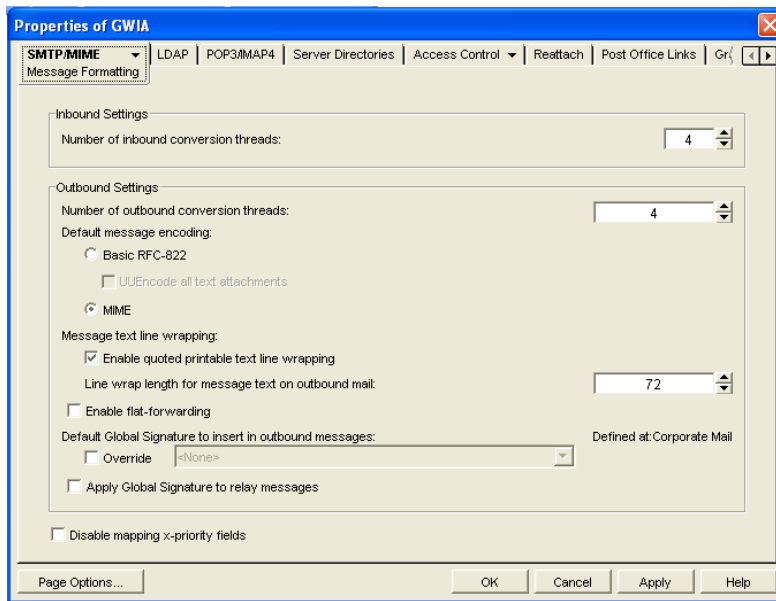


- 3 In the drop-down list, select the default global signature, then click *OK*.

14.3.3 Assigning Global Signatures to GWIAs

If your organization needs more than one global signature on outgoing messages, you can assign different global signatures to GWIAs as needed.

- 1 Browse to and right-click an GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Message Formatting*.



- 3 Under *Default Global Signature to Insert in Outbound Messages*, select *Override*, then select the global signature that you want this GWIA to append to messages.
- 4 Click *OK* to save the setting.

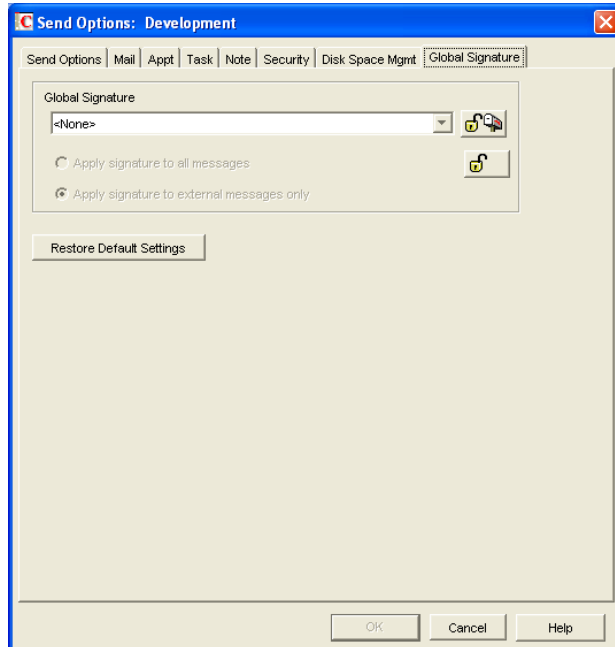
14.3.4 Assigning Global Signatures to Windows Client Users

For Windows client users, you can assign different global signatures to different sets of users by domain, post office, and individual user.

A global signature set at the post office level overrides the global signature set at the domain level. A global signature set at the user level overrides the global signature set at the post office and domain level.

- 1 Browse to and select the domain, post office, or set of users to which you want to assign a global signature.
- 2 Click *Tools > GroupWise Utilities > Client Options*.

- 3 Double-click *Send*, then click *Global Signature*.



- 4 In the *Global Signature* drop-down list, select the global signature that you want to use.
By default, the selected signature is applied only to messages that are being sent outside your GroupWise system.
- 5 Select *Apply Signature to All Messages* if you want to also use global signatures internally.
- 6 Click *OK* to save the settings.

14.3.5 Excluding Global Signatures

You might have a domain, post office, or set of users where you do not want the global signature to be added to messages. You can suppress global signatures at the domain, post office, or user level.

- 1 Browse to and select the domain, post office, or users for which you want to suppress a global signature.
- 2 Click *Tools > GroupWise Utilities > Client Options*.
- 3 Double-click *Send*, then click *Global Signature*.
- 4 In the *Global Signature* drop-down list, select *<None>*, then click *OK*.

14.4 Moving GroupWise Accounts

Expansion or consolidation of your GroupWise system can make it necessary for you to move GroupWise accounts from one post office to another.

When you move a GroupWise account, the user's mailbox is physically moved from one post office directory to another. The user's Novell eDirectory object, including the GroupWise account information, remains in the same eDirectory container.

When you move a user's GroupWise account, all items are moved correctly and all associations (proxy rights, shared folder access, and so on) are resolved so that the move is transparent to the user. Occasionally, some client options the user has set (GroupWise client > *Tools* > *Options*) might be lost and must be re-created for the new mailbox.

The following sections provide information you should know before performing a move and instructions to help you perform the move.

- ♦ [Section 14.4.1, "Live Move vs. File Transfer Move," on page 235](#)
- ♦ [Section 14.4.2, "Preparing for a User Move," on page 235](#)
- ♦ [Section 14.4.3, "Moving a GroupWise Account to Another Post Office in the Same eDirectory Tree," on page 236](#)
- ♦ [Section 14.4.4, "Moving a GroupWise Account to Another Post Office in a Different eDirectory Tree," on page 238](#)
- ♦ [Section 14.4.5, "Monitoring User Move Status," on page 240](#)

14.4.1 Live Move vs. File Transfer Move

GroupWise provides two types of moves: a live move and a file transfer move.

A live move uses a TCP/IP connection between Post Office Agents (POAs) to move a user from one post office to another. In general, a live move is significantly faster (approximately 5 to 10 times) than a file transfer move. However, it does require that TCP/IP is functioning efficiently between the two POAs.

A file transfer move uses the transfer of message files (using POAs and MTAs) rather than a TCP/IP connection between POAs. A file transfer move is required if you are moving a user across a WAN link where TCP/IP might not be efficient.

By default, when you initiate a user move, the post office's POA attempts to establish a live move session with the destination post office's POA. If it cannot, a file transfer move is used instead.

If desired, you can disable the live move capability (Post Office object > *GroupWise* > *Identification* > *Disable Live Move*). Any moves to or from the post office would be done by file transfer.

14.4.2 Preparing for a User Move

Proper preparation can make the process of moving users go more smoothly. Consider the following before moving a user's GroupWise account:

- ♦ Make sure the POAs for the user's current post office and destination post office are running.
See [Chapter 37, "Monitoring the POA," on page 525](#).
- ♦ Configure both POAs for verbose logging, in case troubleshooting is required during the user move process.
See [Section 37.3, "Using POA Log Files," on page 551](#).
- ♦ If you are performing the user move during off hours, optimize both POAs for the user move process. On the Agent Settings property page of the POA object in ConsoleOne, set *Max Thread Usage for Priming and Moves* to 80%. Set *Client/Server Handler Threads* to 40. If you must move multiple users during regular work hours, you can set up additional POA instances customized for the user move process. This would prevent the user move process from impacting users' regular activities in their mailboxes.

See [Section 38.2.2, “Configuring a Dedicated Message File Processing POA \(Windows Only\),”](#) on page 565.

- ♦ Make sure the Message Transfer Agent (MTA) for the user’s current domain and destination domain (if different) are running.
See [Chapter 43, “Monitoring the MTA,”](#) on page 659.
- ♦ Make sure that all links between POAs and MTAs are all open.
See [Section 10.2, “Using the Link Configuration Tool,”](#) on page 161, [Section 71.3.1, “Link Trace Report,”](#) on page 979, and [Section 71.3.2, “Link Configuration Report,”](#) on page 980.
- ♦ Make sure that all domain databases along the route for the user move are valid.
See [Section 26.1, “Validating Domain or Post Office Databases,”](#) on page 401.
- ♦ Make sure that the mailbox to move is valid. Select the *Structure*, *Index*, and *Contents* options in GroupWise Check (GWCheck) or in Mailbox/Library Maintenance in ConsoleOne.
See [Section 27.1, “Analyzing and Fixing User and Message Databases,”](#) on page 409.
- ♦ Enable automatic creation of nicknames for moved users, so that replies and forwarded messages can be delivered successfully after the user has been moved.
See [Section 4.2.4, “Nickname Settings,”](#) on page 75.
- ♦ A user who owns a resource cannot be moved. If the user owns a resource, reassign ownership of the resource to another user who is on the same post office as the resource. You can do this beforehand, or when initiating the user move.
See [Section 16.2, “Changing a Resource’s Owner,”](#) on page 271
- ♦ (Optional) To reduce the number of mailbox items that must be moved, consider asking the user to clean up his or her mailbox by deleting or archiving items. Have the user empty the Trash so that deleted items are not moved with the user.
- ♦ (Optional) Have the user exit the GroupWise client and GroupWise Notify before you initiate the move. When the move is initiated, the user’s POA first creates an inventory list of all information in the user’s mailbox. This inventory list is sent to the new post office’s POA so that it can verify when all items have been received. If the user has not exited when the move begins, the user is automatically logged out so that the inventory list can be built. However, after the move has been initiated, the user can log in to his or her new mailbox even if the move is not complete.

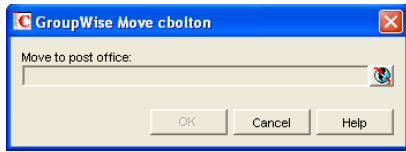
14.4.3 Moving a GroupWise Account to Another Post Office in the Same eDirectory Tree

The following steps apply only if the user’s current post office and destination post office are located in the same eDirectory tree. If not, see [Section 14.4.4, “Moving a GroupWise Account to Another Post Office in a Different eDirectory Tree,”](#) on page 238.

To move a user’s GroupWise account to a different post office in the same eDirectory tree:

- 1 In ConsoleOne, connect to the domain that owns the destination post office where you are moving the user.
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,”](#) on page 69.
- 2 In the GroupWise View, right-click the User object or GroupWise External Entity, then click *Move* to display the GroupWise Move dialog box.

If you want to move multiple users from the same post office to another post office, select all the User objects, right-click the selected objects, then click *Move*.



- 3 Select the post office to which you want to move the user's account, then click *OK*.

If the user owns a resource, the following dialog box appears.



- 4 Select a new owner for the resource, then click *OK*.
- 5 Keep track of the user move process using the User Move utility. See [Section 14.4.5, "Monitoring User Move Status,"](#) on page 240

Resolving Addressing Issues Caused By Moving an Account

The user's new address information is immediately replicated to each post office throughout your system so that the GroupWise Address Book contains the user's updated address. Any user who selects the moved user from the GroupWise Address Book can successfully send messages to the user.

However, some users might have the user's old address (GroupWise user ID) in their Frequent Contacts Address Book. In this case, if the sender types the moved user's name in the To field rather than selecting it from the Address Book, GroupWise uses the old address stored in the Frequent Contacts Address Book instead of the new address in the GroupWise Address Book. This results in the message being undeliverable. The POA automatically resolves this issue when it performs its nightly user upkeep (see [Section 36.4.3, "Performing Nightly User Upkeep,"](#) on page 523). During the nightly user upkeep process, the POA ensures that all addresses in a user's Frequent Contacts Address Book are valid addresses in the GroupWise Address Book.

If you want to ensure that messages sent to the user's old address are delivered even before the POA cleans up the Frequent Contacts Address Book, you can create a nickname using the old GroupWise user ID. For information about creating a nickname, see [Section 14.7.4, "Creating a Nickname for a User,"](#) on page 252. To have a nickname created automatically when the user is moved, see [Section 4.2, "System Preferences,"](#) on page 72.

14.4.4 Moving a GroupWise Account to Another Post Office in a Different eDirectory Tree

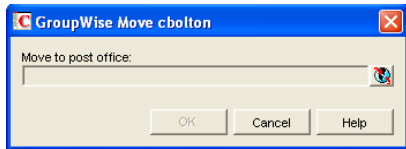
A GroupWise system can span multiple eDirectory trees, provided that all components for a single domain (post offices, users, resources, and so on) are all in the same eDirectory tree. For example, a user cannot be located in one tree and his or her post office in another.

If necessary, you can move a user's account from a post office in one eDirectory tree to a post office in another eDirectory tree as long as the post offices are in the same GroupWise system. This requires the user to have a User object (or GroupWise External Entity object) in the eDirectory tree to which his or her GroupWise account is being moved.

To move a user's GroupWise account to a post office in a different eDirectory tree:

- 1 Make sure the user has a User object or GroupWise External Entity object in the eDirectory tree to which his or her GroupWise account is being moved.
- 2 In ConsoleOne, right-click the User object or GroupWise External Entity object (in the GroupWise View) > click *Move* to display the GroupWise Move dialog box.

If you want to move multiple users from the same post office to another post office, select all the User objects, right-click the selected objects > click *Move*.

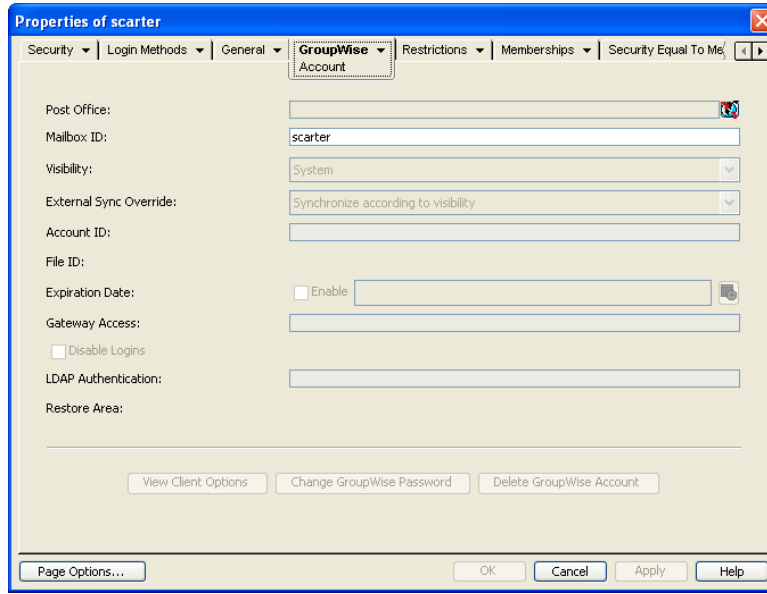


- 3 Select the post office to which you want to move the user's account, then click *OK*.
If the user owns a resource, the following dialog box appears.



- 4 Select a new owner for the resource, then click *OK*.
- 5 Keep track of the user move process by using the User Move utility to determine when the user has been successfully moved. See [Section 14.4.5, "Monitoring User Move Status,"](#) on page 240.
- 6 In the destination eDirectory tree, right-click the User object or GroupWise External Entity object where the GroupWise account will be assigned, then click *Properties*. This is the object referred to in [Step 1](#).

7 Click *GroupWise > Account* to display the Account page.



8 In the Post Office field, select the post office that the user's GroupWise account was moved to.

9 In the *Mailbox ID* field, make sure that the mailbox ID is the same as the user's mailbox ID (GroupWise user ID) on his or her original post office.

10 Click *OK*.

A dialog box appears asking if you want to match the GroupWise account to this eDirectory user.

11 Click *Yes*.

Resolving Addressing Issues Caused By Moving an Account

The user's new address information is immediately replicated to each post office throughout your system so that the GroupWise Address Book contains the user's updated address. Any user who selects the moved user from the GroupWise Address Book can successfully send messages to the user.

However, some users might have the moved user's old address (GroupWise user ID) in their Frequent Contacts Address Book. In this case, if the sender types the moved user's name in the To field instead of selecting it from the Address Book, GroupWise uses the old address stored in the Frequent Contacts Address Book instead of the new address in the GroupWise Address Book. This results in the message being undeliverable. The POA automatically resolves this issue when it performs its nightly user upkeep (see [Section 36.4.3, "Performing Nightly User Upkeep," on page 523](#)). During the nightly user upkeep process, the POA ensures that all addresses in a user's Frequent Contacts Address Book are valid addresses in the GroupWise Address Book.

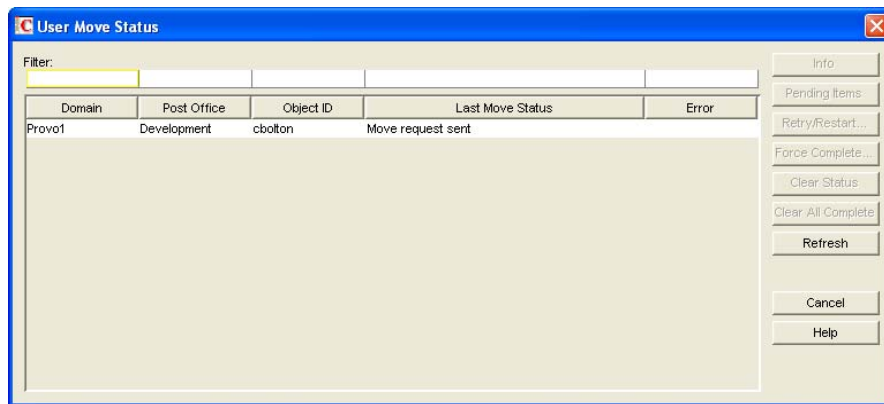
If you want to ensure that messages sent to the user's old address are delivered even before the POA cleans up the Frequent Contacts Address Book, you can create a nickname using the old GroupWise user ID. For information about creating a nickname, see [Section 14.7.4, "Creating a Nickname for a User," on page 252](#). To have a nickname created automatically when the user is moved, see [Section 4.2, "System Preferences," on page 72](#).

14.4.5 Monitoring User Move Status

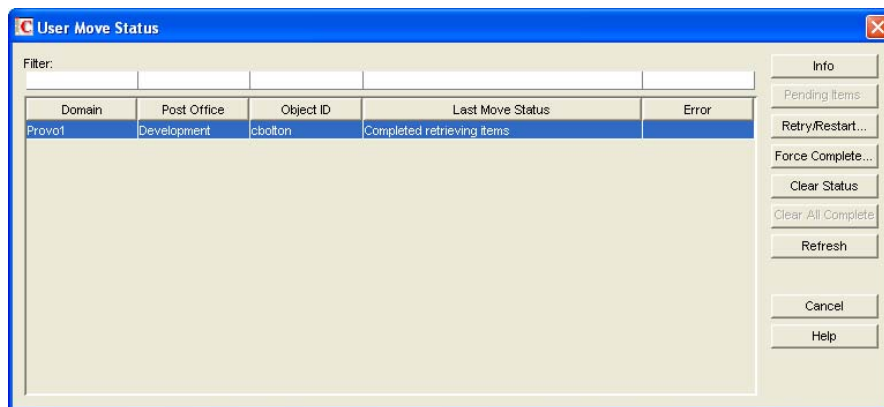
The User Move Status utility helps you track progress as you move users and resources from one post office to another. It displays the user moves associated with the object you selected before displaying the User Move Status dialog box. For example, if you selected a Domain object, all user moves for the selected domain are displayed, but not user moves for other domains.

While a GroupWise user account is being moved, the POA in the source post office and the POA in the destination post office communicate back and forth. You can track the move process progresses through various steps and statuses:

- 1 In ConsoleOne, select a Post Office or Domain object.
All moves occurring within the selected location will be listed.
- 2 Click *Tools > GroupWise Utilities > User Move Status*.



At the beginning of the move process, most buttons are dim, because it would not be safe for you to perform those actions at that point in the move process. When those actions are safe, the buttons become active.

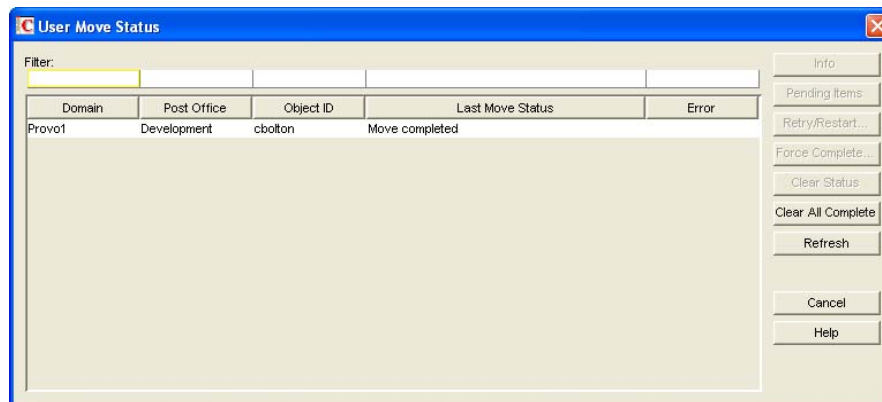


- 3 To restrict the number of users and resources in the list, type distinguishing information in any of the *Filter* fields, then press Enter to filter the list.
- 4 During the move, click *Refresh* to update the status information.

IMPORTANT: The list does not refresh automatically.

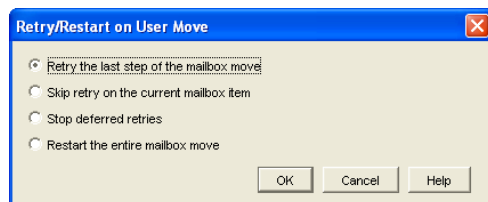
During the move, you might observe some of the following statuses:

- ♦ **Destination post office updated:** The destination POA has updated the destination post office database with the user's account information. At this point, the user account exists in the new location and appears in the Address Book with the new location information.
- ♦ **Source post office updated:** The source POA has updated the user in the source post office database to show the new destination post office. At this point, the user can no longer access the mailbox at the old location.
- ♦ **Moving mailbox information:** The POAs have finished exchanging administrative information and are ready to move items from the old mailbox to the new mailbox.
- ♦ **Sending mailbox inventory list:** The source POA sends the destination POA a list of all the mailbox items that it should expect to receive.
- ♦ **Send item request:** The destination POA starts requesting items from the source POA and the source POA responds to the requests
- ♦ **Retry mailbox item retrieval:** The destination POA was unable to retrieve an item and is retrying. The POA continues to retry every 12 hours for 7 days, then considers the move complete. To complete the move without waiting, click *Force Complete*. Typically, items that cannot be moved were not accessible to the user in the first place, so nothing is missed in the destination mailbox.
- ♦ **Completed retrieving items:** The destination POA has received all of the items on its mailbox inventory list.
- ♦ **Move completed:** After all of the user's mailbox items have arrived in the destination post office, the user's original account in the source post office is deleted and the user move is finished.



The User Move Status utility cannot gather status information for destination post offices that are running POAs older than GroupWise 6.5. Status information for users moving to older post offices displays as Unavailable.

- 5 If something disrupts the user move process, select the problem user or resource, then click *Retry/Restart*.



- 6 Select the option appropriate to the problem you are having, then click *OK*.

Retry the Last Step of the Mailbox Move: Select this option to retry whatever step the user move process has stopped on. This is equivalent to performing one of the POA's automatic retries manually and immediately. Ideally, the step completes successfully on the retry and processing continues normally.

Skip Retry on the Current Mailbox Item: Select this option to skip a particular mailbox item that cannot be successfully moved. The need for this action can usually be avoided by running Mailbox/Library Maintenance on the mailbox before moving the user account. Ideally, the user move processing should continue normally after skipping the problem item.

Stop Deferred Retries: Select this option to stop the POA from retrying to send items that have not been successfully received. This completes the user move process even though some individual items have not been moved successfully.

Restart the Entire Mailbox Move: Select this option if something major disrupts the user move process and you want to start over from the beginning. Because nothing is deleted from the source mailbox until everything has been received in the destination mailbox, you can safely restart a move at any time for any reason.

After you have moved a user in ConsoleOne, you can display detailed information about items belonging to that account that have not yet been moved to the destination post office, perhaps because problems were encountered when trying to move them. This information can help determine the importance of moving residual items that are still pending after all other items have been successfully moved.

- 7 Assess the importance of items that are still pending.

- 7a Select an account for which the move has not completed, then click *Pending Items*.

You can determine the record type (item, folder, Address Book contact, and so on), the item type (mail, appointment, task, and so on), how old the item is, the sender of the item, and the Subject line of the item. Not all columns in the Pending Items dialog box apply to all record types and item types, so some columns might be empty.

- 7b Click *Request* to request pending items.

Pending items are retrieved in groups of 25.

- 7c Click *Yes* to request the first group of pending items, then click *OK*.

You might need to wait for a while before the pending item lists displays because the request goes out through the destination domain to the source domain to the source post office, where the source POA sends the requested information back to the destination domain. Do not click *Request* again before the list appears or you receive the same list twice.

When the pending items appear, you can select an item, then click *Info* to display detailed information about the item. You can also click *Refresh* to reread the domain database to determine if additional items have been moved.

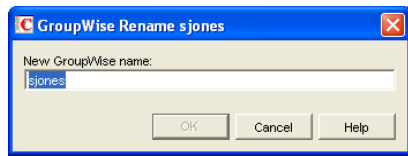
- 7d If you and the user whose mailbox is being moved decide that the pending items are expendable, click *Force Complete* to finish the move process.

14.5 Renaming Users and Their GroupWise Accounts

When you rename a user, the user's GroupWise user ID (mailbox ID) changes but the user remains in the same post office. All of the user's associations remain unchanged. For example, the user retains ownership of any resources and documents while other users who had proxy rights to the user's mailbox retain proxy rights.

- 1 Make sure the user has exited the GroupWise client and GroupWise Notify.
- 2 Make sure the domain's MTA and post office's POA are running.

- 3 In the GroupWise View, right-click the User object, then click *Rename* to display the GroupWise Rename dialog box.



- 4 Specify the GroupWise user ID.
- 5 Click *OK* to rename the user.

Resolving Addressing Issues Caused By Renaming a User

The user's new information is immediately replicated to each post office throughout your system so that the GroupWise Address Book contains the user's updated address. Any user who selects the renamed user from the GroupWise Address Book can successfully send messages to the renamed user.

However, some users might have the user's old address (GroupWise user ID) in their Frequent Contacts Address Books. In this case, if the sender types the renamed user's name in the To field instead of selecting it from the Address Book, GroupWise uses the old address stored in the Frequent Contacts Address Book instead of the new address in the GroupWise Address Book. This results in the message being undeliverable. The POA automatically resolves this issue when it performs its nightly user upkeep (see [Section 36.4.3, "Performing Nightly User Upkeep," on page 523](#)). During the nightly user upkeep process, the POA ensures that all addresses in a user's Frequent Contacts Address Book are valid addresses in the GroupWise Address Book.

If you want to ensure that messages sent to the user's old address are delivered even before the POA cleans up the Frequent Contacts Address Book, you can create a nickname using the old GroupWise user ID. For information about creating a nickname, see [Section 14.7.4, "Creating a Nickname for a User," on page 252](#).

14.6 Managing Mailbox Passwords

The following sections provide information to help you manage GroupWise mailbox passwords:

- ♦ [Section 14.6.1, "Creating or Changing a Mailbox Password," on page 243](#)
- ♦ [Section 14.6.2, "Removing a Mailbox Password," on page 245](#)
- ♦ [Section 14.6.3, "Bypassing the GroupWise Password," on page 246](#)

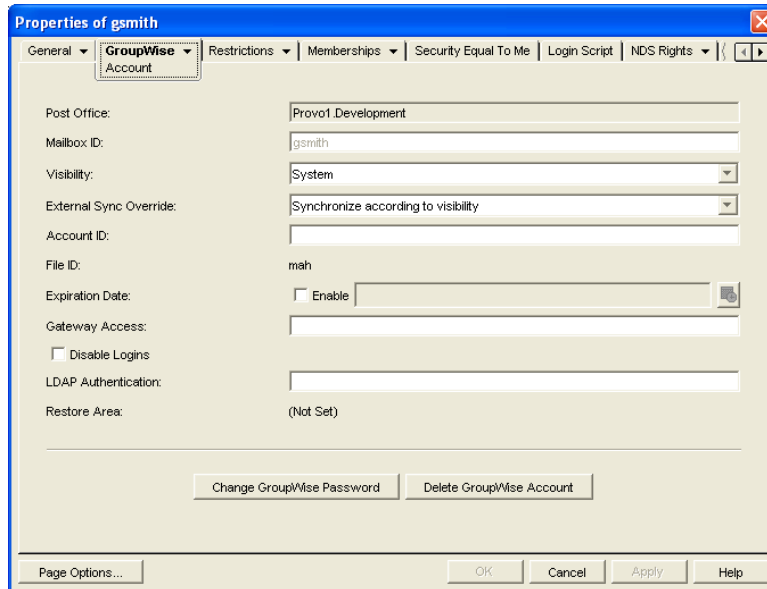
For background information about GroupWise passwords, see [Chapter 82, "GroupWise Passwords," on page 1099](#).

14.6.1 Creating or Changing a Mailbox Password

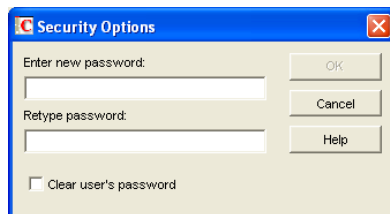
As administrator, you can use ConsoleOne to create a user's mailbox password or change a user's existing password. If a user can log in to GroupWise, he or she can also change the mailbox password through the Security Options dialog box (GroupWise Windows client > *Tools* > *Options* > *Security*) or on the Passwords page (GroupWise WebAccess > *Options* > *Password*).

To create or change a user's mailbox password:

- 1 In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page.



- 3 Click *Change GroupWise Password* to display the Security Options dialog box.

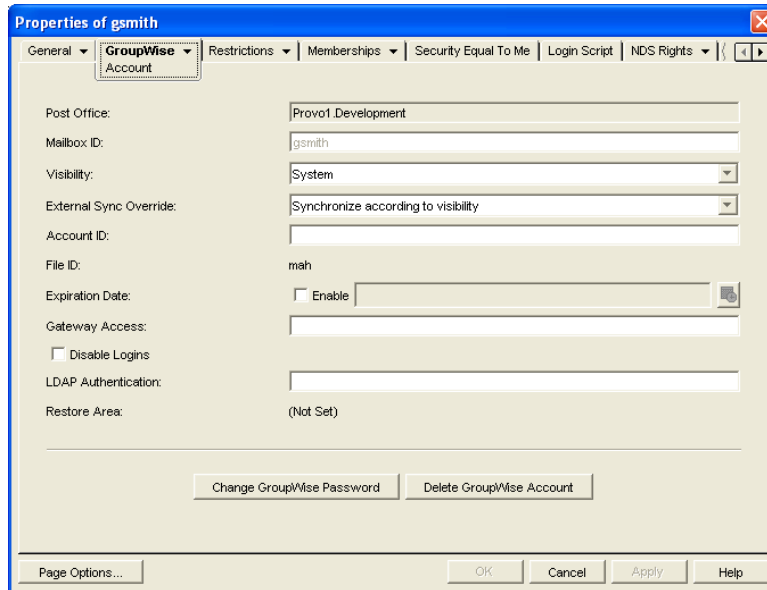


- 4 Enter and reenter a new password.
- 5 Click *OK*.

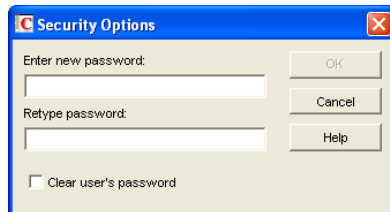
14.6.2 Removing a Mailbox Password

If you want to remove a user's mailbox password but not assign a new password, you can clear the password.

- 1 In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page.



- 3 Click *Change GroupWise Password* to display the Security Options dialog box.



- 4 Select the *Clear User's Password* option.
- 5 Click *OK*.

NOTE: A mailbox with no password cannot be accessed using GroupWise WebAccess.

14.6.3 Bypassing the GroupWise Password

By default, if a user must enter a password when logging in to GroupWise, he or she is prompted for the password.

The GroupWise client includes several options that users can choose from to enable them to log in without providing a password. These options, located on the Security Options dialog box (GroupWise client > *Tools* > *Options* > *Security*), are described in the following table:

GroupWise Client Option	Description
<i>No Password Required with eDirectory</i>	This option is available only when logged in to Novell eDirectory. When GroupWise starts, it automatically logs in to the GroupWise account associated with the user who is logged in to eDirectory at the workstation. No GroupWise password is required.
<i>Use Single Sign-On</i>	This option is available only when using Novell Single Sign-on 2.0 and SecureLogin 3.0 and later products. When GroupWise starts, it uses the GroupWise password stored by Novell Single Sign-on or SecureLogin.
<i>Use Collaboration Single Sign-On (CASA)</i>	This option is available only when using Novell Common Authentication Services Adapter (CASA) 1.0 and later. When GroupWise starts, it uses the GroupWise password stored by Novell CASA.

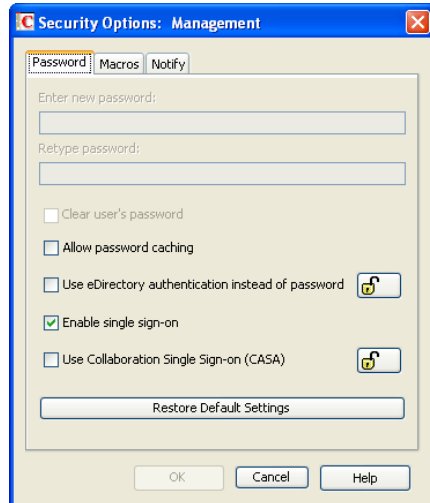
As shown in the table, these options appear only if certain conditions are met, such as the user having Novell Single Sign-on or SecureLogin installed. If you don't want the option to be available to users even if the condition is met, you can disable the option. Doing so removes it from the GroupWise client's Password dialog box.

To disable one or more of the password options:

- 1 In ConsoleOne, click a Domain object if you want to disable password options for all users in the domain.
or
Click a Post Office object if you want to disable password options for all users in the post office.
or
Click a User object or GroupWise External Entity object if you want to disable password options for the individual user.
- 2 With the appropriate GroupWise object selected, click *Tools* > *GroupWise Utilities* > *Client Options* to display the GroupWise Client Options dialog box.



- 3 Click *Security* to display the Security Options dialog box.



- 4 On the *Password* tab, select *Allow Password Caching* if you want Windows 95/98 users to be able to use the GroupWise client's *Remember My Password* option.

NOTE: This option applies only to older GroupWise clients running on older Windows versions, such as Windows 2000 and earlier, which are not supported for the GroupWise 2012 Windows client.

- 5 Select *Allow eDirectory Authentication Instead of Password* if you want eDirectory users to be able to use the GroupWise client's *No Password Required with eDirectory* option.
This option is available only if eDirectory authentication is enabled for the post office, as described in [Section 11.2.11, "Selecting a Post Office Security Level,"](#) on page 180.
- 6 Deselect *Allow Novell Single Sign-on* if you don't want Single Sign-on or SecureLogin users to be able to use the GroupWise client's *Use Novell Single Sign-on* option.
- 7 Select *Use Collaboration Single Sign-On (CASA)* if you want users of Novell collaboration products (GroupWise, Messenger, iFolder, and iPrint) to be able to use the same password for all collaboration products.
- 8 Click *OK* to save your changes.

For more information about addressing formats, see [Chapter 52, "Configuring Internet Addressing,"](#) on page 743.

14.7 Managing User Email Addresses

To ensure that user addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for users. The following sections provide details:

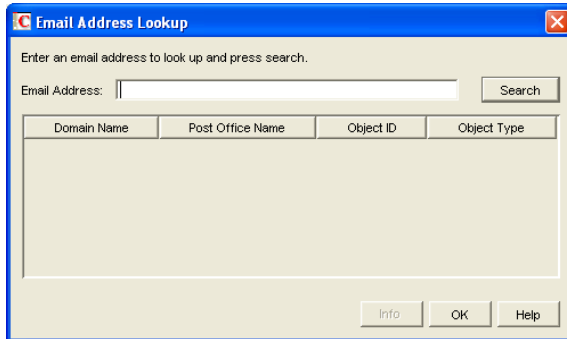
- ♦ [Section 14.7.1, "Ensuring Unique Email Addresses,"](#) on page 248
- ♦ [Section 14.7.2, "Changing a User's Internet Addressing Settings,"](#) on page 249
- ♦ [Section 14.7.3, "Changing a User's Visibility in the Address Book,"](#) on page 251
- ♦ [Section 14.7.4, "Creating a Nickname for a User,"](#) on page 252

14.7.1 Ensuring Unique Email Addresses

Starting with GroupWise 7, you can use the same email ID for more than one user in your GroupWise system, if each user is in a different Internet domain. Rather than requiring that each email ID be unique in your GroupWise system, each combination of email ID and Internet domain must be unique. This provides more flexibility for handling the situation where two people have the same name.

When adding or changing users' email addresses you can check to make sure that the email address you want to use for a particular user is not already in use.

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Email Address Lookup* to display the Email Address Lookup dialog box.



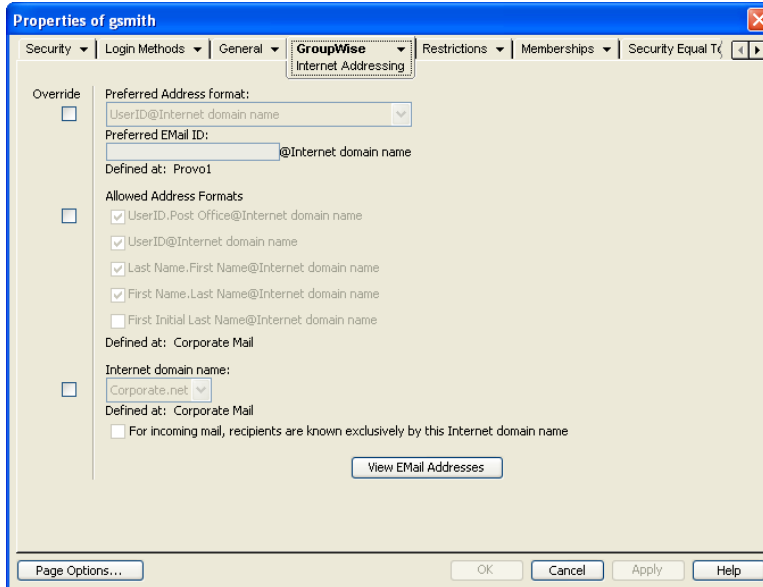
- 2 In the *Email Address* field, specify the email address. You can specify the user ID only (for example, jsmith) or the entire address (for example, jsmith@novell.com).
- 3 Click *Search*.
All objects whose email address match the one you specified are displayed.
- 4 If desired, select an object, then click *Info* to see details about the object.

14.7.2 Changing a User's Internet Addressing Settings

By default, a user inherits his or her Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from the user's post office, domain, or GroupWise system. For more information, see [Chapter 52, "Configuring Internet Addressing,"](#) on page 743.

If necessary, you can override these settings for individual users.

- 1 In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click *Properties*.
- 2 Click *GroupWise > Internet Addressing* to display the Internet Addressing page.



- 3 To override one of the settings, select the *Override* box, then change the setting.

Preferred Address Format: The preferred address format determines how the user's address is displayed in the GroupWise Address Book and in sent messages.

Preferred E-Mail ID: At the user and resource level, the preferred address format can be completely overridden by explicitly defining the user portion of the address format (*user@Internet domain name*). The user portion must include only RFC-compliant characters. The following characters are valid:

Numbers 0-9

Uppercase letters A-Z

Lowercase letters a-z

Plus sign +

Hyphen -

Underscore _

Tilde ~

The user portion must be unique within its Internet domain. This means that a user can be used multiple times in your GroupWise system, if it is used only once in each Internet domain.

If you have two users with the same name in the same Internet domain, you can further modify the user portion. For example, if you have selected *First Name.Last Name@Internet domain name* as your system's preferred address format and you have two John Petersons in the same Internet

domain, you would have two users with the same address (John.Peterson@novell.com). You could use this field to differentiate them by including their middle initials in their addresses (John.S.Peterson@novell.com and John.A.Peterson@novell.com).

Allowed Address Formats: The allowed address formats determine which address formats can be used to send messages to the user. For example, using John Peterson as the user, Research as the post office, and novell.com as the Internet domain, if you select all five formats, John Peterson would receive messages sent using any of the following addresses:

jpg Peterson.research@novell.com
jpg Peterson@novell.com
john.peterson@novell.com
peterson.john@novell.com
jpg Peterson@novell.com

Internet Domain Name: The Internet domain name, along with the preferred address format, is used when constructing the email address that is displayed in the GroupWise Address Book and in the To field of sent messages.

Only the Internet domain names that have been defined are displayed in the list. Internet domain names must be defined at the system level (*Tools > GroupWise System Operations > Internet Addressing*). For more information, see [Section 52, "Configuring Internet Addressing," on page 743](#).

If you override the Internet domain name, the *For Incoming Mail, Recipients are Known Exclusively by This Internet Domain Name* option becomes available. Enable this option if you only want the user to be able to receive messages addressed with this Internet domain name. If you don't enable this option, the user receives messages addressed using any of the Internet domain names assigned to your GroupWise system.

View E-Mail Addresses: Click *View E-Mail Addresses* to display a list of the various email address formats that can successfully deliver email to this user, including any nicknames or gateway aliases that have been defined for this user. For more information, see:

- ◆ [Section 52.1.4, "Preferred Address Format," on page 744](#) and [Section 52.1.5, "Allowed Address Formats," on page 747](#)
- ◆ [Section 14.7.4, "Creating a Nickname for a User," on page 252](#)
- ◆ [Section 52.3, "Transitioning from SMTP Gateway Aliases to Internet Addressing," on page 754](#)

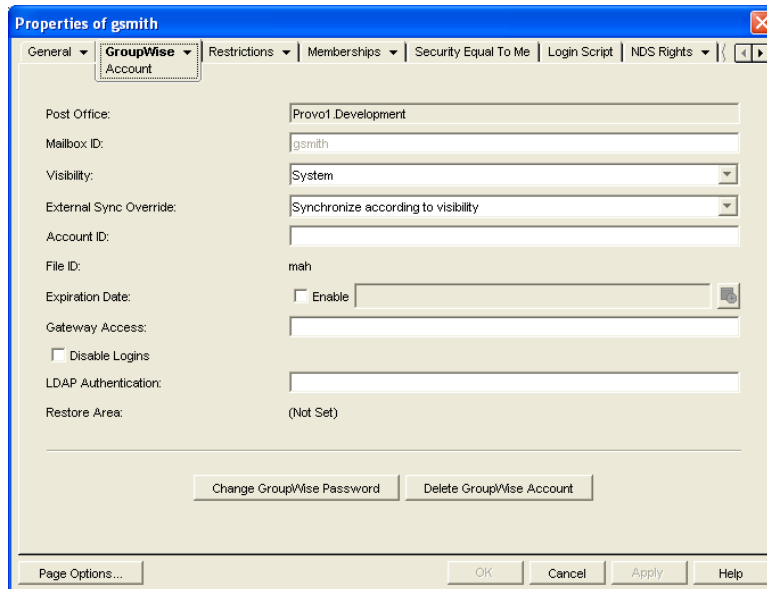
- 4 Click *OK* to save your changes.

14.7.3 Changing a User's Visibility in the Address Book

A user's visibility level determines the extent to which the user's address is visible throughout your GroupWise system. You can make the user visible in the Address Book throughout your entire GroupWise system, you can limit visibility to the user's domain or post office only, or you can make it so that no users can see the user in the Address Book.

Making a user visible in the Address Book simply makes it easier to address items to the user. Regardless of a user's visibility, other users can send items to the user if they know the user's GroupWise user ID.

- 1 In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page.



The screenshot shows the 'Properties of gsmith' dialog box with the 'GroupWise Account' tab selected. The 'Visibility' dropdown menu is set to 'System'. Other fields include Post Office (Provo1.Development), Mailbox ID (gsmith), External Sync Override (Synchronize according to visibility), File ID (mah), and Restore Area ((Not Set)). Buttons for 'Change GroupWise Password' and 'Delete GroupWise Account' are visible at the bottom.

- 3 In the *Visibility* field, select the desired visibility level.

System (Default): All users in your GroupWise system can see the user's information in the Address Book.

Domain: Only users in the same domain as the user can see the user's information in the Address Book.

Post Office: Only users in the same post office as the user can see the user's information in the Address Book.

None: No users can see the user's information in the Address Book. Users need to know the user's GroupWise user ID to send items to him or her.

- 4 Click *OK* to save your changes.

14.7.4 Creating a Nickname for a User

Each user has a GroupWise address consisting of the user ID, post office, and domain (*user_ID.post_office.domain*). You can create one or more nicknames for a user to give the user an additional GroupWise address. Each part of the GroupWise address (*user_ID*, *post_office*, and *domain*) can be different from the user's actual address. Adjustments to the user's GroupWise address are also applied to the user's Internet email address (*user_ID@internet_domain*).

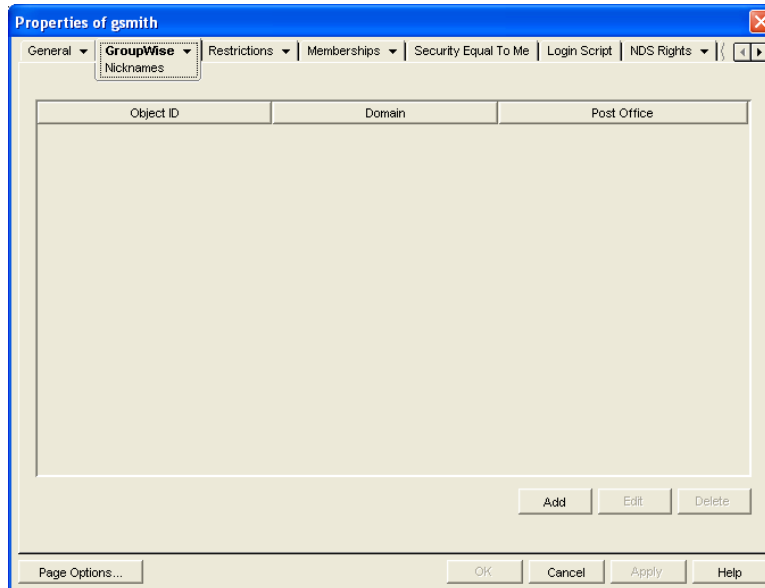
Nicknames are useful in the following situations:

- You rename a user, as described in [Section 14.5, "Renaming Users and Their GroupWise Accounts," on page 242](#). You can create a nickname that retains the old user ID, so that messages with the old user ID in the email address are routed to the new email address.
- You move a user, as described in [Section 14.4, "Moving GroupWise Accounts," on page 234](#). You can create a nickname that retains the old post office location. As messages to the moved user arrive in your GroupWise system, the email address is routed to the new post office location. You can configure ConsoleOne to automatically create nicknames when you move users, as described in [Section 4.2.4, "Nickname Settings," on page 75](#).
- You need to restrict a user's visibility in the GroupWise Address Book, as described in [Section 6.2, "Controlling Object Visibility," on page 110](#), and at the same time, you need to make the user visible in one or more specific Address Books outside of the restricted visibility. You can create a nickname that provides the specific visibility that is ruled out by the required restriction.

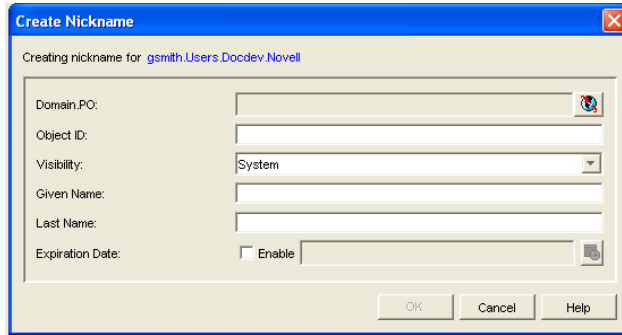
In ConsoleOne, you can list all the nicknames in your GroupWise system in the GroupWise View. In the GroupWise client, you can display nicknames in the GroupWise Address Book if you enable *Filter for Contacts*. When addressing a message, users need to know a nickname in order to use it.

To create a nickname for a user:

- 1 In ConsoleOne, right-click the User object or GroupWise External Entity object, then click *Properties*.
- 2 Click *GroupWise > Nicknames* to display the Nicknames page.



- 3 Click *Add* to display the Create Nickname dialog box.



- 4 Fill in the following fields:

Domain.PO: Select the post office that you want to own the nickname. This can be any post office in your GroupWise system; it does not need to be the user's post office.

Object ID: Specify the name to use as the *user_ID* portion of the nickname. The nickname must be unique.

Visibility: Select the Address Book visibility for the nickname. This determines where the nickname is available (system, domain, or post office). However, nicknames are not displayed in the Address Book unless you filter for them. In order to address a message to a nickname, a user must specify the nickname address, and the nickname must be available in the user's post office.

External Sync Override: This option applies only if your GroupWise system links to and synchronizes with an external GroupWise system, as described in "[Connecting to Other GroupWise Systems](#)" in the *GroupWise 2012 Multi-System Administration Guide*.

- ♦ **Synchronize According to Visibility:** The nickname is synchronized to external GroupWise systems only if Address Book visibility is set to *System*.
- ♦ **Synchronize Regardless of Visibility:** The nickname is synchronized to external GroupWise systems regardless of Address Book visibility.
- ♦ **Don't Synchronize Regardless of Visibility** The nickname is never synchronized to external systems.

Given Name: Specify the user's first name.

Last Name: Specify the user's last name.

Expiration Date: If you want the nickname to be removed by the Expire Records feature after a certain date, as described in [Section 14.11.3, "Managing Expired or Expiring GroupWise Accounts,"](#) on page 258, select *Enable*, then select the desired date.

- 5 Click *OK* to add the nickname to the list.
- 6 Click *OK* to save the changes to the User object or GroupWise External Entity object.

14.8 Checking GroupWise Account Usage

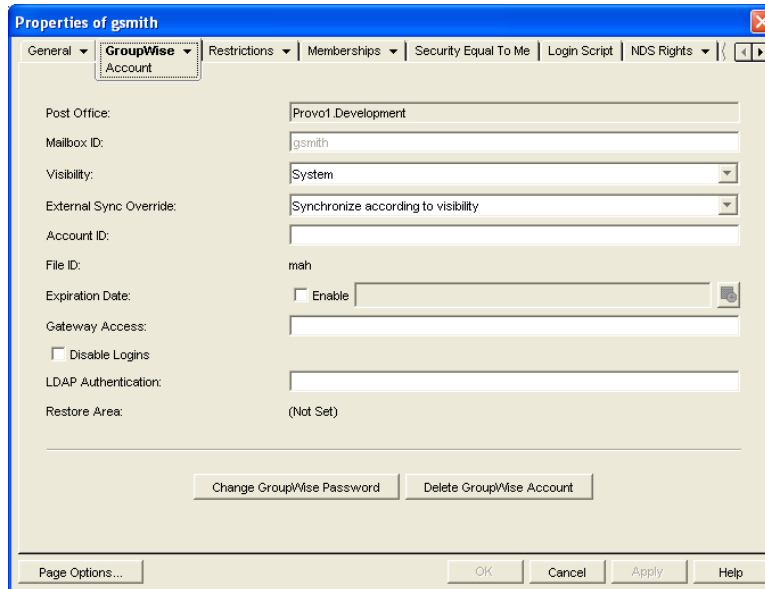
You can identify GroupWise accounts that have been inactive for a specified period of time. See [Section 12.4, "Auditing Mailbox License Usage in the Post Office,"](#) on page 207.

You can measure message traffic from individual GroupWise mailboxes. See [Section 71.3.5, "User Traffic Report,"](#) on page 986.

14.9 Disabling and Enabling GroupWise Accounts

You can disable a GroupWise account so that the user cannot access his or her mailbox until you enable the account again. This might be necessary when a user leaves the company and no longer needs access to the mailbox.

- 1 In ConsoleOne, right-click the User object (or GroupWise External Entity object), then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page.



- 3 Select *Disable Logins*, then click *OK*.
- 4 (Conditional) If the user is logged in to his or her Online mailbox when you disable logins, disconnect the user, as described in [“Disconnecting a User Session from the POA” on page 551](#).
- 5 To enable the user’s account when access is again permitted, deselect *Disable Logins*, then click *OK*.

While a user’s account is disabled, other users to whom proxy rights have been granted can still access the mailbox. This is convenient for reviewing the contents of the mailbox of a departed employee and pulling out those messages that are of use to the incoming employee.

14.10 Unlocking GroupWise Accounts

A GroupWise user’s account is automatically disabled (locked) if you have enabled intruder detection, as described in [Section 36.3.5, “Enabling Intruder Detection,” on page 516](#), and if the user exceeds the number of unsuccessful login attempts that you have allowed. When a user is locked out, access is automatically granted again after the incorrect login reset time interval has passed. If a user needs quicker access, you can unlock the GroupWise account in ConsoleOne or in the POA Web console.

In ConsoleOne:

- 1 Right-click the User object (or GroupWise External Entity object), then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page.
- 3 Deselect *Disable Logins*, then click *OK*.

In the POA Web console:

- 1 Click *Status*.
- 2 In the *Statistics* section, click *Intruder Detection*.
- 3 Click the user ID of the locked out user.
- 4 Select *Reset Lockout*, then click *Submit*.

As soon as the POA receives the changed setting, the user can again log in.

14.11 Removing GroupWise Accounts

You can remove a user's GroupWise account by deleting or expiring it. Deleting an account removes the entire account (address, mailbox, items, and so on) from the GroupWise system. Expiring an account deactivates the account so that it cannot be accessed, but does not remove it from the system. The following sections provide information to help you delete or expire GroupWise accounts

- ♦ [Section 14.11.1, "Deleting a GroupWise Account," on page 255](#)
- ♦ [Section 14.11.2, "Expiring a GroupWise Account," on page 257](#)
- ♦ [Section 14.11.3, "Managing Expired or Expiring GroupWise Accounts," on page 258](#)

If you delete a GroupWise account by accident, or need to retrieve a deleted account for some other reason, see [Section 32.6, "Recovering Deleted GroupWise Accounts," on page 438](#). For additional user repair options, see [Section 5.15, "GW / eDirectory Association," on page 99](#).

NOTE: When you remove a GroupWise account, any personal databases, such as an archive, a Caching mailbox, or a Remote mailbox, that are associated with the account are unaffected by the account deletion. Such databases are not located where ConsoleOne could delete them, so they must be deleted manually.

14.11.1 Deleting a GroupWise Account

When you delete a user's GroupWise account, the user's mailbox is deleted and the user is removed from the GroupWise system. If the user owns library documents, see ["Ensuring that a User's Library Documents Remain Accessible" on page 257](#) before deleting the user. Otherwise, refer to one of the following sections:

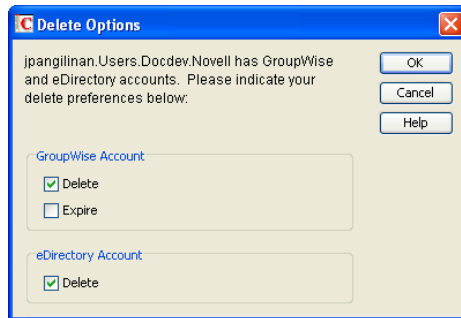
- ♦ ["Deleting an eDirectory User's GroupWise Account" on page 255](#)
- ♦ ["Deleting a Non-eDirectory User's GroupWise Account" on page 256](#)

Deleting an eDirectory User's GroupWise Account

- 1 Make sure the user has exited the GroupWise client and GroupWise Notify.
- 2 Make sure the POA for the user's post office is running.

If the POA is not running, the user mailbox is not deleted until the next time the POA runs.

- 3 In ConsoleOne, right-click the User object, then click *Delete*.
or
Select multiple User objects, right-click the selected object, then click *Delete*.
- 4 Click *Yes* to display the Delete Options dialog box.

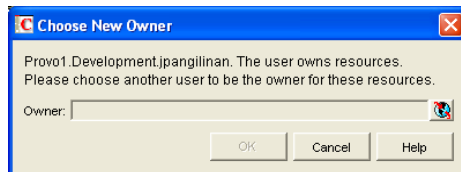


- 5 In the *GroupWise Account* box, select *Delete*.
- 6 In the *eDirectory Account* box, deselect *Delete*.
- 7 Click *OK* to delete the eDirectory user's GroupWise account.

or

If you selected multiple User objects, click *OK to All* to apply the same deletion options to all accounts. If you click *OK* rather than *OK to All*, you can select deletion options for each account individually as it is deleted.

- 8 If a user was a resource owner, the following dialog box appears. Select a new user to be the resource's owner, then click *OK*.



Deleting a Non-eDirectory User's GroupWise Account

Non-eDirectory users are given GroupWise accounts by adding the users to eDirectory as GroupWise external entities (see [Section 13.3, "Creating GroupWise Accounts for Non-eDirectory Users," on page 224](#)). You remove a non-eDirectory user's GroupWise account by deleting the user's GroupWise External Entity object from eDirectory.

NOTE: Remember that external entities do have eDirectory objects, but they are not considered eDirectory users for licensing purposes.

As with eDirectory users, when you remove a non-eDirectory user's GroupWise account, the user's mailbox is deleted and the user is removed from the GroupWise system.

To delete a non-eDirectory user's GroupWise account:

- 1 Make sure the user has exited the GroupWise client and GroupWise Notify.
- 2 Make sure the POA for the user's post office is running.
If the POA is not running, the user's mailbox will not be deleted until the next time the POA runs.

- 3 In ConsoleOne, right-click the user's GroupWise External Entity object, then click *Delete*.
- 4 Click *Yes* to confirm the deletion.

Ensuring that a User's Library Documents Remain Accessible

When you delete a user's GroupWise account, GroupWise does not delete any library documents to which the user has Author or Creator status. These documents remain in the library as "orphaned" documents, meaning that no one can access the documents.

If you or other users need access to the documents, you have the following choices:

- ♦ Rather than deleting the user, change the user's GroupWise mailbox password so that he or she can't log in. Other users can continue accessing the documents, and you can log in as the user to manage the documents. For information about changing a user's password, see [Section 14.6.1, "Creating or Changing a Mailbox Password,"](#) on page 243.
- ♦ Rather than deleting the user or changing the user's password, disable the user's ability to log in. This is done on the user's GroupWise Account page (User object > GroupWise > Accounts > Disable Logins).
- ♦ Delete the user, then reassign the orphaned documents to another user. For information, see [Section 28.2, "Analyzing and Fixing Library and Document Information,"](#) on page 416.

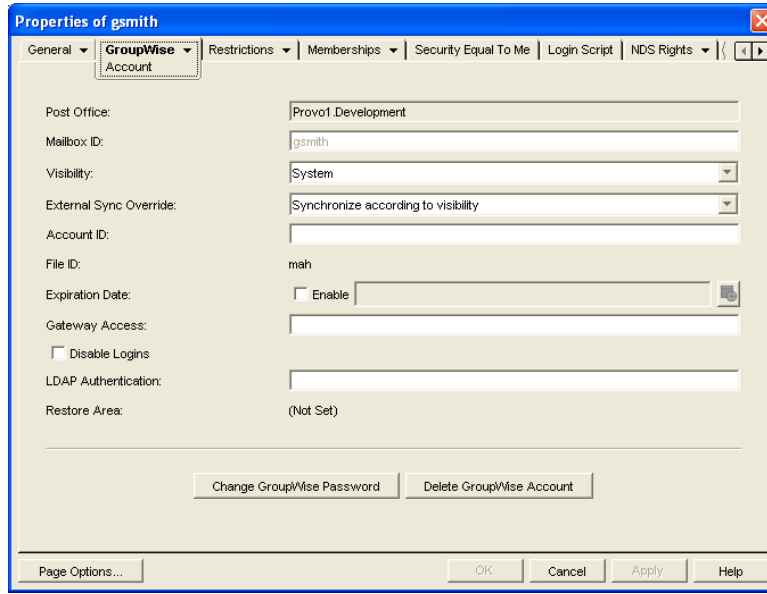
14.11.2 Expiring a GroupWise Account

Rather than delete a user's GroupWise account, you can expire the account. The account, including the user's mailbox and all items, remains in GroupWise but cannot be accessed by the user. If necessary, the user's account can be reactivated at a later date, as described in [Section 14.11.3, "Managing Expired or Expiring GroupWise Accounts,"](#) on page 258. This option is useful for providing GroupWise accounts to temporary or contract employees who come and go.

You can set a user's GroupWise account to expire immediately or at a future date and time.

- 1 Make sure the user has exited the GroupWise client and GroupWise Notify.
- 2 In ConsoleOne, right-click the User object or GroupWise External Entity object with the account you want to expire, then click *Properties*.

3 Click *GroupWise > Account* to display the Account page.



4 In the *Expiration Date* field, select the *Enable* check box to turn on the option.

5 If you want the account to expire immediately, leave the date and time set to the current date and time.

or

If you want the account to expire at a later date, select the desired date and time.

6 Click *OK*.

NOTE: To immediately expire an account assigned to an eDirectory user, you can also right-click the User object, click *Delete*, select the *Expire GroupWise Account* option, then click *OK*. This method is not available for non-eDirectory (GroupWise External Entity object) users.

14.11.3 Managing Expired or Expiring GroupWise Accounts

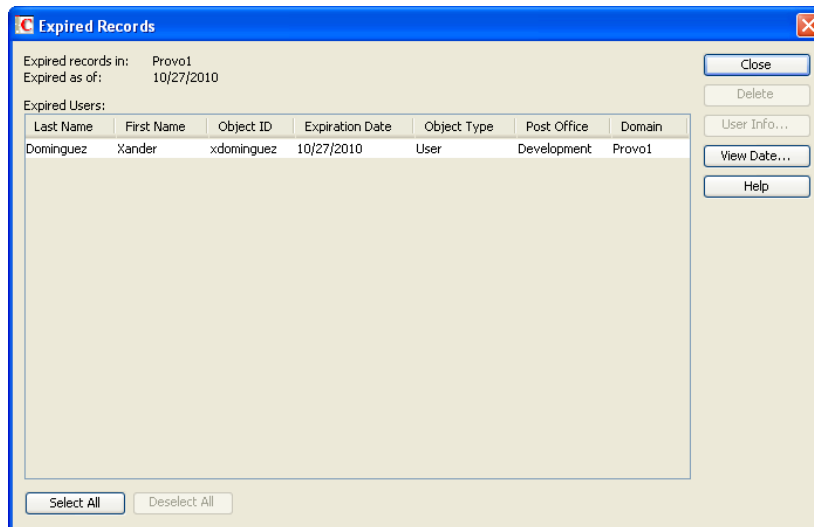
Expired GroupWise accounts remain expired until you reactivate them or delete them. Refer to the following sections for information to help you manage expired accounts:

- ♦ [“Identifying Expired or Expiring Accounts” on page 259](#)
- ♦ [“Changing an Account’s Expiration Date” on page 260](#)
- ♦ [“Reactivating an Expired Account” on page 260](#)

Identifying Expired or Expiring Accounts

Rather than search through all your User or GroupWise External Entity objects in eDirectory to identify which ones have expired or expiring accounts, you can use the Expired Records option to quickly list expired accounts for your entire system, a single domain, or a single post office. Depending on the date you choose, you can see expired accounts only or both expired and expiring accounts.

- 1 In the GroupWise View, select the post office, domain, or GroupWise system that contains the accounts you want to view.
- 2 Click *Tools > GroupWise Utilities > Expired Records* to display the Expired Records dialog box.

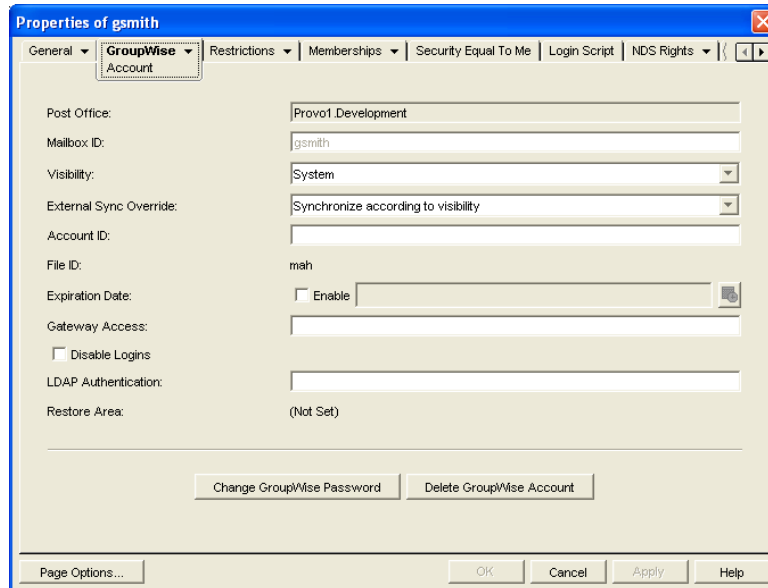


The *Expired As Of* field defaults to the current date. Only accounts that have expired as of this date are displayed in the list. To see accounts that will expire in the future, you need to change the date in the *Expired As Of* field.

- 3 To change the date in the *Expired As Of* field, click *View Date*.
- 4 Click the calendar icon, select the desired date and time, then click *OK*.
For example, in the dialog box shown above, the current date is 1/18/2012 (January 1, 2012). To see what accounts will expire by June 30, 2012, you would change the *Expired As Of* date to 6/30/2012.
- 5 Click *OK* to return to the Expired Records page.
- 6 When you are finished viewing expired or expiring accounts, click *OK* to close the Expired Accounts dialog box.

Changing an Account's Expiration Date

- 1 In ConsoleOne, right-click the User object or GroupWise External Entity object, then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page.

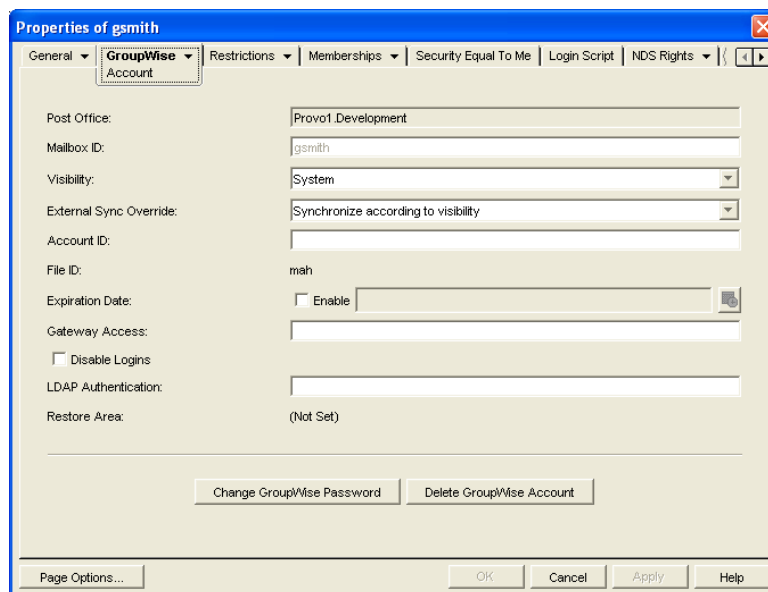


The screenshot shows the 'Properties of gsmith' dialog box with the 'GroupWise Account' tab selected. The 'Expiration Date' field is highlighted, showing a date picker icon. The 'Post Office' is 'Provo1.Development', 'Mailbox ID' is 'gsmith', 'Visibility' is 'System', and 'External Sync Override' is 'Synchronize according to visibility'. The 'File ID' is 'mah'. There are buttons for 'Change GroupWise Password' and 'Delete GroupWise Account' at the bottom.

- 3 In the *Expiration Date* field, change the time and date.
- 4 Click *OK*.

Reactivating an Expired Account

- 1 In ConsoleOne, right-click the User object or GroupWise External Entity object with the expired GroupWise account, then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page.



This screenshot is identical to the one above, showing the 'Properties of gsmith' dialog box with the 'GroupWise Account' tab selected. The 'Expiration Date' field is highlighted, showing a date picker icon. The 'Post Office' is 'Provo1.Development', 'Mailbox ID' is 'gsmith', 'Visibility' is 'System', and 'External Sync Override' is 'Synchronize according to visibility'. The 'File ID' is 'mah'. There are buttons for 'Change GroupWise Password' and 'Delete GroupWise Account' at the bottom.

- 3 In the *Expiration Date* field, deselect the *Enable* check box to turn off the option.
- 4 Click *OK*.

V Resources

- ♦ [Chapter 15, “Creating Resources,” on page 265](#)
- ♦ [Chapter 16, “Managing Resources,” on page 269](#)

15 Creating Resources

A resource is an item or place, such as a computer, company vehicle, or conference room, that users can schedule or check out.

- ♦ [Section 15.1, “Understanding Resources,” on page 265](#)
- ♦ [Section 15.2, “Planning Resources,” on page 266](#)
- ♦ [Section 15.3, “Creating a New Resource,” on page 267](#)

15.1 Understanding Resources

The following sections provide information to help you learn about GroupWise resources:

- ♦ [Section 15.1.1, “Resource Objects,” on page 265](#)
- ♦ [Section 15.1.2, “Resource Types,” on page 265](#)
- ♦ [Section 15.1.3, “Resource Mailboxes,” on page 266](#)
- ♦ [Section 15.1.4, “Resource Owners,” on page 266](#)

15.1.1 Resource Objects

Each resource you want to make available must be added as a Resource object in Novell eDirectory. The name that you give the Resource object becomes the name by which the resource is displayed in the GroupWise Address Book.

Resource objects () can be located in any eDirectory container that is in the same tree as the resource’s domain.

15.1.2 Resource Types

You can identify the resource as a general resource, as a place, or as a role.

When a user schedules a resource that is defined as a place, the resource name is automatically added to the *Place* field in the appointment.

Starting in GroupWise 2012 SP2, a role resource represents a position in an organization that can be reassigned from one owner to the next. As owners change, the role resource mailbox retains all information associated with the role. Unlike general resources and place resources, role resources are included in a Reply to All.

15.1.3 Resource Mailboxes

Like a user, a resource must be assigned to a post office so that it can be given an account (address, mailbox, and so on). You assign the resource to a post office when you create the Resource object.

A resource's account enables it to receive scheduling requests (sent as appointments). The owner assigned to the resource can access the resource's mailbox to accept or decline the requests. For example, you might want to have all your conference rooms defined as place resources. When sending a meeting appointment, users can schedule the conference room as well as the meeting attendees. The place resource, just like the other users scheduled for the meeting, receives an appointment in its mailbox which can be accepted or declined by the owner.

When scheduling a resource, users can perform a busy search to see when the resource is available.

Even though a resource is assigned to a single post office, all users in your GroupWise system can schedule the resource.

Resources can receive all item types (mail messages, phone messages, appointments, tasks, and notes). Generally, if your purpose in defining resources is to allow them to be scheduled through GroupWise, they only receive appointments.

Resources can also send items. If a resource sends an item to an Internet user, both the *To* field and the *From* field are populated with the resource name when the Internet user receives the message.

15.1.4 Resource Owners

When you create a resource, you assign an owner to it. The owner must belong to the same post office as the resource and is responsible for accepting or declining requests to schedule the resource. The owner can do this by proxying to the resource's mailbox and opening the scheduling requests, or by setting up rules to manage the resource automatically. For more information, see [Section 16.1, "Creating Rules for a Resource,"](#) on page 269.

The owner automatically receives proxy rights to the resource's mailbox. The owner can also grant proxy rights to another user to manage the resources.

The owner cannot log in directly to the resource mailbox. However, the owner can set a password on the resource mailbox to facilitate secure access by an IMAP client. After proxying in to the resource mailbox, click *Tools > Options > Security > Password* to set a password on the resource mailbox.

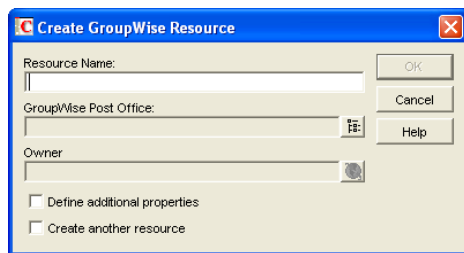
For more information about how owners can manage resources, see "[Managing Resources](#)" in "[Contacts and Address Books](#)" in the *GroupWise 2012 Windows Client User Guide*.

15.2 Planning Resources

Before creating a new resource, make sure that the user who will own the resource has been created and belongs to the same post office where you are planning to create the resource.

15.3 Creating a New Resource

- 1 In ConsoleOne, right-click the container where you want to create the Resource object, then click *New > Resource* to display the Create GroupWise Resource dialog box.



- 2 Fill in the following fields:

Resource Name: Specify a descriptive name. Because the name is used as part of the resource's GroupWise email address, do not use any of the following invalid characters in the resource name:

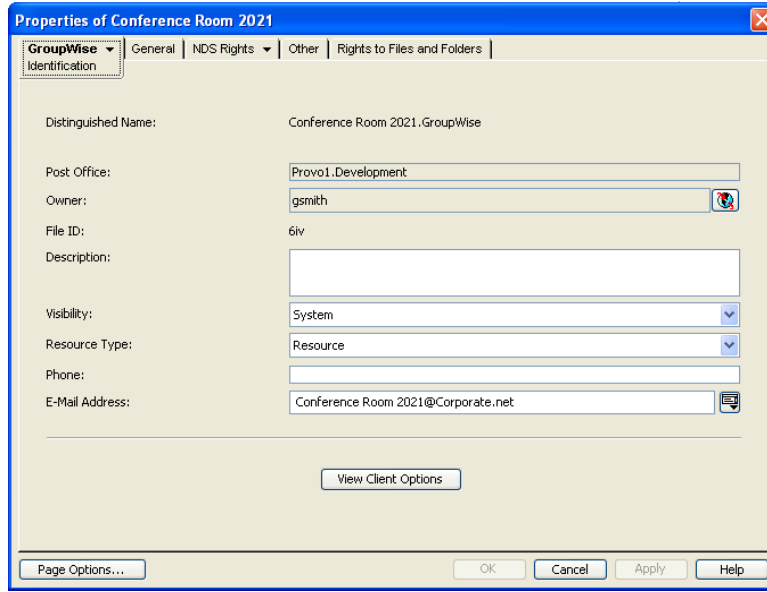
ASCII characters 0-31	Comma ,
Asterisk *	Double quote "
At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

IMPORTANT: Characters that are valid and even desirable in a resource name, such as accented characters, might not be valid in an email address. For some resources, you might need to set up a preferred email ID in order to ensure that they have a valid email address. For instructions, see [Section 16.7.1, "Changing a Resource's Internet Addressing Settings,"](#) on page 274.

GroupWise Post Office: Select the post office where the resource will be located.

Owner: Select the user who will be responsible for accepting or declining requests to use the resource. The owner must have a GroupWise account on the same post office as the resource.

- 3 Select *Define Additional Properties*, then click *OK*.



The screenshot shows the 'Properties of Conference Room 2021' dialog box with the 'Identification' tab selected. The fields are as follows:

Distinguished Name:	Conference Room 2021.GroupWise
Post Office:	Provo1.Development
Owner:	gsmith
File ID:	6iv
Description:	
Visibility:	System
Resource Type:	Resource
Phone:	
E-Mail Address:	Conference Room 2021@Corporate.net

Buttons at the bottom: Page Options..., View Client Options, OK, Cancel, Apply, Help.

- 4 On the Identification page, fill in the following fields:

Description: Specify a description to help users identify the use of the resource. The description is displayed if the user chooses to view information about the resource in the Address Book.

If you define the resource type as a place, the description is automatically added to the *Place* field in the appointment. A good description can help users locate the place more easily.

Visibility: Select the level at which the resource will be visible in the Address Book. *System* causes the resource to be visible to all users in your GroupWise system. *Domain* causes the resource to be visible to all users in the same domain as the resource. *Post Office* causes the resource to be visible to all users on the same post office as the resource. *None* causes the resource to not be visible at any level. However, even if the resource is not displayed in a user's Address Book, he or she can schedule the resource by typing the resource name in an appointment's *To* field.

Resource Type: You can identify the resource as a general resource, as a place, or as a role. When a user schedules a place resource, the resource description is automatically added to the *Place* field in the appointment. A role resource is treated more like a user than a general resource or a place resource, and can be included in a Reply to All.

Phone: If the resource has a telephone number associated with it, such as a conference room with a telephone number, specify the phone number.

E-Mail Address: Displays the default email address for the resource. Click the drop-down list to specify a custom email address. For example, if you created a resource with spaces in its name, you need to remove the spaces to create a valid email address.

View Client Options: Click *View Client Options* as a convenient shortcut for *Tools > GroupWise Utilities > Client Options* in order to modify client options for the currently selected resource. For more information, see [Chapter 76, "Setting Defaults for the GroupWise Client Options," on page 1025](#).

- 5 Click *OK* to save the resource information.
- 6 Skip to [Section 16.1, "Creating Rules for a Resource," on page 269](#).

16 Managing Resources

The following sections provide information to help you manage the resources in your GroupWise system:

- ♦ [Section 16.1, “Creating Rules for a Resource,” on page 269](#)
- ♦ [Section 16.2, “Changing a Resource’s Owner,” on page 271](#)
- ♦ [Section 16.3, “Adding a Resource to a Distribution List,” on page 272](#)
- ♦ [Section 16.4, “Moving a Resource,” on page 273](#)
- ♦ [Section 16.5, “Renaming a Resource,” on page 273](#)
- ♦ [Section 16.6, “Deleting a Resource,” on page 274](#)
- ♦ [Section 16.7, “Managing Resource Email Addresses,” on page 274](#)

A resource’s mailbox, just like a user’s mailbox, is a combination of the information stored in its user database and the message databases located at its post office. Occasionally, you might want to perform maintenance tasks on the resource’s mailbox to ensure the integrity of the databases. For details about performing maintenance on a resource’s mailbox, see [Chapter 27, “Maintaining User/Resource and Message Databases,” on page 409](#).

16.1 Creating Rules for a Resource

Schedulable resources such as conference rooms need effective auto-accept/decline rules to help compensate for times when appointment schedulers fail to use Busy Search.

If you are the resource owner, you can proxy to the resource mailbox in order to set up the rules. If you are not the resource owner, be sure that the resource owner understands how to set up effective rules for the resource.

- ♦ [Section 16.1.1, “Creating an Auto-Accept Rule,” on page 269](#)
- ♦ [Section 16.1.2, “Creating an Auto-Delay Rule,” on page 270](#)

16.1.1 Creating an Auto-Accept Rule

Creating an auto-accept rule provides confirmation to the appointment scheduler that the resource as accepted the appointment.

- 1 In the GroupWise Windows client, in the resource mailbox, click *Tools > Rules*, then click *New*.
- 2 Type a name for the auto-accept rule.
- 3 Select *Received*.
- 4 Select *Appointment*.
- 5 In the *Appointment conflict exists* drop-down list, select *No*.

- 6 Create an action to accept the appointment:
 - 6a Click *Add Action*.
 - 6b Click *Accept*.
 - 6c Select a *Show As* setting.
 - 6d (Optional) Type a comment to include with the acceptance.
 - 6e Click *OK*.
- 7 Create an action to notify the appointment scheduler that the resource has accepted the appointment:
 - 7a Click *Add Action*.
 - 7b Click *Reply*.
 - 7c Click *OK* to accept the default of replying only to the appointment scheduler.
 - 7d In the *Subject* field, indicate that the resource has accepted the appointment.
 - 7e (Optional) In the *Message* field, provide any additional information that might be helpful to the appointment scheduler.
 - 7f Click *OK*.
- 8 Test the rule by scheduling an appointment that includes the resource for a time when the resource is available.
- 9 Continue with [Creating an Auto-Delay Rule](#).

16.1.2 Creating an Auto-Delay Rule

Creating an auto-delay rule notifies the appointment scheduler that the resource is not available. By notifying users in addition to the appointment scheduler, the likelihood of a perceived double-booking of the resource is minimized.

- 1 In the GroupWise Windows client, in the resource mailbox, click *Tools > Rules*, then click *New*.
- 2 Type a name for the auto-delay rule.
- 3 Select *Received*.
- 4 Select *Appointment*.
- 5 In the *Appointment conflict exists* drop-down list, select *Yes*.
- 6 Create an action to decline the appointment:
 - 6a Click *Add Action*.
 - 6b Click *Delete/Decline*.
 - 6c (Optional) Type a comment about the resource declining the appointment.
 - 6d Click *OK*.
- 7 Create an action to notify the appointment scheduler that the resource has declined the appointment:
 - 7a Click *Add Action*.
 - 7b Click *Reply*.
 - 7c Click *OK* to accept the default of replying only to the appointment scheduler.

or

Select *Reply to all (sender and recipients)* to make sure that everyone involved with the appointment is notified that the resource has declined the appointment.

- 7d In the *Subject* field, indicate that the resource has declined the appointment.
 - 7e (Optional) In the *Message* field, provide any additional information that might be helpful to the appointment scheduler.
 - 7f (Optional) In the *CC* field or the *BC* field, include one or more additional users such as the resource owner to notify when a resource declines an appointment.
 - 7g Click *OK*.
- 8 Test the rule by scheduling an appointment that includes the resource for a time when the resource is not available.

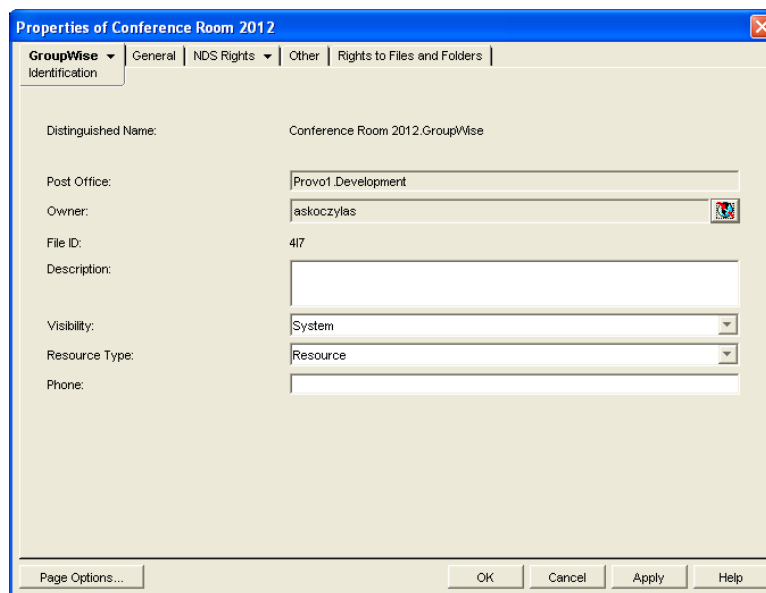
16.2 Changing a Resource's Owner

You can change a resource's owner whenever necessary. The owner must be a user assigned to the same post office as the resource. If you need to give ownership of the resource to a user on a different post office, you must move the resource to that post office. For details, see [Section 16.4, "Moving a Resource," on page 273](#).

The new owner automatically receives proxy rights to the resource's mailbox. Proxy rights are removed for the old owner.

Make sure that the new resource owner understands the auto-accept/decline rules that are associated with the resource.

- 1 In ConsoleOne, right-click the Resource object, then click *Properties*.
- 2 On the Identification page, browse to and select the new owner, then click *OK* to display the user's name in the *Owner* field.

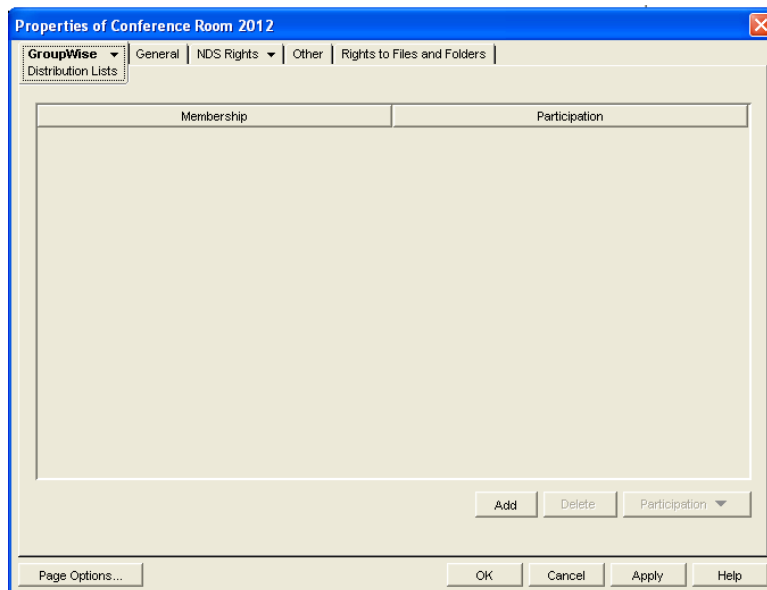


- 3 Click *OK* to save your changes.

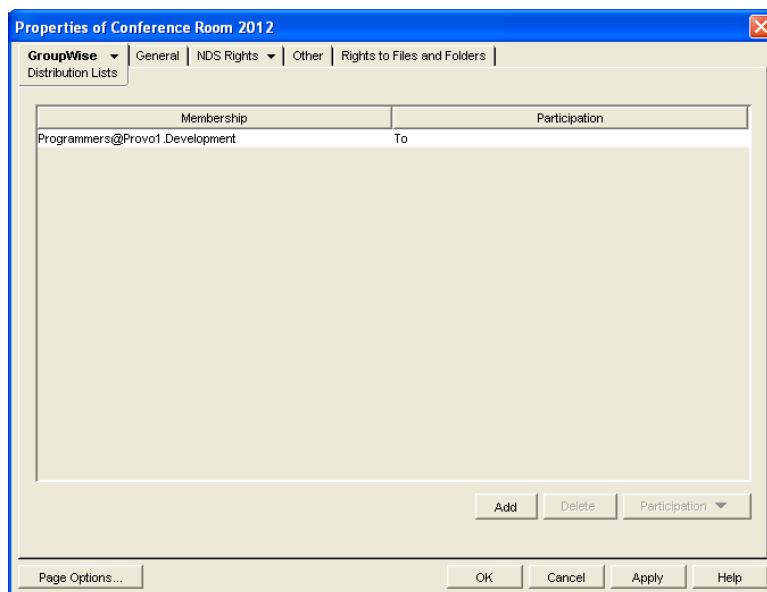
16.3 Adding a Resource to a Distribution List

Just like users, resources can be added to distribution lists.

- 1 In ConsoleOne, right-click the Resource object, then click *Properties*.
- 2 Click *GroupWise > Distribution Lists* to display the Distribution Lists page.



- 3 Click *Add*, select the distribution list that you want to add the resource to, then click *OK*.



By default, the resource is added as a primary recipient (*To* recipient).

- 4 If you want to change the resource's recipient type, select the distribution list, click *Participation*, then click *To*, *CC*, or *BC*.
- 5 Click *OK* to save your changes.

16.4 Moving a Resource

If necessary, you can move a resource from one post office to another. For example, you might need to move a resource if you are removing the resource's post office or if you need to reassign ownership of the resource to a user on another post office.

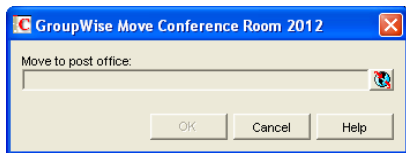
The resource retains the same name in the new post office as it has in the current post office. If another user, resource, or distribution list assigned to the new post office has the same name, you must rename one of them before you move the resource. For details, see [Section 16.5, "Renaming a Resource," on page 273](#).

When you move the resource, all items in its mailbox are moved to the new post office, which means that all schedules for the resource are kept intact.

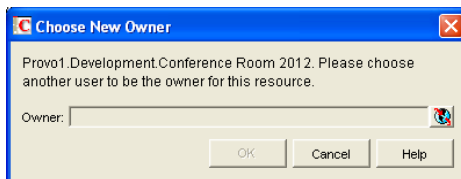
To move a resource:

- 1 In ConsoleOne, right-click the Resource object in the GroupWise View, then click *Move* to display the GroupWise Move dialog box.

IMPORTANT: You must select the Resource object in the GroupWise View. If you select the object in the standard ConsoleOne View, you will move the Resource object from one container to another, not the resource from one post office to another.



- 2 Select the post office to which you want to move the resource, then click *OK* to display the Choose New Owner dialog box.

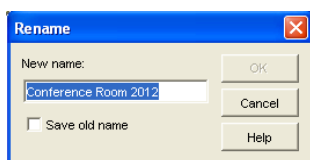


- 3 Select the user who will be the resource's owner, then click *OK* to move the resource.

16.5 Renaming a Resource

Situations might arise where you need to give a resource a new name. For example, you might need to move the resource to another post office that already has a user, resource, or distribution list with the same name.

- 1 In ConsoleOne, right-click the Resource object in the GroupWise View, then click *Rename* to display the *Rename* dialog box



- 2 In the *New Name* field, specify the new name for the resource.
- 3 Make sure the *Save Old Name* box is not selected.
Saving the old name causes duplicate resources to appear in the Address Book.
- 4 Click *OK* to rename the resource.

16.6 Deleting a Resource

When you delete a resource, all information is removed for the resource, including any schedules that have been established for the resource.

- 1 In ConsoleOne, right-click the Resource object in the GroupWise View, then click *Delete*.
- 2 Click *Yes* to confirm the deletion.

16.7 Managing Resource Email Addresses

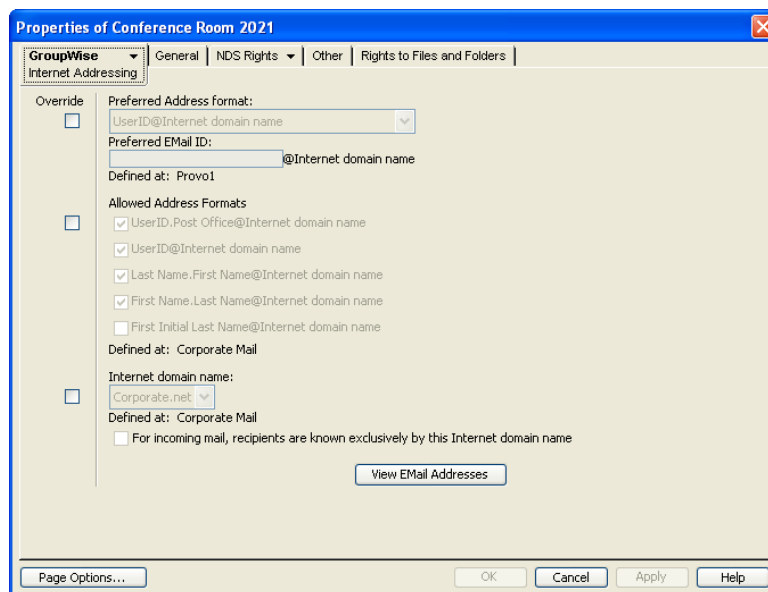
To ensure that resource addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for resources. The following sections provide details:

- ♦ [Section 16.7.1, “Changing a Resource’s Internet Addressing Settings,” on page 274](#)
- ♦ [Section 16.7.2, “Changing a Resource’s Visibility in the Address Book,” on page 275](#)
- ♦ [Section 16.7.3, “Creating a Nickname for a Resource,” on page 276](#)

16.7.1 Changing a Resource’s Internet Addressing Settings

By default, a resource inherits its Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from its post office, domain, or GroupWise system. If necessary, you can override these settings.

- 1 In ConsoleOne, right-click the Resource object, then click *Properties*.
- 2 Click *GroupWise*, then click *Internet Addressing* to display the Internet Addressing page.



- 3 To override one of the settings, select the *Override* box, then change the setting.

Preferred Address Format: The preferred address format determines how the resource's address are displayed in the GroupWise Address Book and in sent messages.

At the resource level, only three preferred address formats are available. The address formats that include first name, last name, and first initial do not apply to resource, so they are not available.

You can completely override the address format by explicitly defining the user portion of the address (*user@Internet domain name*). The user portion can include any RFC-compliant characters (no spaces, commas, and so on). The resource name portion must be unique within its Internet domain. This means that a resource name can be used multiple times in your GroupWise system, if it is used only once in each Internet domain.

Allowed Address Formats: The allowed address formats determine which address formats can be used to send messages to the resource.

Only the *UserID.Post Office@Internet domain name* and *UserID@Internet domain name* formats are valid for resources. The formats that include first name, last name, and first initial are not valid.

For example, assume that you use R1 as the resource ID, Research as the post office, and novell.com as the Internet domain. If you select the two valid formats, the resource receives messages sent using either of the following addresses:

r1.research@novell.com
r1@novell.com

Internet Domain Name: The Internet domain name, along with the preferred address format, is used when constructing the email address that is displayed in the GroupWise Address Book and in the *To* field of sent messages.

Only the Internet domain names that have been defined are displayed in the list. Internet domain names must be defined at the system level (*Tools > GroupWise System Operations > Internet Addressing*). For more information, see [Section 52, "Configuring Internet Addressing," on page 743](#).

If you override the Internet domain name, the *For Incoming Mail, Recipients are Known Exclusively by This Internet Domain Name* option becomes available. Enable this option if you only want the resource to be able to receive messages addressed with this Internet domain name. If you don't enable this option, the resource receives messages addressed using any of the Internet domain names assigned to your GroupWise system.

View E-Mail Addresses: Click *View E-Mail Addresses* to display a list of the various email address formats that can successfully deliver email to this resource, including any nicknames or gateway aliases that have been defined for this resource. For more information, see:

- ♦ [Section 52.1.4, "Preferred Address Format," on page 744](#) and [Section 52.1.5, "Allowed Address Formats," on page 747](#)
- ♦ [Section 14.7.4, "Creating a Nickname for a User," on page 252](#)
- ♦ [Section 52.3, "Transitioning from SMTP Gateway Aliases to Internet Addressing," on page 754](#)

- 4 Click *OK* to save your changes.

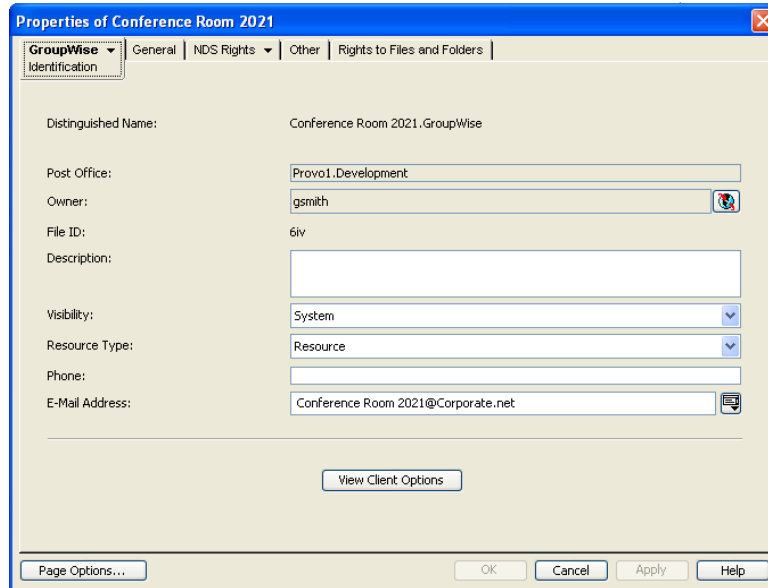
16.7.2 Changing a Resource's Visibility in the Address Book

A resource's visibility level determines which users see the resource in their Address Books. You can control the availability of a resource by displaying it in the Address Books of all users in your GroupWise system, in the Address Books of those users in the resource's domain only, in the Address

Books of those users on the resource's post office only, or in no Address Books. Even if the resource is not displayed in their Address Books, users can schedule the resource if they know the resource's name.

To change a resource's visibility:

- 1 In ConsoleOne, right-click the Resource object, then click *Properties*.



- 2 In the *Visibility* field, select the desired visibility level.

System: The resource is displayed in the Address Books of all users in your GroupWise system.

Domain: The resource is displayed in the Address Books of all users in the resource's domain.

Post Office: The resource is displayed in the Address Books of all users on the resource's post office.

None: The resource is not displayed in any Address Books. Users need to know the resource's name to schedule it.

- 3 Click *OK* to save your changes.

16.7.3 Creating a Nickname for a Resource

Each resource has a specific GroupWise address consisting of the resource's name, post office, and domain (*resource_name.post_office.domain*). You can assign one or more nicknames to a resource to give it an additional address. Each part of the address (*resource_name*, *post_office*, and *domain*) can be different than the resource's actual address.

Nicknames are useful in the following situations:

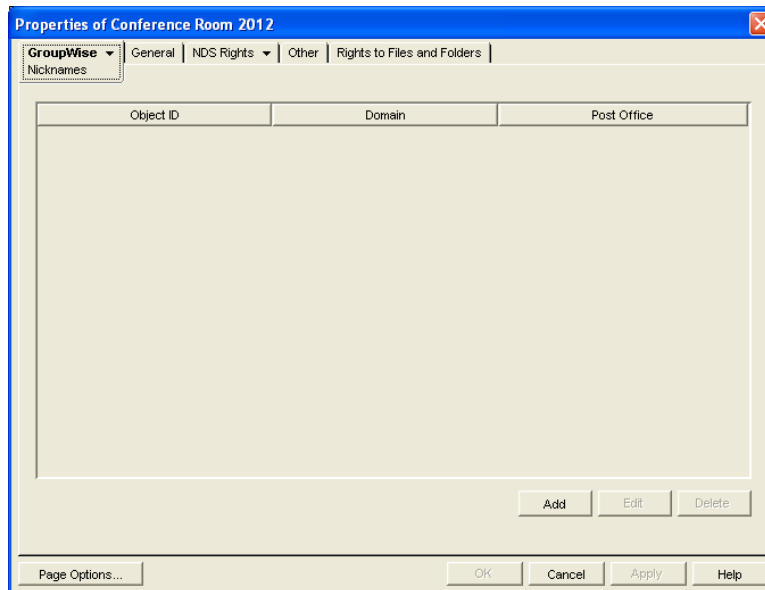
- ♦ You rename a resource, as described in [Section 16.5, "Renaming a Resource," on page 273](#). You can create a nickname that retains the old resource name, so that messages with the old resource name in the email address are routed to the new email address.

- ♦ You move a resource, as described in [Section 16.4, “Moving a Resource,”](#) on page 273. You can create a nickname that retains the old post office location. As messages to the moved resource arrive in your GroupWise system, the email address is routed to the new post office location. .
- ♦ You need to restrict a resource’s visibility in the GroupWise Address Book, as described in [Section 6.2, “Controlling Object Visibility,”](#) on page 110, and at the same time, you need to make the resource visible in one or more specific Address Books outside of the restricted visibility. You can create a nickname that provides the specific visibility that is ruled out by the required restriction.

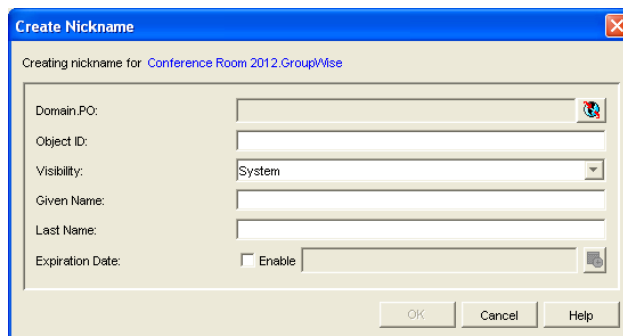
In ConsoleOne, you can list all the nicknames in your GroupWise system in the GroupWise View. In the GroupWise client, you can display resource nicknames in the GroupWise Address Book if you enable *Filter for Resources*. When addressing a message, users need to know a nickname in order to use it.

To create a nickname for a resource:

- 1 In ConsoleOne, right-click the Resource object, then click *Properties*.
- 2 Click *GroupWise > Nicknames* to display the Nicknames page.



- 3 Click *Add* to display the Create Nickname dialog box.



- 4 Fill in the following fields:

Domain.PO: Select the post office that you want to own the nickname. This can be any post office in your GroupWise system; it does not need to be the resource’s post office.

Object ID: Specify the name to use as the *resource_name* portion of the nickname. The nickname must be unique.

Visibility: Select the Address Book visibility for the nickname. This determines where the nickname is available (system, domain, or post office). However, nicknames are not displayed in the Address Book unless you filter for them. In order to address a message to a nickname, a user must specify the nickname address, and the nickname must be available in the user's post office.

External Sync Override: This option applies only if your GroupWise system links to and synchronizes with an external GroupWise system, as described in [“Connecting to Other GroupWise Systems”](#) in the *GroupWise 2012 Multi-System Administration Guide*.

- ♦ **Synchronize According to Visibility:** The nickname is synchronized to external GroupWise systems only if Address Book visibility is set to *System*.
- ♦ **Synchronize Regardless of Visibility:** The nickname is synchronized to external GroupWise systems regardless of Address Book visibility.
- ♦ **Don't Synchronize Regardless of Visibility** The nickname is never synchronized to external systems.

Given Name: This field is not used for resource nicknames.

Last Name: This field is not used for resource nicknames.

Expiration Date: If you want the nickname to no longer work after a certain date, click *Enable* and then select the desired date.

- 5 Click *OK* to add the nickname to the list.
- 6 Click *OK* to save the changes to the Resource object.

VI Distribution Lists, Groups, and Organizational Roles

- ♦ Chapter 17, “Understanding Distribution Lists, Groups, and Organizational Roles,” on page 281
- ♦ Chapter 18, “Creating and Managing Distribution Lists,” on page 285
- ♦ Chapter 19, “Using eDirectory Groups as GroupWise Distribution Lists,” on page 301
- ♦ Chapter 20, “Using eDirectory Organizational Roles as GroupWise Distribution Lists,” on page 307

17 Understanding Distribution Lists, Groups, and Organizational Roles

Distribution lists are specific to GroupWise. Groups and organizational roles are eDirectory objects that can be configured to work with GroupWise.

Distribution lists, groups, and organizational roles are all sets of users and (optionally) resources that can be addressed as a single entity. When a GroupWise user addresses an item (message, appointment, task, or note) to a distribution list, group, or organizational role, each user or resource that is a member receives the item if he or she has a GroupWise account.

The following sections provide information to help you learn about distribution lists, groups, and organizational roles:

- ◆ [Section 17.1, “Public vs. Personal Address Lists,” on page 281](#)
- ◆ [Section 17.2, “Distribution Lists,” on page 281](#)
- ◆ [Section 17.3, “eDirectory Groups and Organizational Roles,” on page 282](#)

17.1 Public vs. Personal Address Lists

Distribution lists and groups are public address lists, meaning that they are administrator-defined lists available to all users in your GroupWise system.

If users want to create personal address lists, they can create personal groups in the GroupWise client. When a user creates personal groups, the groups are saved in his or her mailbox and are available for use only by that user. They cannot be shared by, or transferred to, other users.

If a user wants to send to all users in a particular post office or domain, he or she can use wildcard addressing, if it has been enabled. See [Section 6.7, “Enabling Wildcard Addressing,” on page 114](#).

17.2 Distribution Lists

A distribution list is specific to GroupWise. It is a public address list that you, as the GroupWise administrator, can create to facilitate easier addressing within your GroupWise system. Distribution lists can only contain users that have GroupWise accounts.

Each distribution list you want to create must be added as a Distribution List object in eDirectory. The name that you give the Distribution List object becomes the name by which the distribution list is displayed in the GroupWise Address Book.

Distribution List objects can be located in any eDirectory container that is in the same tree as the distribution list’s domain.

Because a distribution list is an addressable entity, you must assign it to a post office when you create it. This ensures that the distribution list has a standard GroupWise address (*distribution_list_name.post_office.domain*).

Regardless of the distribution list's post office, all GroupWise users can use the distribution list when addressing a message.

You can determine which users see the distribution list in the Address Book. System visibility enables all users in your GroupWise system to see the distribution list. Domain visibility enables all users in the distribution list's domain to see the distribution list. Post Office visibility enables all users in the distribution list's post office to see the distribution list. Setting the visibility level to *None* means that no users see the distribution list in the Address Book.

Users who cannot see the distribution list in the Address Book can still use the distribution list by typing the distribution list name in the To field of the message.

A distribution list can contain users and resources as well as other distribution lists, groups, and organizational roles. Members do not need to be on the same post office as the distribution list's post office.

For details about distribution lists, see [Chapter 18, "Creating and Managing Distribution Lists," on page 285](#).

17.3 eDirectory Groups and Organizational Roles

eDirectory groups and organizational roles are general eDirectory objects that can be created to facilitate easier administration of eDirectory users who have common needs or who share a common role or responsibility.

If you have eDirectory groups or organizational roles that you want GroupWise users to be able to address messages to, you need to make them available in your GroupWise system. When doing so, you can choose the groups and roles that you want available, and choose which users they are available to.

If a group or role contains both eDirectory users with GroupWise accounts and eDirectory users without GroupWise accounts, only those users with GroupWise accounts receive messages addressed to the group or role.

As mentioned previously, Group and Organizational Role objects are not specific to GroupWise. For information about creating these objects, see your eDirectory documentation.

The name given to the Group object or Organizational Role object becomes the name by which it is displayed in the GroupWise Address Book when you make it available. You make a group or role available in your GroupWise system by assigning it to a post office. This ensures that the group or role has a standard GroupWise address (*name.post_office.domain*). Regardless of the post office where the group or role is assigned, all GroupWise users can use it when addressing a message.

You can determine which users see the group or role in the Address Book. System visibility enables all users in your GroupWise system to see the group or role. Domain visibility enables all users in the distribution list's domain to see the group or role. Post Office visibility enables all users in the distribution list's post office to see the group or role. Setting the visibility level to *None* means that no users can see the group or role in the Address Book.

Users who cannot see the group or role in the Address Book can still use it by typing the name in the To field of the message.

For details about eDirectory groups and organizational roles, see [Chapter 19, “Using eDirectory Groups as GroupWise Distribution Lists,”](#) on page 301 and [Chapter 20, “Using eDirectory Organizational Roles as GroupWise Distribution Lists,”](#) on page 307.

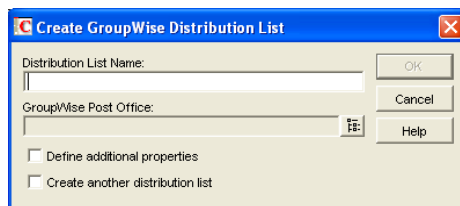
18 Creating and Managing Distribution Lists

A GroupWise distribution list can contain GroupWise users, resources, and other distribution lists. When creating the distribution list, you can determine each entry's participation in the list (primary recipient, carbon copy recipient, or blind copy recipient). Distribution lists are created in the GroupWise Address Book. When a GroupWise user addresses an item (message, appointment, task, or note) to a distribution list, group, or organizational role, each user or resource that is a member receives the item if he or she has a GroupWise account.

- ♦ [Section 18.1, "Creating a New Distribution List," on page 285](#)
- ♦ [Section 18.2, "Adding Members to a Distribution List," on page 289](#)
- ♦ [Section 18.3, "Removing Members from a Distribution List," on page 290](#)
- ♦ [Section 18.4, "Moving a Distribution List," on page 290](#)
- ♦ [Section 18.5, "Renaming a Distribution List," on page 291](#)
- ♦ [Section 18.6, "Enabling Users to Modify a Distribution List," on page 291](#)
- ♦ [Section 18.7, "Controlling Access to a Distribution List," on page 293](#)
- ♦ [Section 18.8, "Deleting a Distribution List," on page 294](#)
- ♦ [Section 18.9, "Managing Email Addresses," on page 294](#)
- ♦ [Section 18.10, "Adding External Users to a Distribution List," on page 299](#)

18.1 Creating a New Distribution List

- 1 In ConsoleOne, right-click the eDirectory container where you want to create the Distribution List object, then click *New > Distribution List*.



- 2 Fill in the following fields:

Distribution List Name: Specify a descriptive name. Because the name is used as part of the distribution list's GroupWise email address, do not use any of the following invalid characters in the distribution list name:

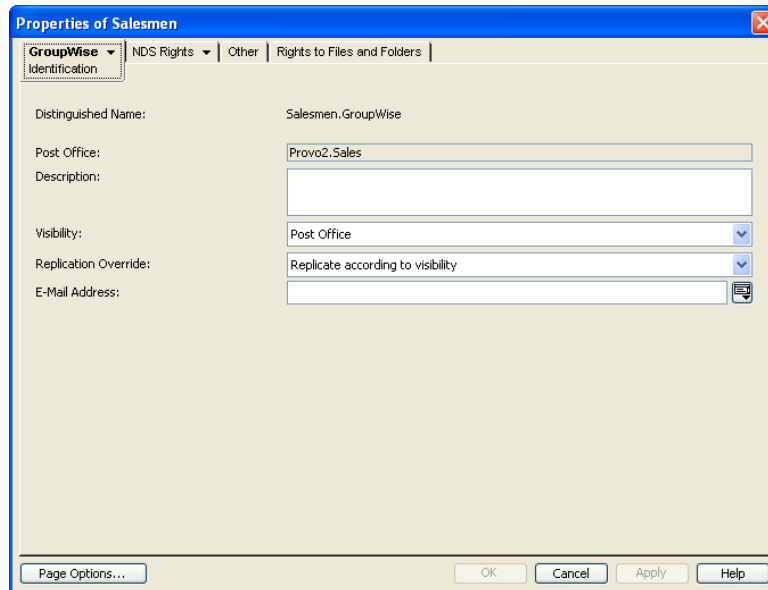
ASCII characters 0-31 Comma ,
Asterisk * Double quote "

At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

IMPORTANT: Characters that are valid and even desirable in a distribution list name, such as accented characters, might not be valid in an email address. For some distribution lists you might need to set up a preferred email ID in order to ensure that they have a valid email address. For instructions, see [Section 18.9.1, “Changing a Distribution List’s Internet Addressing Settings,”](#) on page 295.

GroupWise Post Office: Select the post office the distribution list will be assigned to. The distribution list can contain members of other post offices.

- 3 Select *Define Additional Properties*, then click *OK*.



- 4 On the Identification page, fill in the following fields:

Description: Specify a description to help you identify the purpose or members of the distribution list.

Visibility: Select the level at which the distribution list will be visible in the Address Book. *System* enables the distribution list to be visible to all users in your GroupWise system. *Domain* enables the distribution list to be visible to all users in the same domain as the distribution list. *Post Office* enables the distribution list to be visible to all users on the same post office as the distribution list. Setting the visibility level to *None* means that no users can see the distribution list in the Address Book.

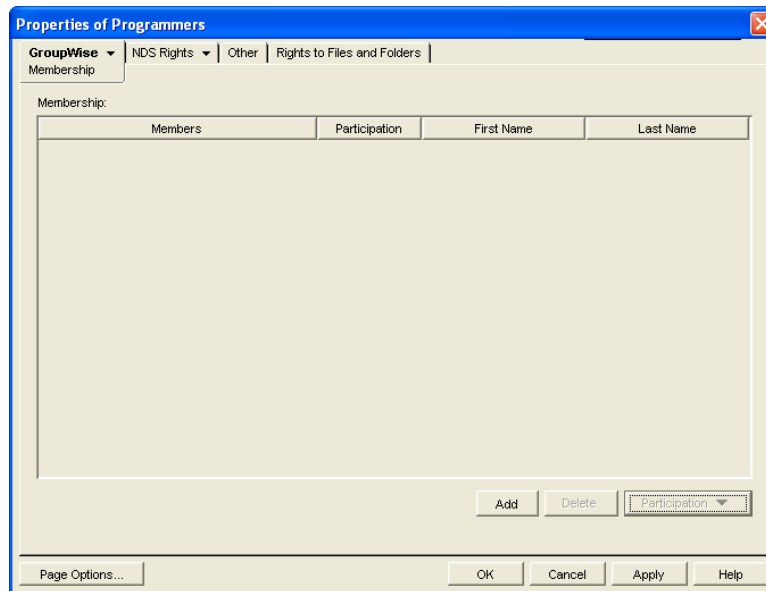
Replication Override: By default, distribution lists are replicated throughout your GroupWise system based on the selected visibility level. With the default visibility level, distribution lists are visible in the GroupWise Address Book for local post office users only and are not replicated to other post offices.

If you set Visibility to *Domain*, the distribution list is replicated to all post offices in the domain, but not to post offices belonging to other domains. If you set Visibility to *System*, the distribution list is replicated to all post offices in your GroupWise system. This default behavior corresponds to the *Replicate According to Visibility* setting.

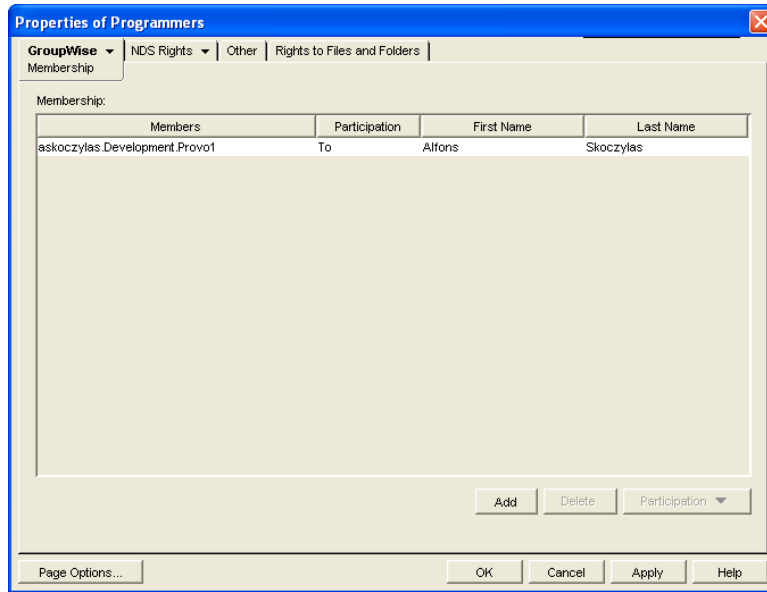
Select *Replicate Everywhere Regardless of Visibility* if you want the distribution list replicated throughout your GroupWise system regardless of the selected visibility level. With this setting, the distribution list is made available in all post offices, although it is still only visible in the GroupWise Address Book according to the selected visibility level. The availability of the distribution list in all post offices means that it can be nested into other distribution lists that are visible in any post office, and that users in any post office can manually specify the distribution list name in the To field of an item.

E-Mail Address: Displays the default email address for the distribution list. Click the drop-down list to specify a custom email address. For example, if you created a distribution list with spaces in its name, you need to remove the spaces to create a valid email address.

- 5 Click *GroupWise > Membership* to display the Membership page.



- Click *Add*, select the user, resource, distribution list, eDirectory group, or organizational role you want to add as a member, then click *OK* to add the member to the list.



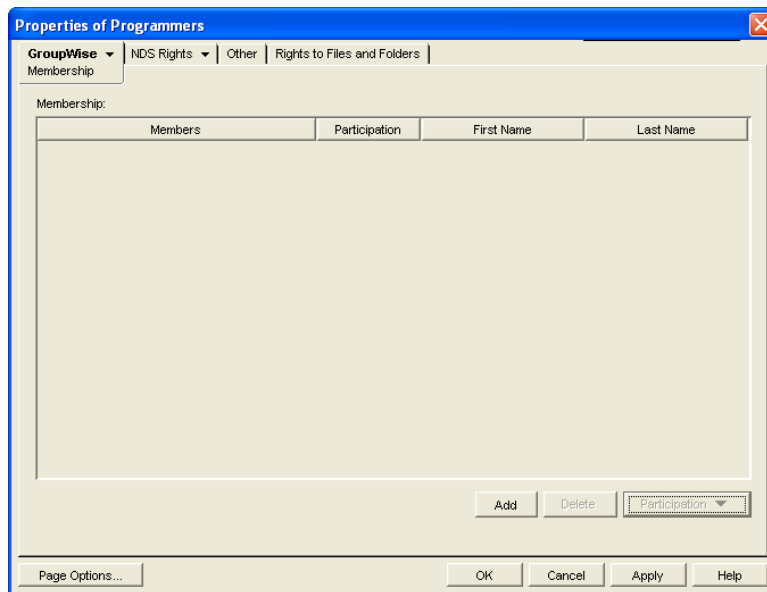
By default, the member is added as a primary recipient (To: recipient).

- If you want to change the member's recipient type, select the member, click *Participation*, then click *To*, *CC*, or *BC*.
- Repeat [Step 6](#) and [Step 7](#) to add additional members.
- Click *OK* to save your changes.

18.2 Adding Members to a Distribution List

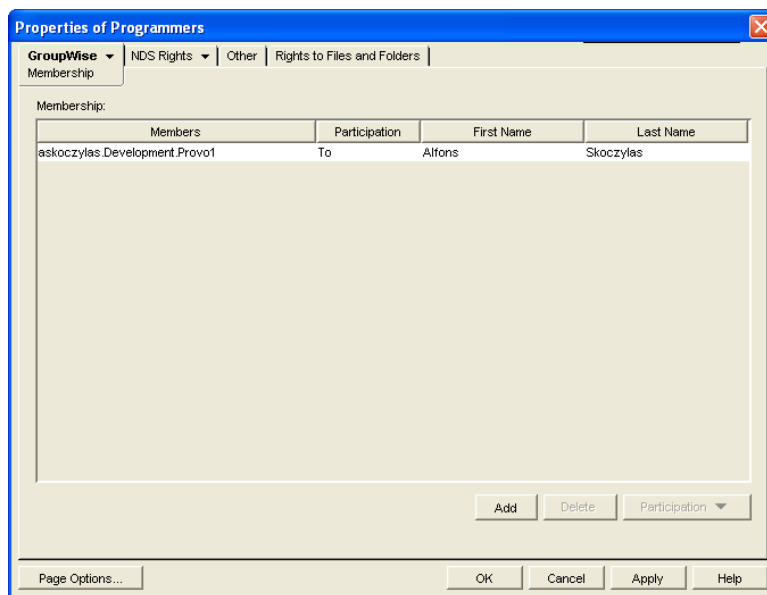
Distribution lists can contain users, resources, groups, organizational roles, and other distribution lists.

- 1 In ConsoleOne, right-click the Distribution List object, then click *Properties*.
- 2 Click *GroupWise > Membership* to display the Membership page.



- 3 Click *Add*, select the user, resource, distribution list, group, or organizational role you want to add as a member, then click *OK* to add the member to the list.

If you want to add an external user that is not listed for selection, see [Section 18.10, “Adding External Users to a Distribution List,”](#) on page 299.



By default, the selected member is added as a primary recipient (To: recipient).

- 4 If you want to change the member's recipient type, select the member, click *Participation*, then click *To*, *CC*, or *BC*.
- 5 Repeat [Step 3](#) and [Step 4](#) to add additional members.
- 6 Click *OK* to save your changes.

Distribution lists are typically managed by an administrator in ConsoleOne. Starting in GroupWise 7, users can be granted rights to modify distribution lists, as described in [Section 18.6, "Enabling Users to Modify a Distribution List,"](#) on page 291.

In addition, GroupWise client users can create shared address books and then create groups within those shared address books so that the groups are available to all users with whom the address book has been shared. The creator of the shared address book can give other users read only rights, or can choose to grant them additional rights for adding, editing, and deleting information. For more information about shared address books, see ["Sharing an Address Book with Another User"](#) in ["Contacts and Address Books"](#) in the *GroupWise 2012 Windows Client User Guide*.

18.3 Removing Members from a Distribution List

When you remove users' or resources' GroupWise accounts, delete groups, delete organizational roles, or delete distribution lists, they are automatically removed from any distribution lists in which they have membership.

To manually remove members from a distribution list:

- 1 In ConsoleOne, right-click the Distribution List object, then click *Properties*.
- 2 Click *GroupWise > Membership* to display the Membership page.
- 3 Select the member you want to remove from the list, then click *Delete*.

18.4 Moving a Distribution List

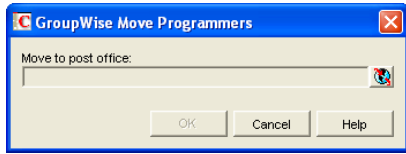
If necessary, you can move a distribution list from one post office to another. For example, you might need to move a distribution list from a post office you are removing.

The distribution list retains the same name on the new post office as it has on the current post office. If another user, resource, or distribution list assigned to the new post office has the same name, you must rename one of them before you move the distribution list. For details, see [Section 18.5, "Renaming a Distribution List,"](#) on page 291.

To move a distribution list:

- 1 In ConsoleOne, right-click the Distribution List object in the GroupWise View, then click *Move* to display the GroupWise Move dialog box.

IMPORTANT: You must select the Distribution List object in the GroupWise View. If you select the object in the standard Console View, you will move the Distribution List object from one container to another, not the distribution list from one post office to another.



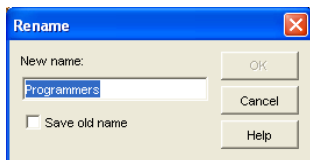
- 2 Select the post office to which you want to move the distribution list, then click *OK* to move the distribution list.

18.5 Renaming a Distribution List

Situations might arise where you need to give a distribution list a new name. For example, you might need to move the distribution list to another post office that already has a user, resource, or distribution list with the same name.

To rename a distribution list:

- 1 In ConsoleOne, right-click the Distribution List object in the GroupWise View, then click *Rename* to display the Rename dialog box.



- 2 In the *New Name* field, specify the new name for the distribution list.
- 3 Make sure the *Save Old Name* box is not selected. Saving the old name causes duplicate distribution lists to appear in the Address Book.
- 4 Click *OK* to rename the distribution list.

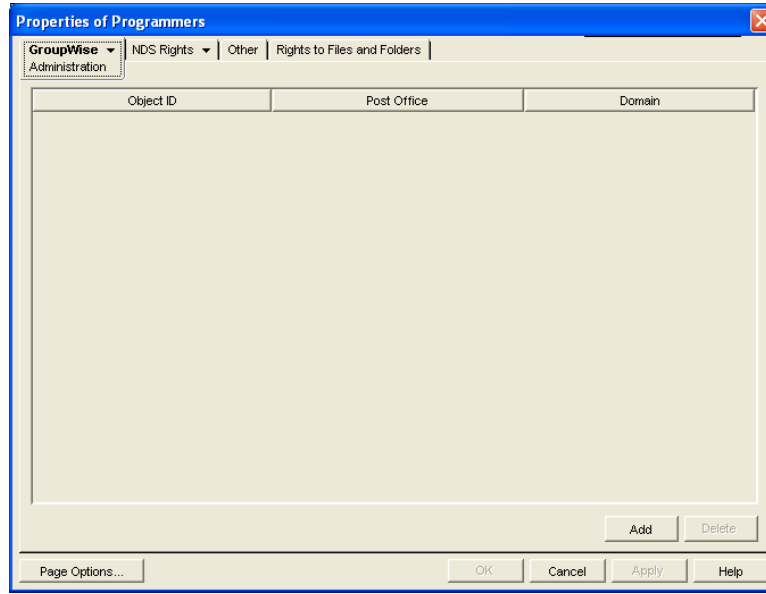
18.6 Enabling Users to Modify a Distribution List

In ConsoleOne, you can grant rights to users to modify distribution lists from the GroupWise Windows client. However, users cannot create or delete distribution lists; that can be done only in ConsoleOne by an administrator.

To grant edit rights to a specific distribution list to one or more users:

- 1 Browse to and right-click a Distribution List object, then click *Properties*.

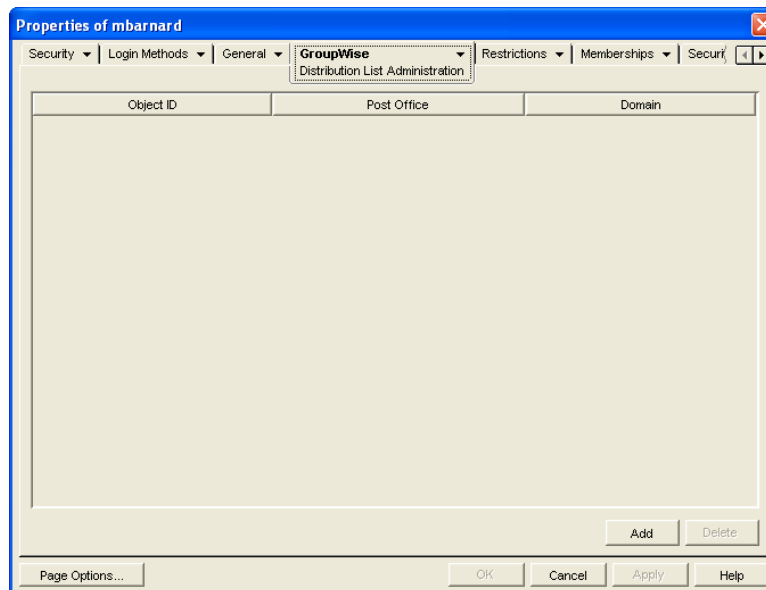
2 Click *GroupWise > Administration*.



- 3 Click *Add*, then select one or more users who can edit the distribution list.
- 4 Click *OK* to grant the edit rights.
- 5 Notify the users that they have rights to modify the distribution list.

To give a specific user rights to edit one or more distribution lists:

- 1 Browse to and right-click a User object, then click *Properties*.
- 2 Click *GroupWise > Distribution List Administration*.



- 3 Click *Add*, then select one or more distribution lists for the user to edit.
- 4 Click *OK* to grant the edit rights.

- 5 Notify the user that he or she has rights to modify the distribution lists.

In the GroupWise client, the editable distribution list does not appear any different to the user who has rights to edit it, except that *Add* and *Remove* are active for that user.

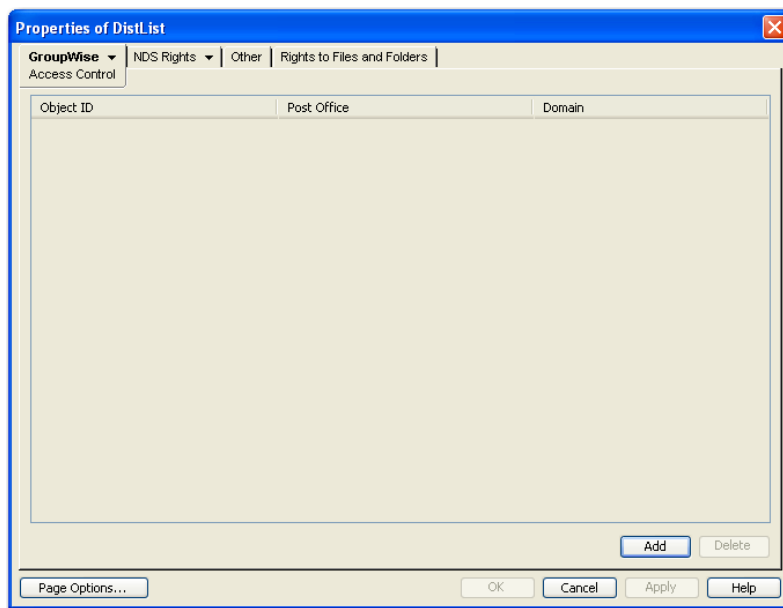
In Online mode, the user can edit the distribution list in the GroupWise Address Book. In Caching mode, the user cannot edit the distribution list in the GroupWise Address Book. However, the user can edit the distribution list in the Address Selector in a new message.

18.7 Controlling Access to a Distribution List

By default, all GroupWise users can send to all distribution lists that appear in the GroupWise Address Book. If necessary, you can restrict which users are allowed to send to a specific distribution list. The restricted distribution list still appears in the GroupWise Address Book, but if unauthorized users try to send to the restricted distribution list, they receive an error indicating that they do not have the rights to use the restricted distribution list.

To restrict access to a distribution list:

- 1 Browse to and right-click a Distribution List object, then click *Properties*.
- 2 Click *GroupWise > Access Control*.



- 3 Click *Add*, select one or more users who are allowed to send to the restricted distribution list, then click *OK* to add the users to the Access Control list.
- 4 (Optional) Click *Add*, select *Distribution Lists*, select one or more distribution lists that are allowed to send to the restricted distribution list, then click *OK* to add the distribution lists to the Access Control list.
- 5 Click *OK* to grant the rights to the listed users and distribution lists for sending to the restricted distribution list.
- 6 Notify the users that they have rights to send to the restricted distribution list.

In addition to the users that you add to the Access Control list, users to whom you have granted edit rights, as described in [Section 18.6, “Enabling Users to Modify a Distribution List,”](#) on page 291, can also send to the restricted distribution list, even if you do not explicitly add them to the Access Control list.

NOTE: This functionality was introduced in GroupWise 8 Support Pack 2. If you still run GroupWise 8 clients in your GroupWise 2012 system, you must update all GroupWise 8 clients to Support Pack 2 or later in order for this feature to function for GroupWise 8 client users.

18.8 Deleting a Distribution List

To delete a single distribution list:

- 1 In ConsoleOne, right-click the Distribution List object, then click *Delete*.
- 2 Click *Yes* to confirm the deletion.

To delete multiple distribution lists that belong to the same post office:

- 1 In ConsoleOne, right-click the Post Office object, then click *Properties*.
- 2 Click *GroupWise > Distribution Lists*.
- 3 Select one or more distribution lists, then click *Delete*.
- 4 Click *OK* to complete the deletion.

18.9 Managing Email Addresses

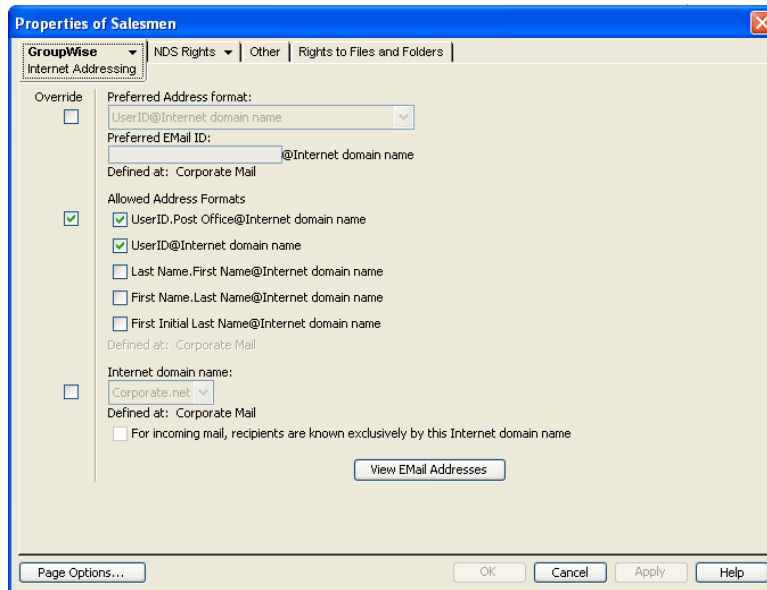
To ensure that distribution list addresses meet your needs, GroupWise enables you to determine the format and visibility of addresses, as well as create additional names for distribution lists. The following sections provide details:

- ♦ [Section 18.9.1, “Changing a Distribution List’s Internet Addressing Settings,”](#) on page 295
- ♦ [Section 18.9.2, “Changing a Distribution List’s Visibility in the Address Book,”](#) on page 296
- ♦ [Section 18.9.3, “Creating a Nickname for a Distribution List,”](#) on page 297

18.9.1 Changing a Distribution List's Internet Addressing Settings

By default, a distribution list inherits its Internet address settings (preferred Internet address format, allowed address formats, and Internet domain name) from its post office, domain, or GroupWise system. If necessary, you can override these settings for a distribution list.

- 1 In ConsoleOne, right-click the Distribution List object, then click *Properties*.
- 2 Click GroupWise, then click *Internet Addressing* to display the Internet Addressing page.



- 3 To override one of the settings, select the *Override* box, then change the setting.

Preferred Address Format: The preferred address format determines how the distribution list's address is displayed in the GroupWise Address Book and in sent messages.

At the distribution list level, only three preferred address formats are available. The address formats that include first name, last name, and first initial do not apply to distribution lists, so they are not available.

You can completely override the address format by explicitly defining the user portion of the address (*user@Internet domain name*). The user portion can include any RFC-compliant characters (no spaces, commas, and so on). The distribution list name portion must be unique within its Internet domain. This means that a distribution list name can be used multiple times in your GroupWise system, provided it is used only once in each Internet domain.

Allowed Address Formats: The allowed address formats determine which address formats can be used to send messages to the distribution list.

Only the *UserID.Post Office@Internet domain name* and *UserID@Internet domain name* formats are valid for distribution lists. The formats that include first name, last name, and first initial are not valid.

For example, assume that you use DL1 as the distribution list ID, Research as the post office, and novell.com as the Internet domain. If you select the two valid formats, members of the distribution list receive messages sent using either of the following addresses:

dl1.research@novell.com
dl1@novell.com

Internet Domain Name: The Internet domain name, along with the preferred address format, is used when constructing the email address that is displayed in the GroupWise Address Book and in the To field of sent messages.

Only the Internet domain names that have been defined are displayed in the list. Internet domain names must be defined at the system level (*Tools > GroupWise System Operations > Internet Addressing*). For more information, see [Section 52, “Configuring Internet Addressing,”](#) on page 743.

If you override the Internet domain name, the *For Incoming Mail, Recipients are Known Exclusively by This Internet Domain Name* option becomes available. Enable this option if you only want the distribution list to be able to receive messages addressed with this Internet domain name. If you don't enable this option, the distribution list receive messages addressed using any of the Internet domain names assigned to your GroupWise system.

View E-Mail Addresses: Click *View E-Mail Addresses* at the bottom of the Internet Addressing page to display a list of the various email address formats that can successfully deliver email to this distribution list, including any nicknames or gateway aliases that have been defined for this distribution list. For more information, see:

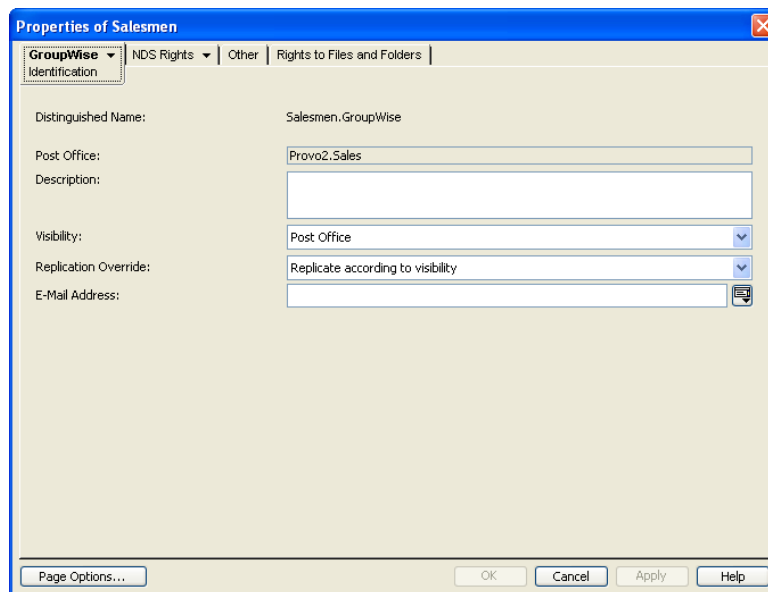
- ◆ [Section 52.1.4, “Preferred Address Format,”](#) on page 744 and [Section 52.1.5, “Allowed Address Formats,”](#) on page 747
- ◆ [Section 14.7.4, “Creating a Nickname for a User,”](#) on page 252
- ◆ [Section 52.3, “Transitioning from SMTP Gateway Aliases to Internet Addressing,”](#) on page 754

4 Click *OK* to save your changes.

18.9.2 Changing a Distribution List's Visibility in the Address Book

A distribution list's visibility level determines which users see the distribution list in the Address Books. You can control the availability of a distribution list by displaying it in the Address Book for all users in your GroupWise system, in the Address Book for those users in the distribution list's domain only, in the Address Book for those users on the distribution list's post office only, or not displaying it at all.

1 In ConsoleOne, right-click the Distribution List object, then click *Properties*.



- 2 In the *Visibility* field, select the desired visibility level.

System: The distribution list is displayed in the Address Book for all users in your GroupWise system.

Domain: The distribution list is displayed in the Address Book for all users in the distribution list's domain.

Post Office: The distribution list is displayed in the Address Book for all users on the distribution list's post office.

None: The distribution list not displayed in the Address Book.

- 3 Click *OK* to save your changes.

18.9.3 Creating a Nickname for a Distribution List

Each distribution list has a specific GroupWise address consisting of the distribution list's name, post office, and domain (*distribution_list_name.post_office.domain*). You can assign one or more nicknames to a distribution list to give it an additional address. Each part of the address (*distribution_list_name*, *post_office*, and *domain*) can be different than the distribution list's actual address.

Nicknames are useful in the following situations:

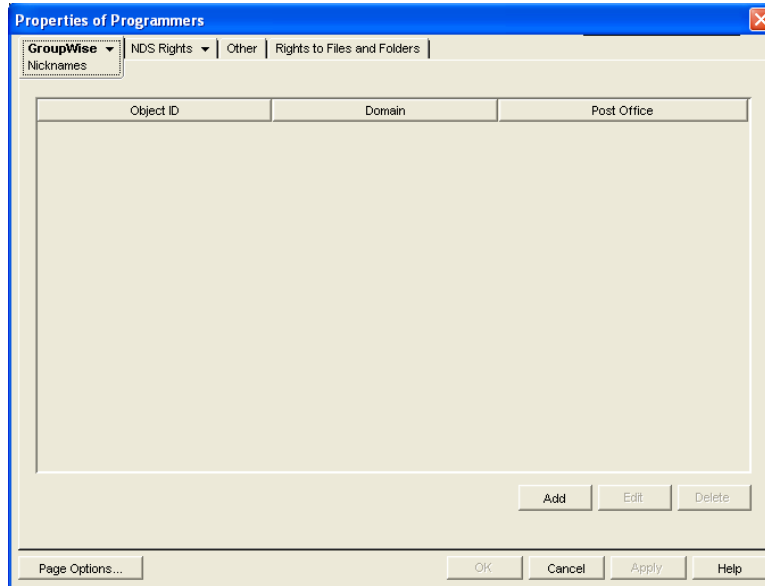
- ♦ You rename a distribution list, as described in [Section 18.5, "Renaming a Distribution List," on page 291](#). You can create a nickname that retains the old distribution list name, so that messages with the old distribution list name in the email address are routed to the new email address.
- ♦ You move a distribution list, as described in [Section 18.4, "Moving a Distribution List," on page 290](#). You can create a nickname that retains the old post office location. As messages to the moved distribution list arrive in your GroupWise system, the email address is routed to the new post office location.
- ♦ You need to restrict a distribution list's visibility in the GroupWise Address Book, as described in [Section 6.2, "Controlling Object Visibility," on page 110](#), and at the same time, you need to make the distribution list visible in one or more specific Address Books outside of the restricted visibility. You can create a nickname that provides the specific visibility that is ruled out by the required restriction.

In ConsoleOne, you can list all the nicknames in your GroupWise system in the GroupWise View. In the GroupWise client, you can display resource nicknames in the GroupWise Address Book if you enable *Filter for Resources*. When addressing a message, users need to know a nickname in order to use it.

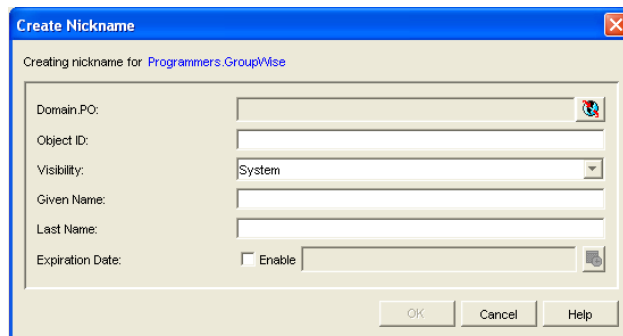
To create a nickname for a distribution list:

- 1 In ConsoleOne, right-click the Distribution List object, then click *Properties*.

2 Click *GroupWise > Nicknames* to display the Nicknames page.



3 Click *Add* to display the Create Nickname dialog box.



4 Fill in the following fields:

Domain.PO: Select the post office that you want to own the nickname. This can be any post office in your GroupWise system; it does not need to be the distribution list's post office.

Object ID: Specify the name to use as the *distribution_list_name* portion of the nickname. The name must be unique.

Visibility: Select the Address Book visibility for the nickname. This determines where the nickname is available (system, domain, or post office). However, nicknames are not displayed in the Address Book unless you filter for them. In order to address a message to a nickname, a user must specify the nickname address, and the nickname must be available in the user's post office.

External Sync Override: This option applies only if your GroupWise system links to and synchronizes with an external system, as described in "[Connecting to Other GroupWise Systems](#)" in the *GroupWise 2012 Multi-System Administration Guide*.

- ◆ **Synchronize According to Visibility:** The nickname information is synchronized to external systems only if visibility is set to *System*.
- ◆ **Synchronize Regardless of Visibility:** The nickname information is synchronized to external systems regardless of the object visibility.

- ♦ **Don't Synchronize Regardless of Visibility** The nickname information is not synchronized to external systems.

Given Name: This field is not used for distribution list nicknames.

Last Name: This field is not used for distribution list nicknames.

Expiration Date: If you want the nickname to no longer work after a certain date, click **Enable** and then select the desired date.

- 5 Click *OK* to add the nickname to the list.
- 6 Click *OK* to save the changes to the Distribution List object.

18.10 Adding External Users to a Distribution List

Members of distribution lists must have corresponding eDirectory objects. If you want to add users to a distribution list, and the users do not belong to your GroupWise system, you must create objects to represent these external users within your GroupWise system.

- ♦ [Section 18.10.1, "Creating an External Domain," on page 299](#)
- ♦ [Section 18.10.2, "Creating an External Post Office," on page 299](#)
- ♦ [Section 18.10.3, "Creating an External User," on page 299](#)

For more information, see [Section 6.8, "Adding External Users to the GroupWise Address Book," on page 116](#).

18.10.1 Creating an External Domain

You create an external domain to represent the world outside your GroupWise system.

- 1 In ConsoleOne, right-click GroupWise System, then click *New > External Domain*.
- 2 Provide a unique name for the domain, then click *OK*.

18.10.2 Creating an External Post Office

You create an external post office in the external domain to hold External User objects.

- 1 In ConsoleOne, right-click the External Domain object, then click *New > External Post Office*.
- 2 Provide a unique name for the post office, then click *OK*.

18.10.3 Creating an External User

You create an external user so that it can be selected when adding members to a distribution list.

- 1 In ConsoleOne, right-click the External Post Office object, then click *New > External User*.
- 2 Provide a unique name for the user, then click *OK*.
- 3 Right-click the new External User object, then click *Properties*.
- 4 On the Identification page, fill in at least the first and last names.
- 5 Click *GroupWise > Internet Addressing*.
- 6 Select *Override*.
- 7 Select the preferred addressing format depending on how you want email to this user to be addressed.

or

Provide a preferred email ID.

- 8** Click *OK* to save the user information.
- 9** Follow the instructions in [Section 18.2, “Adding Members to a Distribution List,”](#) on page 289 to add the external user to a distribution list.

19 Using eDirectory Groups as GroupWise Distribution Lists

Novell eDirectory groups can be configured to function as GroupWise distribution lists.



- ♦ [Section 19.1, “Setting Up an eDirectory Group for Use in GroupWise,” on page 301](#)
- ♦ [Section 19.2, “Seeing Which Members of an eDirectory Group Have GroupWise Accounts,” on page 303](#)
- ♦ [Section 19.3, “Changing a Group’s Visibility in the Address Book,” on page 304](#)
- ♦ [Section 19.4, “Moving a Group,” on page 304](#)
- ♦ [Section 19.5, “Renaming a Group,” on page 305](#)
- ♦ [Section 19.6, “Removing a Group from GroupWise,” on page 305](#)

19.1 Setting Up an eDirectory Group for Use in GroupWise

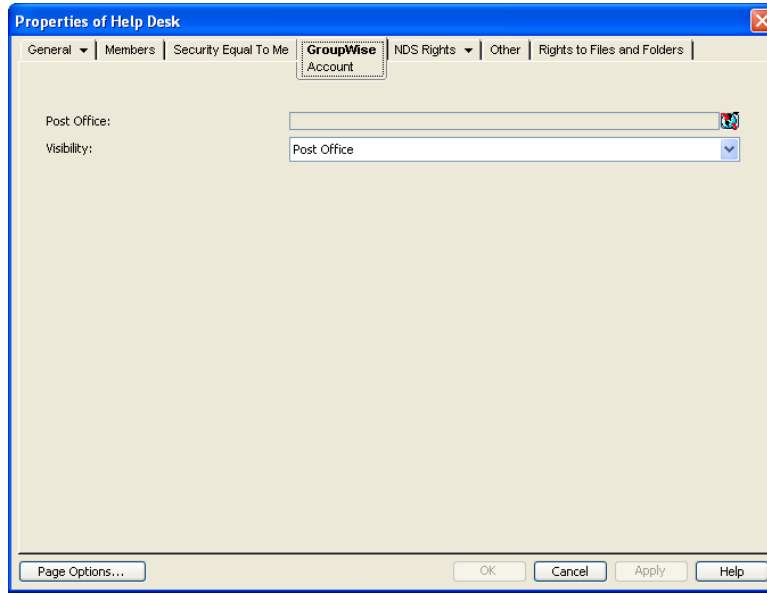
By default, eDirectory groups are not automatically available for use as distribution lists in GroupWise. To make an eDirectory group available as a GroupWise distribution list, you need to assign it to a GroupWise post office.

- 1 In ConsoleOne, right-click the eDirectory Group object, then click *Properties*.

Group objects and Distribution List objects have similar icons in ConsoleOne.

Icon	Object
	eDirectory Group object
	GroupWise Distribution List object

2 Click *GroupWise > Account* to display the Account page.



3 Fill in the following fields:

Post Office: Select the post office where you want to assign the group. You can choose any post office you want. If you plan to limit visibility of the group to users on a specific post office or in a specific domain, you should select that post office or a post office in the desired domain.

Visibility: Select the level at which the group is visible in the Address Book. *System* enables the group to be visible to all users in your GroupWise system. *Domain* enables the group to be visible to all users in the same domain as the group. *Post Office* enables the group to be visible to all users on the same post office as the group. Setting the visibility to *None* means that the group is not visible at any level. However, even if the group is not displayed in a user's Address Book, he or she can use the group by typing the group's name in a message's To field.

4 Click *OK* to save the changes.

The group is now treated like a GroupWise distribution list and is visible in the GroupWise View when you filter on distribution lists. However, its icon does not change.

When GroupWise users send messages to the group, only those group members who have GroupWise accounts receive messages.

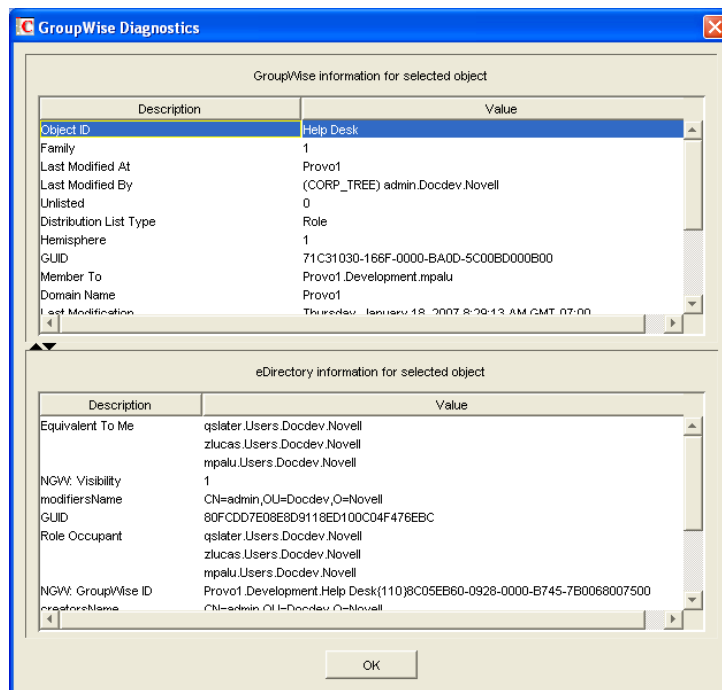
For information about using dynamic groups with GroupWise, see TID 3074853 in the [Novell Support Knowledgebase](http://www.novell.com/support) (<http://www.novell.com/support>).

19.2 Seeing Which Members of an eDirectory Group Have GroupWise Accounts

eDirectory groups can include members who have GroupWise accounts and members who do not have GroupWise accounts. When the group is used to address a message, only those members who have GroupWise accounts receive the message.

To see which members have GroupWise accounts and which ones do not:

- 1 In ConsoleOne, select the Group object, then click *Tools > GroupWise Diagnostics > Display Object*.



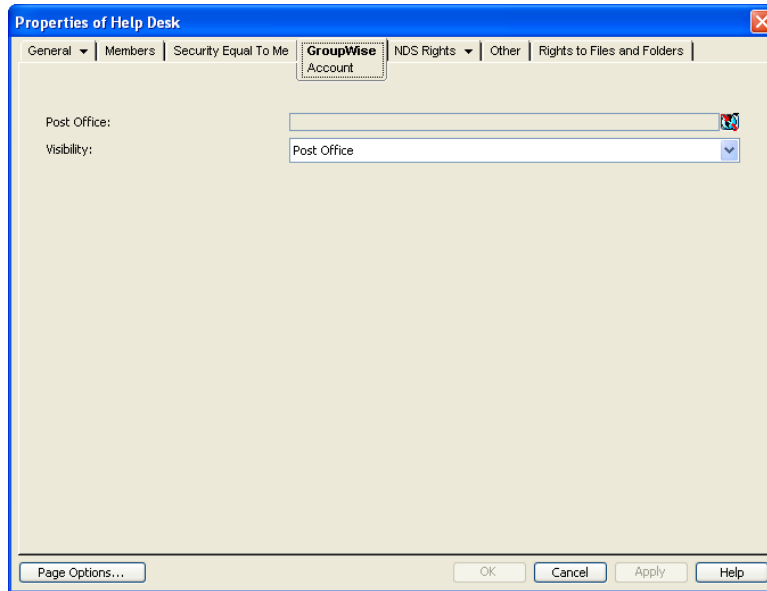
The *Member To* field in the top window displays the members who have GroupWise accounts. The *Role Occupant* field in the bottom window displays all members.

- 2 When you have finished viewing the information, click *OK*.

19.3 Changing a Group's Visibility in the Address Book

An eDirectory group's visibility level determines which users see the group in the Address Books. You can control the availability of a group by displaying it in the Address Book for all users in your GroupWise system, in the Address Book for those users in the group's domain only, in the Address Book for those users on the group's post office only, or not displaying it at all.

- 1 In ConsoleOne, right-click the Group object, then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page:



- 3 In the *Visibility* field, select the desired visibility level.
System: The group is displayed in the Address Book for all users in your GroupWise system.
Domain: The group is displayed in the Address Book for all users in the group's domain.
Post Office: The group is displayed in the Address Book for all users on the group's post office.
None: The group is not displayed in the Address Book.
- 4 Click *OK* to save your changes.

19.4 Moving a Group

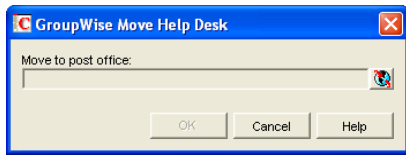
If necessary, you can move an eDirectory group from one post office to another. For example, you might need to move a group from a post office you are removing.

The group retains the same name on the new post office as it has on the current post office. If another object (user, resource, distribution list, group, or organizational role) assigned to the new post office has the same name, you must rename one of them before you move the group. For details, see [Section 18.5, "Renaming a Distribution List," on page 291](#).

To move an eDirectory group from one post office to another:

- 1 In ConsoleOne, right-click the Group object in the GroupWise View, then click *Move* to display the GroupWise Move dialog box.

IMPORTANT: You must select the eDirectory Group object in the GroupWise View by listing GroupWise distribution lists. If you select the Group object in the standard Console View, you move the Group object from one eDirectory container to another, not the group/distribution list from one post office to another.



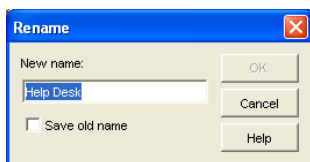
- 2 Select the post office to which you want to move the group, then click *OK* to move the group.

19.5 Renaming a Group

Situations might arise where you need to give an eDirectory group a new name. For example, you might need to move the group to another post office that already has an object (user, resource, distribution list, group, or organizational unit) with the same name.

When you rename an eDirectory group, you rename the Group object. This means that not only are you changing the name in GroupWise, but also in eDirectory.

- 1 In ConsoleOne, right-click the Group object, then click *Rename* to display the Rename dialog box.



- 2 In the *New Name* field, specify the new name for the group.
- 3 Make sure the *Save Old Name* box is not selected. Saving the old name causes duplicate groups to appear in the Address Book.
- 4 Click *OK* to rename the group.

19.6 Removing a Group from GroupWise

If you decide that you no longer want an eDirectory group to be a distribution list in GroupWise, you can remove its association with a GroupWise post office, so that it returns to being just an eDirectory group.

- 1 In ConsoleOne, right-click the Group object, click *Delete*, then click *Yes* to confirm that you want to delete the object.
- 2 In the eDirectory Account box, deselect *Delete* to retain the Group object in eDirectory.
The *Delete* option in the GroupWise Account box is selected by default and cannot be deselected.
- 3 Click *OK* twice to complete the deletion.

20 Using eDirectory Organizational Roles as GroupWise Distribution Lists

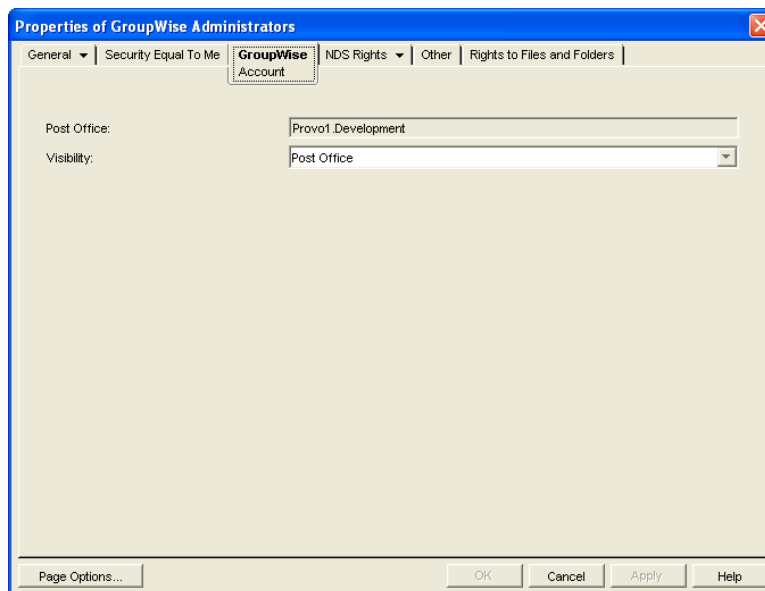
Organizational roles can be configured to function as GroupWise distribution lists.

- ♦ Section 20.1, “Setting Up an Organizational Role for Use in GroupWise,” on page 307
- ♦ Section 20.2, “Seeing Which Members of an Organizational Role Have GroupWise Accounts,” on page 308
- ♦ Section 20.3, “Changing an Organizational Role’s Visibility in the Address Book,” on page 309
- ♦ Section 20.4, “Moving an Organizational Role,” on page 310
- ♦ Section 20.5, “Renaming an Organizational Role,” on page 310
- ♦ Section 20.6, “Removing an Organizational Role from GroupWise,” on page 311

20.1 Setting Up an Organizational Role for Use in GroupWise

By default, Novell eDirectory organizational roles are not automatically available for use as distribution lists in GroupWise. To make an organizational role available, you need to assign it to a GroupWise post office.

- 1 In ConsoleOne, right-click the Organizational Role object, then click *Properties*.
- 2 Click the *GroupWise* tab to display the Account page.



- 3 Fill in the following fields:

Post Office: Select the post office where you want to assign the organizational role. You can choose any post office you want. If you plan to limit visibility of the organizational role to users on a specific post office or in a specific domain, you should select that post office or a post office in the desired domain.

Visibility: Select the level at which the role is visible in the Address Book. *System* enables the role to be visible to all users in your GroupWise system. *Domain* enables the role to be visible to all users in the same domain as the role. *Post Office* enables the role to be visible to all users on the same post office as the role. Setting the visibility to *None* means that the role is not visible at any level. However, even if the role is not displayed in a user's Address Book, he or she can use the role by typing the role's name in a message's To field.

- 4 Click *OK* to save the changes.

The organizational role is now treated like a GroupWise distribution list and is visible in the GroupWise View when you filter on distribution lists. However, its icon does not change.

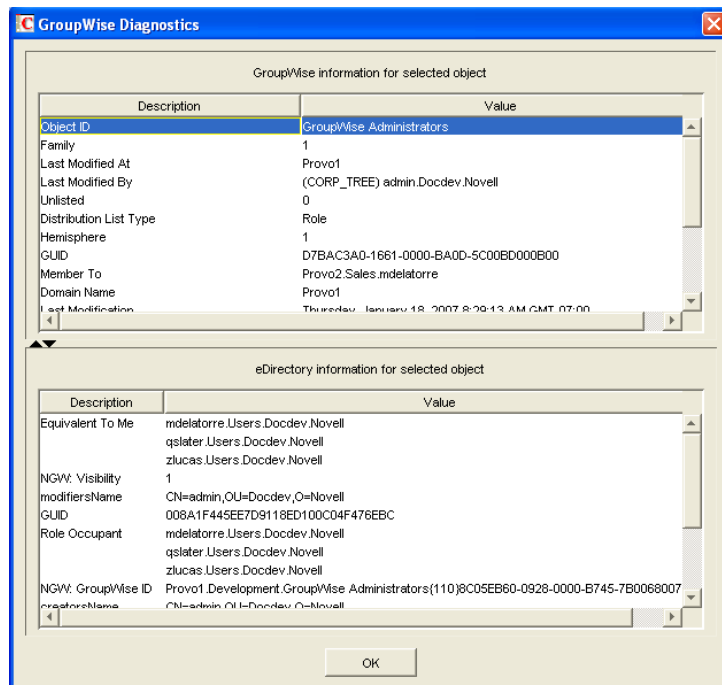
When GroupWise users send messages to the organization role, only those role members who have GroupWise accounts receive messages.

20.2 Seeing Which Members of an Organizational Role Have GroupWise Accounts

eDirectory organizational roles can include members who have GroupWise accounts and members who do not have GroupWise accounts. When the organizational role is used to address a message, only those members who have GroupWise accounts receive the message.

To see which members have GroupWise accounts and which ones do not:

- 1 In ConsoleOne, select the Organizational Role object, then click *Tools > GroupWise Diagnostics > Display Object*.



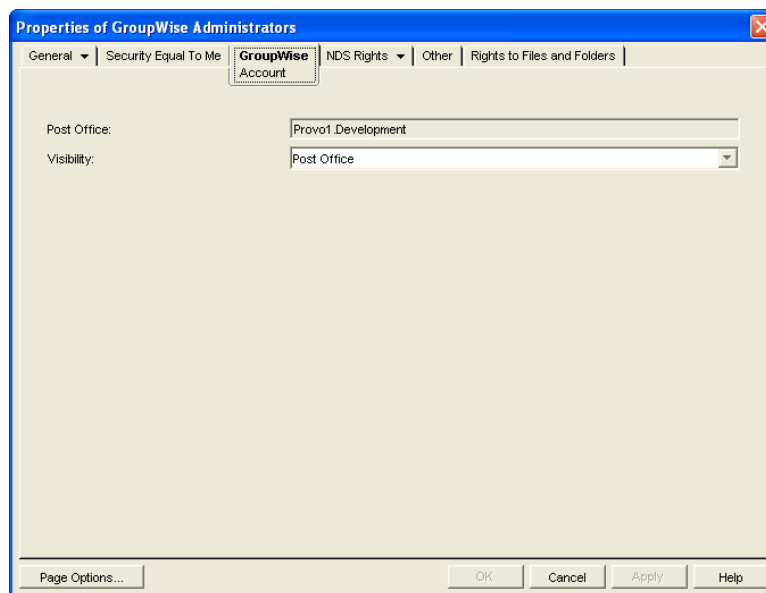
The top window displays the members who have GroupWise accounts. The bottom window displays all members.

- 2 When you have finished viewing the information, click *OK*.

20.3 Changing an Organizational Role's Visibility in the Address Book

An organizational role's visibility level determines which users see the role in the Address Books. You can control the availability of a role by displaying it in the Address Book for all users in your GroupWise system, in the Address Book for those users in the role's domain only, in the Address Book for those users on the role's post office only, or not displaying it at all.

- 1 In ConsoleOne, right-click the Organizational Role object, then click *Properties*.
- 2 Click *GroupWise > Account* to display the Account page:



- 3 In the *Visibility* field, select the desired visibility level.

System: The organizational role is displayed in the Address Book for all users in your GroupWise system.

Domain: The organizational role is displayed in the Address Book for all users in the role's domain.

Post Office: The organizational role is displayed in the Address Book for all users on the role's post office.

None: The organizational role is not displayed in the Address Book.

- 4 Click *OK* to save your changes.

20.4 Moving an Organizational Role

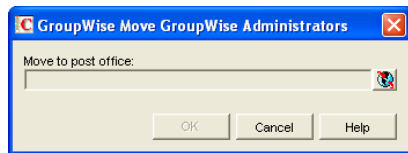
If necessary, you can move an organizational role from one post office to another. For example, you might need to move an organizational role from a post office you are removing.

The organizational role retains the same name on the new post office as it has on the current post office. If another object (user, resource, distribution list, group, or organizational role) assigned to the new post office has the same name, you will need to rename one of them before you move the organizational role. For details, see [Section 18.5, “Renaming a Distribution List,” on page 291](#).

To move an organizational role from one post office to another:

- 1 In ConsoleOne, right-click the Organizational Role object in the GroupWise View, then click *Move* to display the GroupWise Move dialog box.

IMPORTANT: You must select the Organizational Role object in the GroupWise View by listing GroupWise distribution lists. If you select the Organizational Role object in the standard Console View, you move the Organizational Role object from one eDirectory container to another, not the organizational role/distribution list from one post office to another.



- 2 Select the post office to which you want to move the organizational role, then click *OK* to move the organizational role.

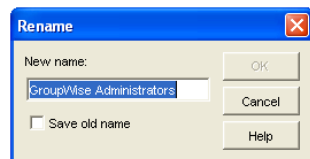
20.5 Renaming an Organizational Role

Situations might arise where you need to give an organizational role a new name. For example, you might need to move the organizational role to another post office that already has an object (user, resource, distribution list, group, or organizational unit) with the same name.

When you rename an organizational role, you rename the Organizational Role object. This means that you are not only changing the name in GroupWise, but also in eDirectory.

To rename an organizational role:

- 1 In ConsoleOne, right-click the Organizational Role object, then click *Rename* to display the GroupWise Rename dialog box.



- 2 In the *New Name* field, specify the new name for the organizational role.
- 3 Click *OK* to rename the organizational role.

20.6 Removing an Organizational Role from GroupWise

If you decide that you no longer want an organizational role to be a public address list in GroupWise, you can remove its association with a GroupWise post office, so that it returns to being just an eDirectory organizational role.

- 1 In ConsoleOne, right-click the Organizational Role object, click *Delete*, then click *Yes* to confirm that you want to delete the object.
- 2 In the eDirectory Account box, deselect *Delete* to retain the Organizational Role object in eDirectory.
The *Delete* option in the GroupWise Account box is selected by default and cannot be deselected.
- 3 Click *OK* twice to complete the deletion.

VII Libraries and Documents

- ♦ [Chapter 21, “Document Management Services Overview,” on page 315](#)
- ♦ [Chapter 22, “Creating and Managing Libraries,” on page 323](#)
- ♦ [Chapter 23, “Creating and Managing Documents,” on page 359](#)
- ♦ [Chapter 24, “Integrations,” on page 387](#)

21 Document Management Services Overview

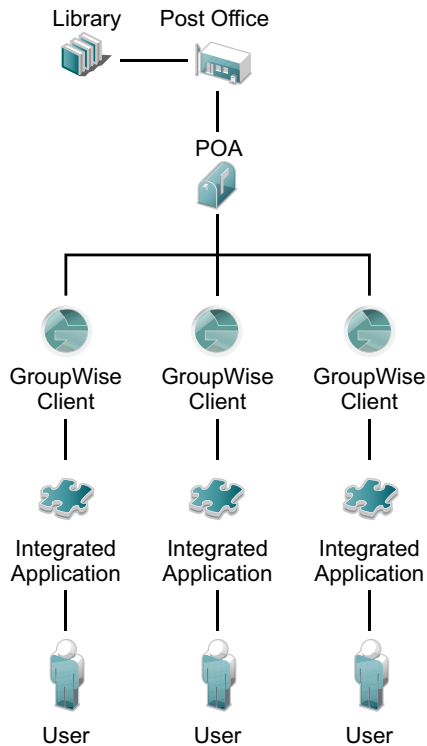
GroupWise Document Management Services (DMS) lets users create documents with integrated applications, save them, then easily locate a specific document later without knowing the application, a specific document name, or the document's physical location. Users can create, share, locate, edit, view, and check out documents that are created under the management of GroupWise DMS.

A GroupWise DMS system consists of the following components:

- ♦ [Section 21.1, "Libraries," on page 316](#)
- ♦ [Section 21.2, "Document Storage Areas," on page 317](#)
- ♦ [Section 21.3, "Documents," on page 318](#)
- ♦ [Section 21.4, "Integrations," on page 321](#)

21.1 Libraries

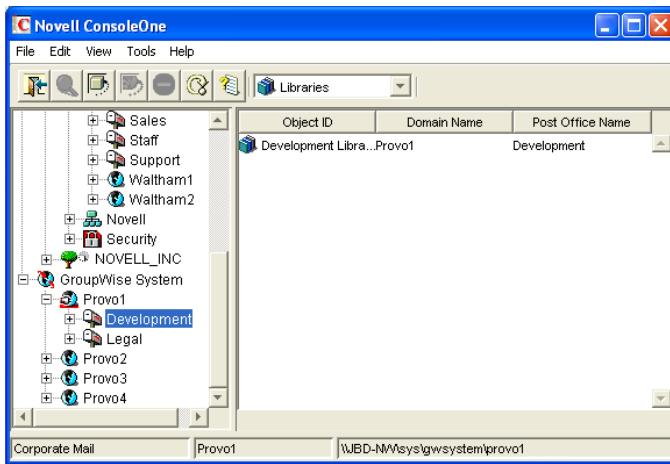
A library is a set of documents and a database that allows the documents to be managed as a unit. A library must belong to a specific post office but can be accessed by users in other post offices. The GroupWise client enables users to store and manage their documents in the library. The GroupWise Post Office Agent (POA) transfers documents between the GroupWise client and the library.



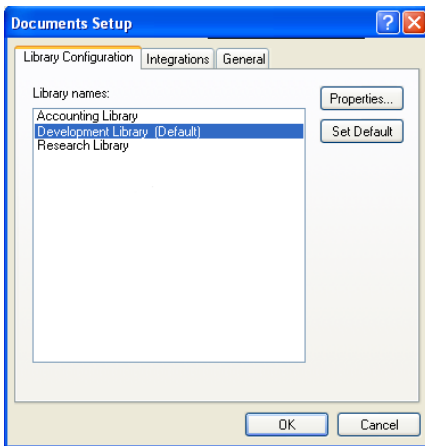
In ConsoleOne, a library can be viewed where it resides in the Novell eDirectory tree.



A library can also be viewed in relationship to the post office that owns it.



In the GroupWise Windows client, users can view a list of all the libraries to which they have access by clicking *Tools > Options > Documents*.



Physically, a library consists of a set of directories and databases stored in the `gwdms` subdirectory of the post office, as illustrated in “*Post Office Directory*” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

For complete information on libraries, see [Chapter 22, “Creating and Managing Libraries,”](#) on [page 323](#).

21.2 Document Storage Areas

Documents can be stored at the post office, as illustrated in “*Post Office Directory*” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*. This is the simplest configuration, but it is not recommended for libraries where substantial growth is anticipated because documents stored at the post office cannot easily be moved to a different location where additional storage space is available.

Preferably, documents should be stored outside the post office, in document storage areas. Document storage areas are physical locations, such as drive volumes, optical devices, hard drives on other servers, and so on. Document storage areas can be located anywhere that the POA can access them locally or using direct network access (mapped drive or mounted file system).

A document storage area has the same internal directory structure that is used to store documents at the post office. The only difference is that a document storage area can be located anywhere in your system. Therefore, a document storage area can be moved easily, so it is easy to expand your document storage capacity if you store documents in a document storage area rather than at the post office.

For complete information on document storage areas, see [Section 22.6.2, “Managing Document Storage Areas,”](#) on page 345.

21.3 Documents

Documents created using GroupWise DMS are not stored as individual files. Instead, documents are stored in database structures called binary large objects (BLOBs). A document and all of its versions are stored in the separate BLOB files. BLOBs are compressed (50% or more) to conserve storage space. BLOBs are encrypted to provide security.

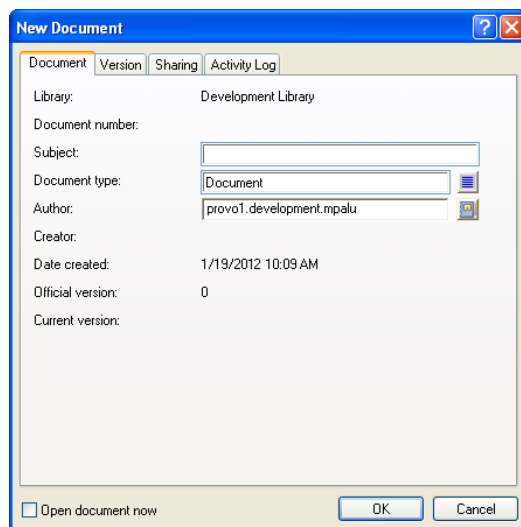
Because documents are stored in a database structure, information can be associated with each document that is not part of the document itself, such as:

- ◆ [Section 21.3.1, “Document Properties,”](#) on page 318
- ◆ [Section 21.3.2, “Document Types,”](#) on page 319

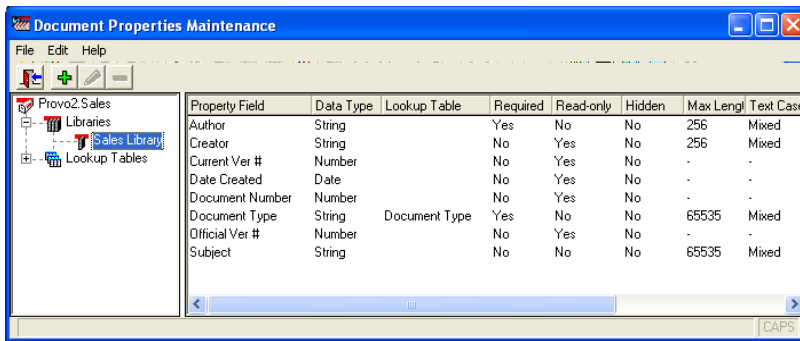
For complete information on documents, see [Chapter 23, “Creating and Managing Documents,”](#) on page 359.

21.3.1 Document Properties

Document properties are attributes that determine what users see on the document property sheets when they create DMS documents. In the GroupWise Windows client, the default document properties for a new document appear like this:



In ConsoleOne, the default document properties for a library are defined like this:

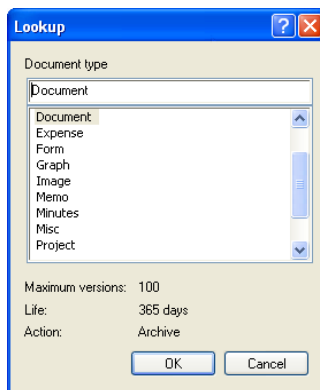


The default document properties are often adequate, but for some libraries, additional customized document properties can be very useful. For example, the legal department might want Client and Matter fields to be required for most documents created by anyone in that department.

NOTE: Document properties cannot be set in ConsoleOne on Linux. However, you can use ConsoleOne on Windows to set document properties for libraries that are located on Linux.

21.3.2 Document Types

The Document Type property defines how a document is disposed of when its “life” in the system has expired. It is a required field. Users select a document type each time they create a new document.



A number of default document types are provided, as shown above. If needed, you can set up additional document types. For example, you could set up Pleading for the legal department, Spreadsheet for accounting, Correspondence for administration, RFP for marketing, White Paper for R&D, and so on.

The document type establishes the following document characteristics:

- ◆ “Maximum Versions” on page 320
- ◆ “Document Life” on page 320
- ◆ “Expiration Actions” on page 320

The following table lists some of the default document types and their default characteristics:

Document Type	Maximum Versions	Expiration Action	Document Life
Agenda	100	Archive	99 days
Document	100	Archive	365 days
Memo	1	Delete	99 days
Minutes	100	Archive	99 days
Misc	10	Archive	30 days
Proposal	100	Archive	99 days
Report	100	Archive	99 days
Template	100	Archive	365 days

Maximum Versions

Users can create new versions of their documents when they revise them. Version numbers are automatically incremented.

Any version of a document can be designated as the official version by the user. The official version, which is not necessarily the most recently edited version, is the one located in searches. GroupWise users have the right to designate an official version if they have Edit rights to the document.

Each document type property has a maximum number of versions (up to 50,000 per document). Most types have a default of 99 versions. A maximum of 0 (zero) versions means that documents of that type cannot have versions.

Document Life

Document life is the number of days that must pass between the time when a document is last accessed and when it is ready for archival or deletion. A document life value of 0 (zero) indicates that the document will never be available for archival or deletion.

Expiration Actions

When a document's life expires, its associated expiration action takes place:

Archive: The document is archived when it reaches its document life date. This is useful for important documents because archived documents can be unarchived.

Delete: The document is automatically deleted when its document life date is reached. This is useful for documents that are temporary in nature.

Retain: The document is not deleted or archived, and remains in the system indefinitely. This option is practical for documents that have a recurring use, such as template documents.

21.4 Integrations

Integrations serve as the “glue” between document-producing applications and your GroupWise DMS system. Integrations provide code specifically designed to allow function calls, such as Open or Save, to be redirected to the GroupWise Windows client. This allows GroupWise dialog boxes to be displayed instead of the application’s normal dialog boxes for the integrated functions. Integrations also allow GroupWise to pull documents from a library and deliver them to applications for modification. Then, integrations enable GroupWise to return modified documents to the library so that other users can access them.

For complete information on the integrations available for the Windows client, see [Chapter 24, “Integrations,”](#) on page 387.

22 Creating and Managing Libraries

When you first set up a new GroupWise system, a basic library is automatically created for the first post office. A basic library is adequate when:

- ◆ Document management is not a primary activity of your GroupWise users.
- ◆ The library will store documents created and used by members of the post office that owns the library, or, if you do not need one basic library per post office, by all users within a domain.
- ◆ All documents will be stored at the post office or in a single document storage area external to the post office that owns the library.

If your anticipated document management needs are more demanding than those listed above, you can set up one or more full-service libraries, where you can implement the full range of document management capabilities offered by GroupWise Document Management Services (DMS).

NOTE: The Linux version of ConsoleOne allows you to create libraries, but it does not allow you to set document properties as described in [Section 23.2, “Organizing Documents in Libraries,”](#) on page 362.

To use one or more libraries as part of your GroupWise system, perform the following tasks as needed:

- ◆ [Section 22.1, “Planning a Basic Library,”](#) on page 324
- ◆ [Section 22.2, “Setting Up a Basic Library,”](#) on page 326
- ◆ [Section 22.3, “Planning Full-Service Libraries,”](#) on page 328
- ◆ [Section 22.4, “Setting Up a Full-Service Library,”](#) on page 338
- ◆ [Section 22.5, “Viewing a New Library in Your GroupWise System,”](#) on page 341
- ◆ [Section 22.6, “Managing Libraries,”](#) on page 342
- ◆ [Section 22.7, “Library Worksheets,”](#) on page 355

IMPORTANT: If you are creating a new library in a clustered GroupWise system, see the [GroupWise 2012 Interoperability Guide](#) before you create the library.

22.1 Planning a Basic Library

An initial basic library was created along with the first post office when you set up your GroupWise system. That initial basic library is available for immediate use. However, you might want to change the location where documents are stored, as described in [Section 22.1.4, “Deciding Where to Store Documents,” on page 325](#). You can also create additional basic libraries as needed.

This section provides the information you need in order to set up a new basic library. [Section 22.7.1, “Basic Library Worksheet,” on page 355](#) lists all the information you need as you set up a basic library. You should print the worksheet and fill it out as you complete the tasks listed below:

- ♦ [Section 22.1.1, “Selecting the Post Office That the Library Will Belong To,” on page 324](#)
- ♦ [Section 22.1.2, “Determining the Context for the Library Object,” on page 324](#)
- ♦ [Section 22.1.3, “Choosing the Library Name,” on page 324](#)
- ♦ [Section 22.1.4, “Deciding Where to Store Documents,” on page 325](#)

After you have completed the tasks and filled out the worksheet, you are ready to continue with [Section 22.2, “Setting Up a Basic Library,” on page 326](#).

22.1.1 Selecting the Post Office That the Library Will Belong To

If you are creating a basic library for each post office in your GroupWise system, print a copy of [Section 22.7.1, “Basic Library Worksheet,” on page 355](#) for each post office.

If users in several post offices will store documents in the same basic library, you must decide which post office should own the library. A library can never be reassigned to a different post office, so you should choose the owning post office carefully. You should consider which users will use the library most frequently and where you might want to create additional libraries in the future.

BASIC LIBRARY WORKSHEET

Under [Item 3: Post Office](#), specify the name of the post office that will own the new basic library.

22.1.2 Determining the Context for the Library Object

Generally, you should create the Library object in the same context as its post office. You cannot move a Library object after you have created it.

BASIC LIBRARY WORKSHEET

Under [Item 1: eDirectory Container](#), specify the container for the Library object.

22.1.3 Choosing the Library Name

When you create the Library object, you must give the library a name. This is the name that is displayed in ConsoleOne.

After you have specified the library’s name and created the Library object, the name cannot be changed. Therefore, if you have or will have other libraries, you should pick a name that uniquely identifies the library. For example, use the name to identify the post office it is assigned to.

Do not use any of the following invalid characters in the library's name:

ASCII characters 0-31	Comma ,
Asterisk *	Double quote "
At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

By default, the library name that users see in the GroupWise client is the same as the Library object name. However, you can change the display name if you want it to be different from the Library object name.

BASIC LIBRARY WORKSHEET

Under [Item 2: Library Name](#), specify the Library object name.

Under [Item 7: Library Description](#), provide a brief description of the planned use for the library.

Under [Item 8: Display Name](#), specify the library name you want users to see in the GroupWise client, if it is different from the Library object name.

22.1.4 Deciding Where to Store Documents

You can store documents at the post office in the `post_office\gwdms\library\docs` subdirectory of the post office. You can later add document storage areas outside the post office if DMS usage grows. However, the documents stored at the post office can never be moved.

A document storage area has the same internal directory structure that is used to store documents at the post office, but it can be located anywhere in your system. Document storage areas can be moved easily, so it is easy to expand your document storage capacity when you store documents in document storage areas rather than at the post office.

You might want to set up a document storage area on the same server where the POA runs so as not to increase network traffic. The POA can index and serve documents to users most efficiently if the document storage area is located locally.

BASIC LIBRARY WORKSHEET

Under [Item 4: Store Documents at the Post Office?](#), mark Yes or No. (No is recommended for permanent document storage).

To define a document storage area, you must know its direct access path. For example, a UNC path specifies the absolute location of the document storage directory.

```
\\Windows_server\sharename\storage_directory
```

For example:

```
\\win7\c$\docs
```

NOTE: On Linux, ConsoleOne interprets a UNC path so that the first item in the UNC path is the Linux server hostname, followed by a Linux path to the document storage area.

BASIC LIBRARY WORKSHEET

If you entered No for [Item 4](#), specify the direct access path under [Item 6: Document Storage Area Path](#).

Under [Item 5: Document Storage Area Description](#), enter a useful description of the document storage area. (This description is displayed only in ConsoleOne.)

If you need to add a document storage area to the initial library that was created with the first post office in your GroupWise system, use the Storage Areas properties page of the Library object in ConsoleOne to provide the direct access path, as described in [“Adding a Document Storage Area” on page 345](#).

22.2 Setting Up a Basic Library

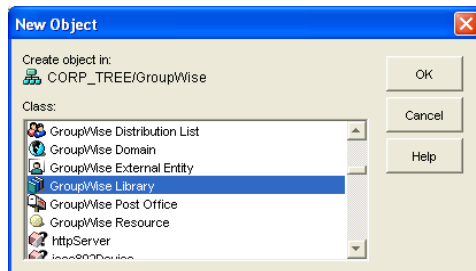
You should already have reviewed [Section 22.1, “Planning a Basic Library,” on page 324](#) and filled out [Section 22.7.1, “Basic Library Worksheet,” on page 355](#). Complete the following tasks to set up a new basic library:

- ♦ [Section 22.2.1, “Creating the Basic Library,” on page 326](#)
- ♦ [Section 22.5, “Viewing a New Library in Your GroupWise System,” on page 341](#)

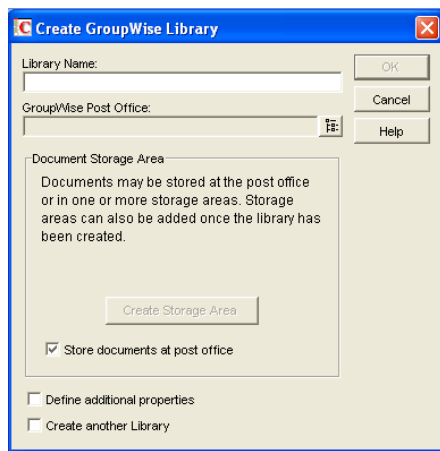
22.2.1 Creating the Basic Library

To create a new library:

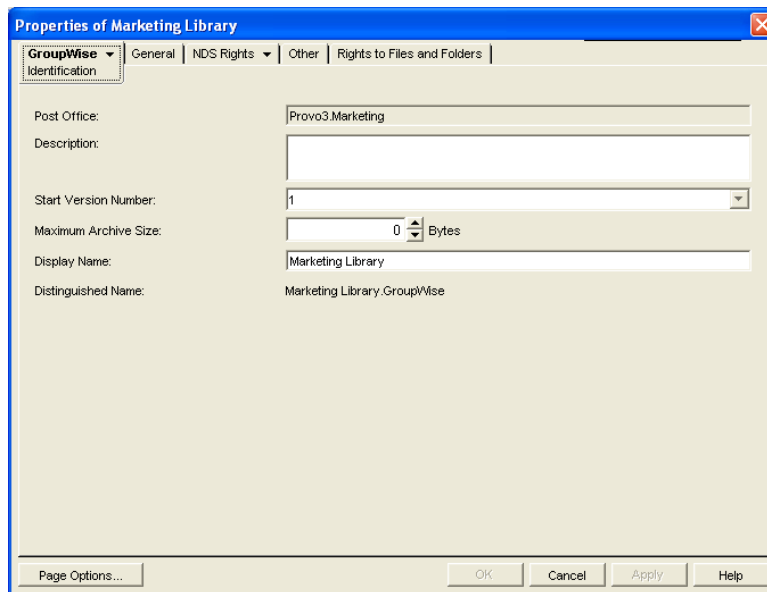
- 1 Make sure the POA is running for the post office that will own the new basic library.
- 2 In ConsoleOne, browse to and right-click the Novell eDirectory container where you want to create the library ([worksheet item 1](#)), then click *New > Object*.



- 3 Double-click *GroupWise Library*, then fill in the fields in the Create GroupWise Library dialog box ([worksheet items 2 through 6](#)).



- 4 Click *Define Additional Properties*, then click *OK* to create the Library object and display the library Identification page.



- 5 Fill in the *Description* field ([worksheet item 7](#)).
- 6 If necessary, edit the *Display Name* field ([worksheet item 8](#)).
- 7 Click *OK* to save the library information.
- 8 Test the new library. See [Section 22.5, "Viewing a New Library in Your GroupWise System,"](#) on [page 341](#).

Although there are many configuration options for libraries and documents, as described in [Section 22.3, "Planning Full-Service Libraries,"](#) on [page 328](#), no additional setup is required for a basic library. GroupWise client users can begin to store documents in the new library at once.

22.3 Planning Full-Service Libraries

If your document management requirements go beyond basic libraries, you can create one or more full-service libraries. You might or might not need to make use of all document management features in order to meet your DMS users' needs.

This section covers everything you should consider when you set up full-service libraries. The [“Full-Service Library Worksheet” on page 356](#) lists all the information you need as you set up a full-service library. You should print a copy of the worksheet for each library you plan to create. Fill out the worksheet for each library as you complete the tasks listed below.

- ♦ [Section 22.3.1, “Deciding Which Libraries to Create,” on page 328](#)
- ♦ [Section 22.3.2, “Selecting the Post Offices To Own Libraries,” on page 332](#)
- ♦ [Section 22.3.3, “Determining the Contexts for Library Objects,” on page 332](#)
- ♦ [Section 22.3.4, “Choosing Library Names,” on page 332](#)
- ♦ [Section 22.3.5, “Deciding Where to Store Documents,” on page 333](#)
- ♦ [Section 22.3.6, “Setting Document Version Options,” on page 335](#)
- ♦ [Section 22.3.7, “Figuring Maximum Archive Directory Size,” on page 335](#)
- ♦ [Section 22.3.8, “Designating Initial Librarians,” on page 336](#)
- ♦ [Section 22.3.9, “Restricting Initial Public Library Rights,” on page 337](#)
- ♦ [Section 22.3.10, “Determining Your Indexing Needs,” on page 338](#)
- ♦ [Section 22.3.11, “Determining If You Need to Set Up Integrations for DMS Users,” on page 338](#)

After you have completed the above tasks and filled out the worksheets, you are ready to continue with [Section 22.4, “Setting Up a Full-Service Library,” on page 338](#).

22.3.1 Deciding Which Libraries to Create

When designing a system of libraries for your GroupWise system, you should review the following considerations:

- ♦ [“Library Access for DMS Users” on page 328](#)
- ♦ [“Centralized vs. Decentralized Library Configurations” on page 328](#)
- ♦ [“Library Specialization” on page 331](#)

Library Access for DMS Users

Client/server access is the preferred access mode for GroupWise client users. It is the best access mode for DMS users because it enables them to access libraries outside their own post offices.

For information about access modes, see [Section 35.4, “Post Office Access Mode,” on page 476](#).

Centralized vs. Decentralized Library Configurations

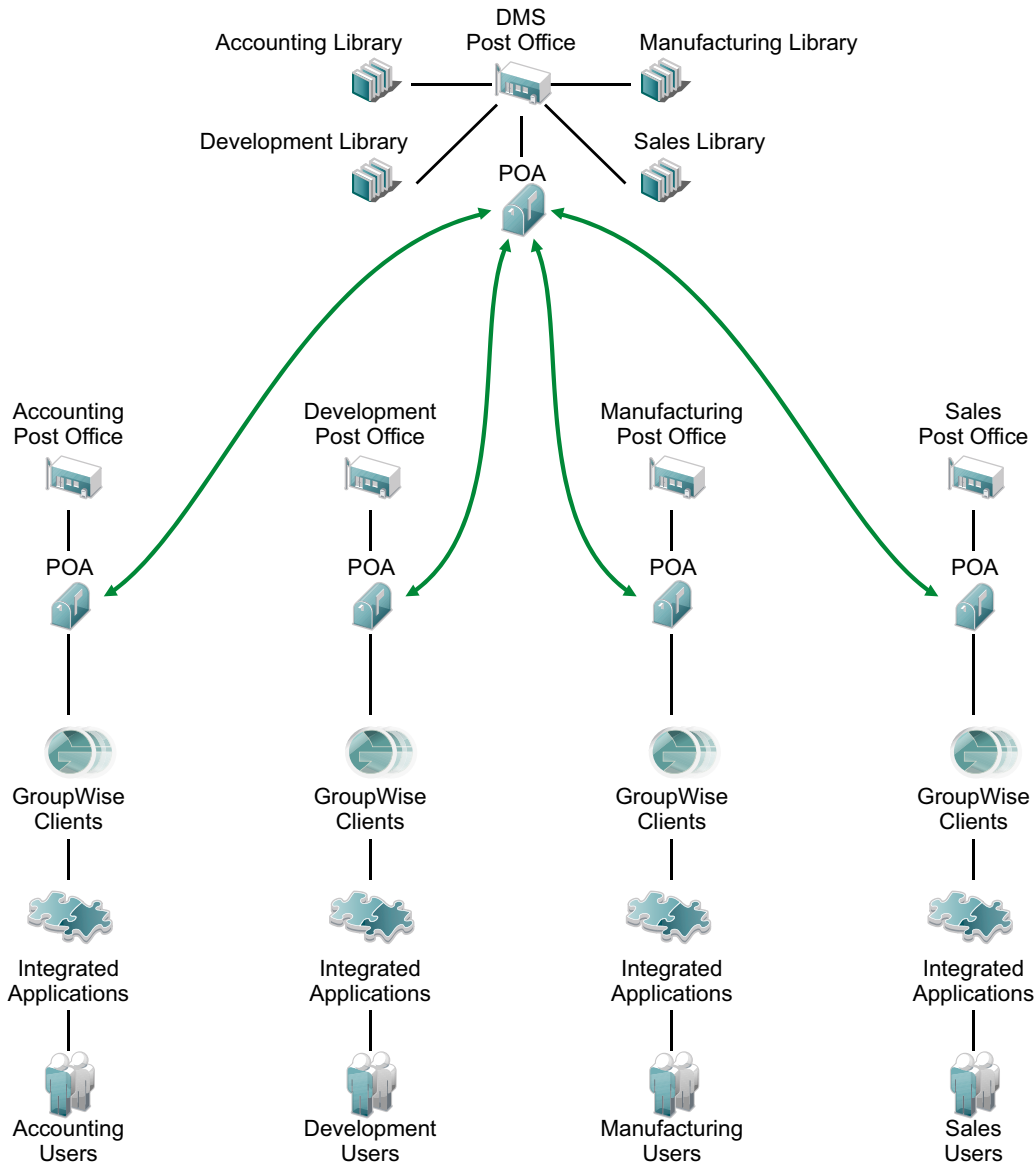
Reorganizing existing libraries is not a simple process. Therefore, you should determine whether you want a centralized or decentralized library configuration before you start creating libraries.

- ♦ [“Centralized Libraries” on page 329](#)
- ♦ [“Decentralized Libraries” on page 330](#)
- ♦ [“Comparative Scenarios” on page 331](#)

Centralized Libraries

Centralized libraries are located in a post office that is dedicated to libraries (no users). Centralized libraries are serviced by the POA in the dedicated DMS post office, as shown in the following illustration:

Figure 22-1 *Centralized Libraries*



In the illustration, notice that all libraries belong to the DMS post office, which has no users. All GroupWise client users are using client/server access mode, which is required because there are no libraries in their local post offices. Each user has access to all four libraries through TCP/IP links to the DMS POA.

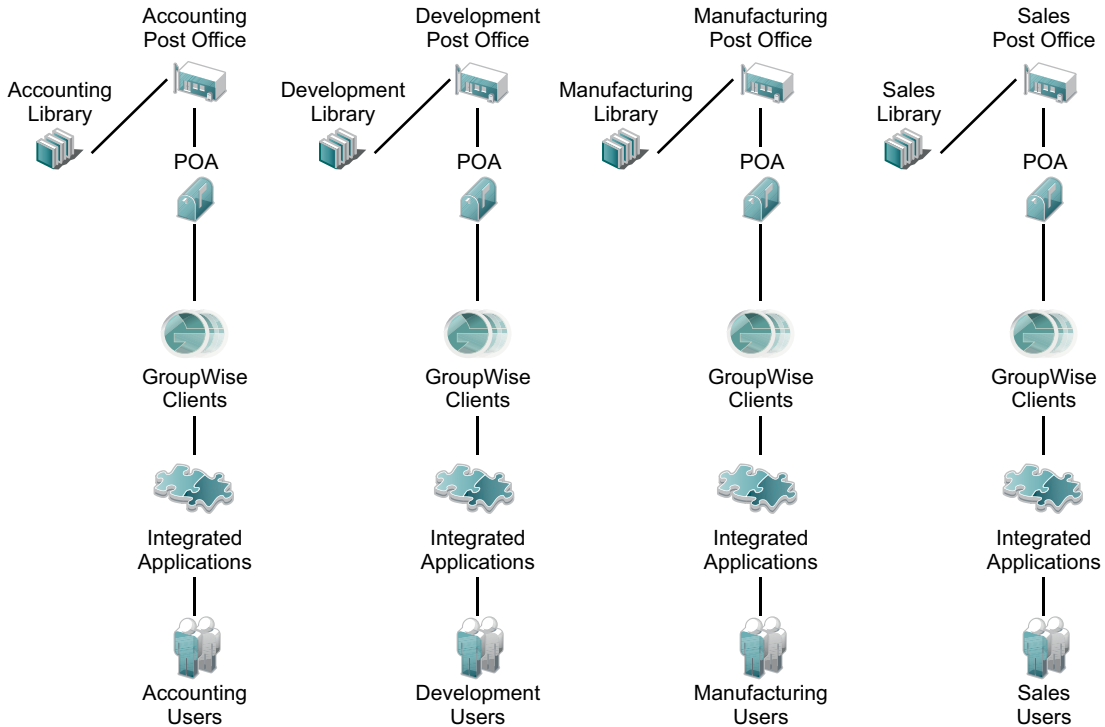
The following table lists some advantages and disadvantages of centralized libraries:

Advantages	Disadvantages
<ul style="list-style-type: none"> ◆ Administration can be consolidated, allowing one administrator to specialize in document management. ◆ Backup can be easier with hardware dedicated to one DMS post office, such as optical drives, RAID, fast backup units, and so on. ◆ If a post office server other than the one dedicated to libraries goes down, DMS access is unaffected for users in the remaining post offices. 	<ul style="list-style-type: none"> ◆ You must create and maintain a post office that is dedicated to libraries only (no users). ◆ This configuration guarantees that all document searching and accessing is back and forth between users' post offices and the libraries' post office, possibly degrading network performance. ◆ If the post office server dedicated to libraries goes down, DMS is unusable for the whole GroupWise system.

Decentralized Libraries

Decentralized libraries are located along with users in different post offices. Decentralized libraries are serviced by their own local POAs as shown in the following illustration:

Figure 22-2 Decentralized Libraries



In the illustration, notice that each post office has its own library. Users can see each others' libraries as well as their own because of client/server access mode.

The following table lists some advantages and disadvantages of decentralized libraries

Advantages	Disadvantages
<ul style="list-style-type: none"> ◆ Network traffic is minimized because most document accessing are in users' local post offices. ◆ You do not need to maintain an extra DMS post office dedicated to libraries only. ◆ Users in a post office where a library resides can use direct access mode if necessary. 	<ul style="list-style-type: none"> ◆ Libraries and their documents are scattered over different servers, adding to your administrative workload (such as doing backups).

Comparative Scenarios

The following scenarios further illustrate the differences between centralized and decentralized libraries:

- ◆ Assume that you assigned your first library to the same post office your users have membership in. By initially assigning a library to the same post office as your users, you establish a decentralized configuration for future libraries. You now want a centralized library configuration. However, because you cannot reassign the library to another post office, you must do one of the following:
 - ◆ Create one or more new libraries under a DMS post office, export all of the documents from the first library and import them to the new libraries, delete the first library, and then ensure that users can locate their documents.
 - ◆ Create one or more new libraries under a DMS post office and have your librarian use mass document operations to move the documents from the first library to the other libraries, delete the first library, and then ensure that users can locate their documents.
- ◆ Assume that you assigned your first library to a DMS post office that is used only for libraries. Now you can use either the centralized or decentralized library configuration for your additional libraries. The DMS post office can be used for all future libraries to create a centralized configuration, or you could assign future libraries to other post offices and leave that first one where it is, giving you a decentralized configuration. Setting up your first library on a post office server dedicated to only libraries allows you to use either configuration option. However, this method initially requires additional hardware and administration.

Library Specialization

You can create libraries for such user specialties as administration, accounting, development, human resources, legal, marketing, manufacturing, payroll, R&D, sales, shipping, and so on. You can also specialize libraries by such functions as general (for all users), administration (including legal and payroll), engineering and documentation development (R&D), marketing and sales, manufacturing and shipping, and so on.

You can also use specialization to provide security for sensitive libraries. You do this by setting up access restrictions for the libraries. The default is for all DMS users to have access to all libraries in the GroupWise system. For more information about restricting library access, see [Section 22.6.3, "Managing Library Access," on page 348](#).

Restricting library access can also improve users' search time. When users install the GroupWise client on their workstations, they are either automatically assigned a default library (if there is one on their post office), or they are asked to select one from the libraries they have access to. By default, DMS searches are performed only on the user's default library. To search other libraries ("global" search), users can select other libraries using the Look In list in the Find dialog box. If you limit users' access to libraries (perhaps by department), their global searches would also be faster.

Another reason for creating specialized libraries could be for different library configuration needs. For example, each library could have specialized document types and document properties that would not be needed in other libraries. For a review of document types and properties, see [Section 21.3, “Documents,” on page 318](#). For more detailed information, see [“Customizing the Default Document Type Property” on page 363](#) and [Section 23.2.1, “Customizing Document Properties,” on page 362](#).

Specialization can also facilitate library management activities, such as controlling library accessibility for individual users or groups of users, or managing different uses of document types, document properties, or field label naming schemes.

22.3.2 Selecting the Post Offices To Own Libraries

As a result of deciding whether you want to use a centralized or decentralized configuration for your libraries and whether or not you need specialized libraries, you should have a good idea of what post offices you want to create libraries in.

If you are using a centralized configuration, create the DMS post office by following the instructions in [Chapter 11, “Creating a New Post Office,” on page 173](#), then return to this point.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 3: Post Office](#), specify the name of the post office that will own the new library.

22.3.3 Determining the Contexts for Library Objects

You can create a Library object in any container in the eDirectory tree. For example, you could create the Library object in the same container as its Post Office object. Or you could create it in a special container just for Library objects:

The containers in which you place the Library objects have no bearing on whether your libraries are centralized or decentralized. Library objects can be located anywhere in the tree, no matter which post offices the libraries belong to.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 1: eDirectory Container](#), specify the name of the eDirectory container where you want to create the new library.

22.3.4 Choosing Library Names

A library's name must be unique within the post office; it also must be unique within its container. You should devise a naming scheme that helps to identify all libraries in the GroupWise system. It can be useful to include within the library name an indication of which post office it belongs to.

After you have specified the library's name and created the Library object, the name cannot be changed.

Do not use any of the following invalid characters in the library's name:

ASCII characters 0-31	Comma ,
Asterisk *	Double quote "

At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

By default, the library name that users see in the GroupWise client is the same as the Library object name. However, you can change the display name if you want it to be different from the Library object name.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 2: Library Name](#), specify the Library object name.

Under [Item 7: Library Description](#), provide a brief description of the planned use for the library.

Under [Item 10: Display Name](#), specify the library name you want users to see in the GroupWise client, if it is different from the Library object name.

22.3.5 Deciding Where to Store Documents

When deciding where to store documents, you should review the following considerations:

- ◆ [“Document Storage Location” on page 333](#)
- ◆ [“Disk Space Requirements” on page 333](#)
- ◆ [“Direct Access Paths to Document Storage Areas” on page 334](#)

Document Storage Location

Documents belonging to full-service libraries should *not* be stored at the post office. Instead, they should be stored in document storage areas. For a review, see [Section 21.2, “Document Storage Areas,” on page 317](#).

A library can have more than one document storage area. The only requirement is that the POA that services the library must have direct network access (mapped drive or mounted file system) to each storage area.

You can set up one document storage area for each library as you create the Library object. Additional document storage areas can be set up using the Storage Areas properties page of the Library object, as described in [“Adding a Document Storage Area” on page 345](#).

Disk Space Requirements

You need to know the disk space requirements for your libraries in order to choose appropriate locations for document storage areas.

If you have chosen a centralized library configuration, your document storage areas are all serviced by the POA of the DMS post office. Therefore, you can calculate the disk space requirements for your GroupWise system as a whole. If you have chosen a decentralized configuration, document storage areas are located throughout your GroupWise system. Therefore, disk space requirements must be calculated separately for each library.

If your current document storage statistics are an accurate indicator for a given library or for your system, use them for calculating your disk space requirements. Otherwise, use the following formula for determining DMS storage needs:

Formula:

```
Number of Users
x Average Number of Documents per User
x Average Document Size
x Average Number of Versions per Document
-----
Disk Space Required for Library
```

Example:

```
250 Users
x 200 Documents per User
x 50 KB per Document
x 10 Versions per Document
-----
25 GB of Disk Space
```

Users might create a new version of a document any time they revise it. Because all versions of a document are saved in BLOB storage with the original document, disk space can be used up quickly! If you know how many versions per document your users average, use that value in the formula; otherwise, allow for an average of at least ten versions per document.

If your Average Document Size value for the formula is based on non-GroupWise documents, they will be compressed by about 50% after they have been imported into GroupWise and stored in BLOBs.

You should research your current or expected document usage before deciding where to store documents.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 4: Document Usage Estimate](#), enter the requested values and calculate the resulting disk space requirements.

If your values are calculated for the system (rather than per library), enter this information on only one of the worksheets.

Direct Access Paths to Document Storage Areas

To define a document storage area, you need to know its direct access path. For example, a UNC path specifies the absolute location of the document storage directory.

```
\\Windows_server\sharename\storage_directory
```

For example:

```
\\win2008\c$\docs
```

NOTE: On Linux, ConsoleOne interprets a UNC path so that the first item in the UNC path is the Linux server hostname, followed by a Linux path to the document storage area.

You might want to set up a document storage area on the same server where the POA runs so as not to increase network traffic. The POA can index and serve documents to users most efficiently if the document storage area is located locally.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 6: Document Storage Area Path](#), specify the direct access path.

Under [Item 5: Document Storage Area Description](#), provide a useful description of the document storage area. (This description is displayed only in ConsoleOne.)

22.3.6 Setting Document Version Options

When you create a new library, you can establish how document versions are handled. For an overview of document versioning, see [“Maximum Versions” on page 320](#).

- ♦ [“Official Version” on page 335](#)
- ♦ [“Start Version Number” on page 335](#)

Restricting the maximum number of versions should be done after the library has been created, as described in [Section 22.6.1, “Editing Library Properties,” on page 343](#).

Official Version

By default, any user can establish the official version of a document. However, you can remove that right from one or more users if needed.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 11: Restrict Public Access Rights](#), cross out Designate Official Version if you want to eliminate that right for all users.

You can later grant the Designate Official Version to specific users or distribution lists, as described in [Section 22.6.3, “Managing Library Access,” on page 348](#).

Start Version Number

You must set the start number for each library to either 0 (zero) or 1. The default is 1. This number identifies the original document.

Version numbers are automatically increased from the number you select. If you select 0, the first version of a document will be 000. If you select 1, the first version will be 001.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 8: Start Version Number](#), select 0 or 1.

22.3.7 Figuring Maximum Archive Directory Size

Documents created with GroupWise DMS can be archived, depending on their Document Type properties. A document’s type determines its disposition, such as archiving or deleting. For more information, see [“Customizing the Default Document Type Property” on page 363](#).

When you archive documents, their BLOB files are moved into archive directories. Each library in a document storage area has its own set of archive directories that are automatically created as needed. They are named arxxxxxx (where xxxxxx is an incremental integer with leading zeros). A document

storage area has the same archive directory structure as the gwdms subdirectory in the post office, as illustrated in “[Post Office Directory](#)” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

When a document is archived, GroupWise determines if the document’s BLOB file can fit in the current archive directory. If it cannot fit, another archive directory is created and the BLOB is archived there.

An archive set consists of all documents in one archive directory. The Maximum Archive Size property on the Library object establishes in bytes each archive directory’s size limit. You should set this to mirror the capacity of your archival medium (such as a CD or DVD). It should not be more than your archival medium’s capacity.

It is usually better to keep archive sets small in comparison to the size of the backup medium. This lets you back up archive directories often enough to keep your hard disk space from being used up too quickly between backups. For example, if your backup medium has 1 GB capacity, you could limit your archive sets to a maximum archive size of 200 MB.

If your archival system only lets you back up in one pass (in other words, you cannot perform consecutive backups to the medium), the Maximum Archive Size should match the archival medium’s capacity.

Some archival mediums require extra space for recording file storage data, such as an index of the files stored to tape. Ten percent is usually sufficient. For example, a tape system with 100 MB capacity means you should set your Maximum Archive Size to 90 MB.

Consult your archival medium documentation for information on setting up an effective backup strategy. Include in your strategy such concepts as multiple archive sets per backup medium, or allowing extra space for the medium’s file storage data.

ADDITIONAL LIBRARIES WORKSHEET

Under [Item 9: Maximum Archive Size](#), enter a number (in bytes, with no abbreviations or commas).

22.3.8 Designating Initial Librarians

A librarian has full rights to the properties of every document in the library, and can therefore perform management tasks on all library documents. You can assign yourself as a librarian. You can also delegate these tasks by assigning responsible users in each library as librarians. Any GroupWise user who normally has access to the library can be a librarian. You can also have multiple librarians for each library.

When you first create a new library, you might want to simply designate yourself as the librarian and assign other users later. For more detailed information, see [Section 22.6.4, “Adding and Training Librarians,”](#) on page 350.

ADDITIONAL LIBRARIES WORKSHEET

Under [Item 12: Librarians](#), list any users that you want to function as librarians for the new library.

22.3.9 Restricting Initial Public Library Rights

The rights to documents in a library apply to the library as a whole; therefore, they are referred to as public rights. By default, all public rights are granted to all users in a new library.

You can restrict which GroupWise library features individual users or distribution lists should have by removing the public rights and then restoring them for selected users or distribution lists.

The following table summarizes the public library rights:

Public Right	Description
Add	Allows users to add new documents to the library.
Change	Allows users to make changes to existing documents in the library.
Delete	Allows users to delete documents, regardless of who else created them or has rights to the documents. However, to be able to delete a document, users must also have rights to locate and modify the document (View and Change rights), in addition to the Delete right.
View	By itself, this right allows searching, viewing, or copying documents, but does not permit editing them. Copies can be edited, because a copy is saved as a separate document. Therefore, editing a copy does not affect the original document or any of its versions.
Designate Official Version	Allows any version of a document to be designated as the official version. The official version, which is not necessarily the most recently-edited version, is the one located in searches. The official version is usually determined by the creator or author of the document. However, the official version can be designated by the last user to edit the document (if the user has this right). A user also needs the Change right to the document to be able to designate an official version. However, you might still want to deselect this as an initial public right.
Reset In-Use Flag	The In-Use flag protects against data loss by preventing multiple users from concurrently opening the same document. The purpose of the Reset In-Use Flag right is to allow a user or librarian to reset a document's status when the document is in use by someone else or when it is erroneously flagged as in use. Because you can manually reset the In-Use flag to change a document's status, even if the document is currently open, you should use prudence in allowing users the public right to change the In-Use flag. You might want to deselect this as a public right.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 11: Restrict Public Access Rights](#), cross out any public rights you want to eliminate for all users.

You can later grant the rights to specified users or groups, as described in [Section 22.6.3, "Managing Library Access,"](#) on page 348.

Rights to individual documents in a library can be modified at any time by the user listed as the creator or author of the document. Just because users might have public rights in a library does not mean that they have the equivalent rights to every document in the library. For additional information on rights, see "[Sharing Documents](#)" in "[Document Management](#)" in the *GroupWise 2012 Windows Client User Guide*.

22.3.10 Determining Your Indexing Needs

The POA performs many tasks in the post offices, as described in [Section 35.5, “Role of the Post Office Agent,” on page 477](#). Indexing documents is just one of its many functions.

If necessary, you can configure an extra POA on another server to handle indexing. Separating POA functions can optimize the processing load for the respective POAs, particularly if your GroupWise system will regularly search and index a large number of documents.

If you feel you might need dedicated indexing for DMS documents, see [Section 23.3, “Indexing Documents in Libraries,” on page 374](#) for in-depth information on different configurations. Then determine whether you need dedicated indexing.

FULL-SERVICE LIBRARY WORKSHEET

Under [Item 13: Dedicated POA for Indexing](#), mark whether or not you plan to set up a separate indexing POA.

22.3.11 Determining If You Need to Set Up Integrations for DMS Users

For an overview of integrations, see [Section 21.4, “Integrations,” on page 321](#). To determine if you should set up integrations for a given application, see [Chapter 24, “Integrations,” on page 387](#).

ADDITIONAL LIBRARIES WORKSHEET

Under [Item 14: Set Up Integrations](#), mark whether or not you need to manually set up integrated applications for your DMS users.

22.4 Setting Up a Full-Service Library

You should have already reviewed [Section 22.3, “Planning Full-Service Libraries,” on page 328](#) and filled out [Section 22.7.2, “Full-Service Library Worksheet,” on page 356](#) for each new library. Before starting to create new libraries, be sure your system meets the following prerequisites:

- ♦ Make sure the eDirectory contexts exist where you will create new Library objects.
- ♦ Make sure the post offices exist that will own the new libraries. If you are using a centralized configuration, make sure you have created the DMS post office that will own all the libraries by following the instructions in [Chapter 11, “Creating a New Post Office,” on page 173](#).
- ♦ Make sure the POA is running for each post office that will own a new library.
- ♦ Make sure you have access to the physical locations where you will set up document storage areas.

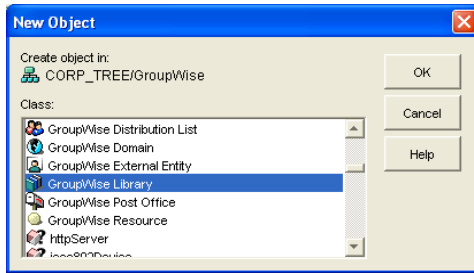
After the prerequisites are met, you are ready set up one or more full-service libraries.

- ♦ [Section 22.4.1, “Creating the Full-Service Library,” on page 338](#)
- ♦ [Section 22.5, “Viewing a New Library in Your GroupWise System,” on page 341](#)
- ♦ [Section 22.4.2, “What’s Next,” on page 340](#)

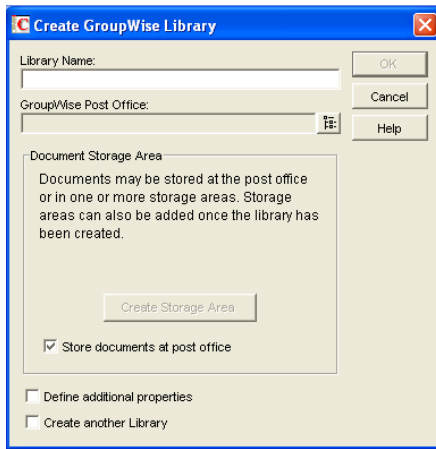
22.4.1 Creating the Full-Service Library

- 1 Make sure you are logged in to the eDirectory tree where you want to create the library.
This must be the same tree as the post office the library will belong to ([worksheet item 3](#)).

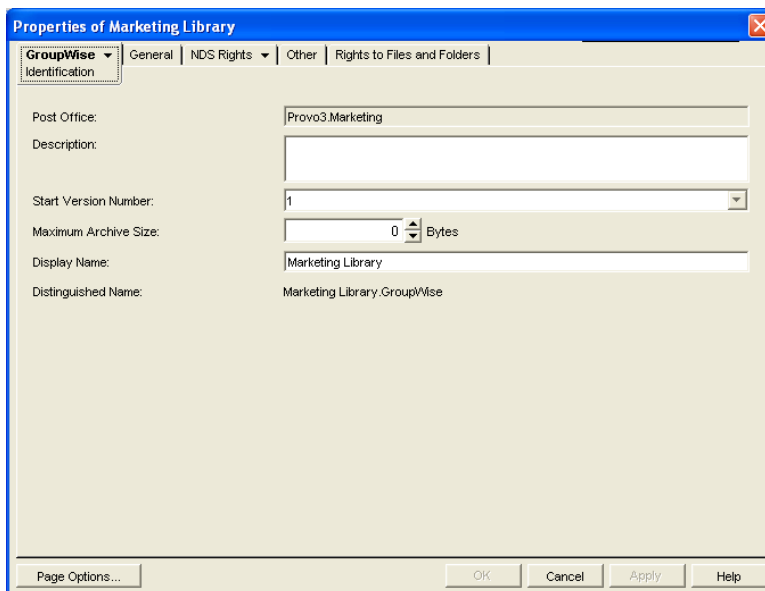
- 2 In ConsoleOne, browse to and right-click the eDirectory container where you want to create the library ([worksheet item 1](#)), then click *New > Object*.



- 3 Double-click *GroupWise Library*, then fill in the fields in the *New Library* dialog box ([worksheet items 2 through 6](#)).

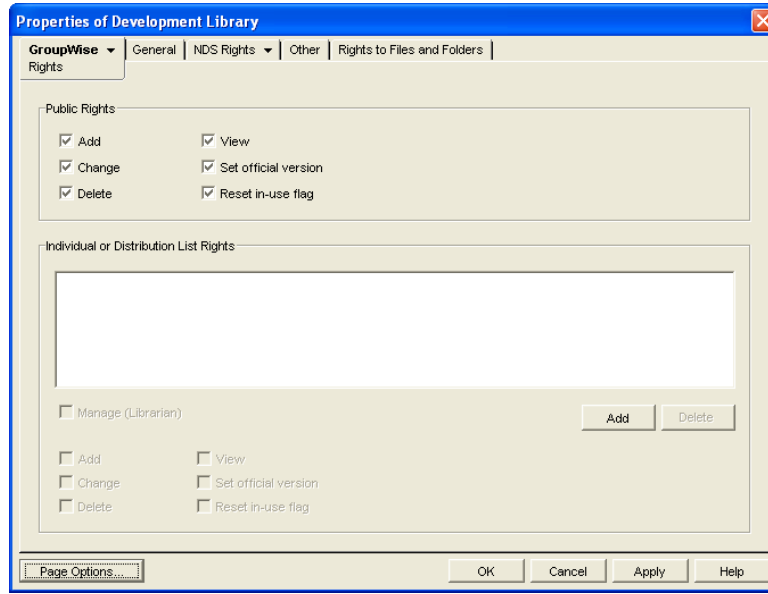


- 4 Click *Define Additional Properties*, then click *OK* to create the new Library object and display the library Identification page.



- 5 Fill in the fields ([worksheet items 7 through 10](#)).

- 6 Click *GroupWise > Rights* to display the Rights page.



- 7 In the Public Rights box, deselect any rights you want to remove from all library users ([worksheet item 11](#)).
- 8 If you want to set up one or more librarians, click *Add*, browse to and select one or more users or distribution lists ([worksheet item 12](#)), then click *OK*. Select the users and distribution lists, then select *Manage (Librarian)* to give them rights to the properties of all documents in the library.
- 9 Click *OK* to save the library information.
- 10 Test the library. See [Section 22.5, “Viewing a New Library in Your GroupWise System,” on page 341](#).

22.4.2 What’s Next

After you have created the new library, you can expand its capabilities as needed:

- ♦ Import and manage documents.
See [Chapter 23, “Creating and Managing Documents,” on page 359](#).
- ♦ Set up integrated applications for DMS users ([worksheet item 14](#)).
See [Chapter 24, “Integrations,” on page 387](#).
- ♦ Grant library rights to specific users or distribution lists.
See [Section 22.6.3, “Managing Library Access,” on page 348](#).
- ♦ Assign librarians.
See [Section 22.6.4, “Adding and Training Librarians,” on page 350](#).
- ♦ Set up multiple document storage areas.
See [“Adding a Document Storage Area” on page 345](#).
- ♦ Set up a dedicated indexing POA ([worksheet item 13](#)).
See [Section 23.3, “Indexing Documents in Libraries,” on page 374](#).

22.5 Viewing a New Library in Your GroupWise System

After you create a new library, you can see it in ConsoleOne and GroupWise client users can see it in the GroupWise client.

- ♦ [Section 22.5.1, “Seeing the New Library in ConsoleOne,” on page 341](#)
- ♦ [Section 22.5.2, “Seeing the New Library in the GroupWise Windows Client,” on page 342](#)

22.5.1 Seeing the New Library in ConsoleOne

In the Console View in ConsoleOne, you can see the new Library object in the context of its eDirectory container object.

Figure 22-3 Console View Showing the New Library Object

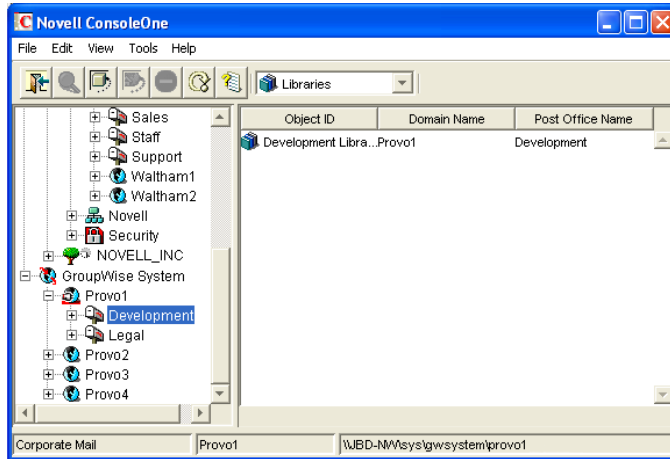


In the GroupWise View, you can see the relationship between the new library and the post office it belongs to.

To locate the library in the GroupWise view:

- 1 Expand the GroupWise System object.
- 2 Expand the Domain object where the owning post office resides.
- 3 Select the owning post office.

- 4 In the drop-down list of objects, select *Libraries*.

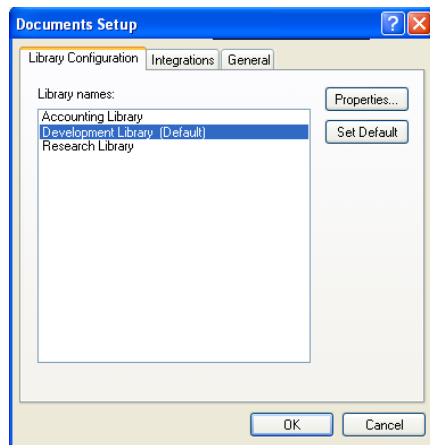


22.5.2 Seeing the New Library in the GroupWise Windows Client

GroupWise Windows client users can see that a new library has been created. They can set it as their default library if desired.

In the GroupWise client:

- 1 Click *Tools > Options > Documents*.



The *Library Configuration* tab should include the new library.

- 2 Select the new library, click *Set as Default*, then click *OK* to use the new library as the default location for storing documents and searching for documents.

22.6 Managing Libraries

As your GroupWise DMS system grows and evolves, you might need to perform the following activities:

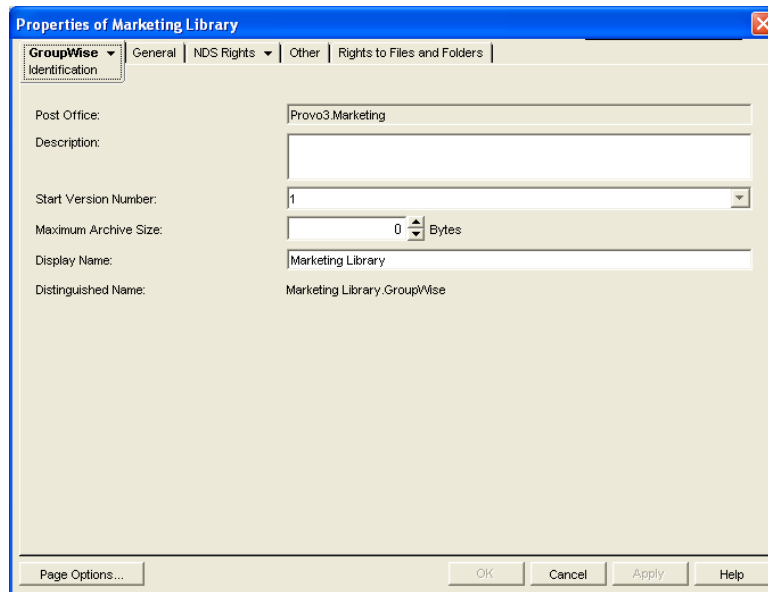
- ♦ [Section 22.6.1, “Editing Library Properties,”](#) on page 343
- ♦ [Section 22.6.2, “Managing Document Storage Areas,”](#) on page 345

- ♦ Section 22.6.3, “Managing Library Access,” on page 348
- ♦ Section 22.6.4, “Adding and Training Librarians,” on page 350
- ♦ Section 22.6.5, “Maintaining Library Databases,” on page 354
- ♦ Section 22.6.6, “Moving a Library,” on page 354
- ♦ Section 22.6.7, “Deleting a Library,” on page 354

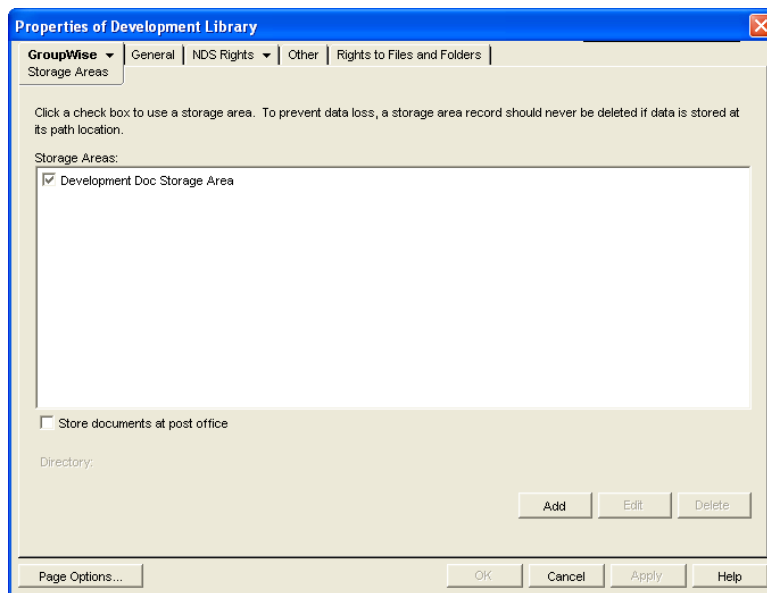
22.6.1 Editing Library Properties

After creating a library, you can change some library properties. Other library properties cannot be changed.

- 1 In ConsoleOne, browse to and right-click the Library object, then click *Properties* to display the library Identification page.

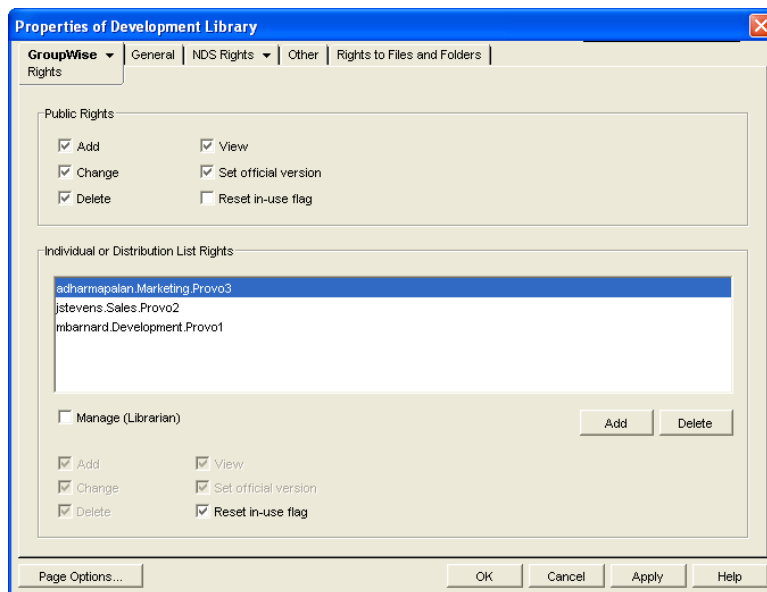


- 2 Change editable fields as needed. For information about individual fields, click *Help*.
- 3 Click *GroupWise > Storage Areas* to display the Storage Areas page.



All document storage areas associated with the library are listed, no matter where they are located. On this page, you can add, move, and delete document storage areas. See [Section 22.6.2, “Managing Document Storage Areas,”](#) on page 345.

- 4 Click *GroupWise > Rights* to display the library Rights page.



Public library rights granted to all users are selected in the *Public Rights* box. The *Individual and Distribution List Rights* box shows any additional rights that have been granted to specific users. See [Section 22.6.3, “Managing Library Access,”](#) on page 348 and [Section 22.6.4, “Adding and Training Librarians,”](#) on page 350.

- 5 Click *OK* to save changes to the library properties.

22.6.2 Managing Document Storage Areas

For a review, see [Section 21.2, “Document Storage Areas,”](#) on page 317 and [Section 22.1.4, “Deciding Where to Store Documents,”](#) on page 325.

Typically, the initial document storage area for a library is set up when the library is created. Thereafter, you can create additional document storage areas as the library grows. You can move a document storage area to a location where more storage is available. You can delete a document storage area if it is no longer used.

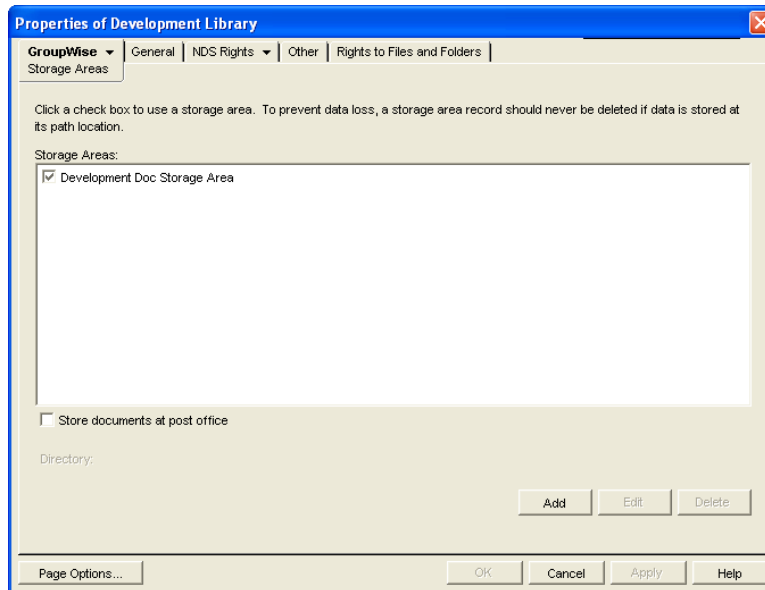
- ♦ [“Adding a Document Storage Area”](#) on page 345
- ♦ [“Moving a Document Storage Area”](#) on page 346
- ♦ [“Deleting a Document Storage Area”](#) on page 347

Adding a Document Storage Area

To help you plan where to create the new document storage area, see [Section 22.1.4, “Deciding Where to Store Documents,”](#) on page 325.

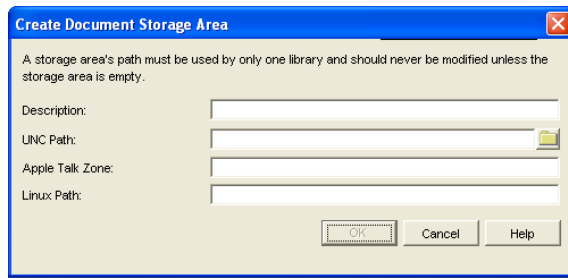
To create a new document storage area for a library:

- 1 In ConsoleOne, browse to and right-click the Library object, then click *Properties*.
- 2 Click *GroupWise > Storage Areas* to display the Storage Areas page.



Existing document storage areas are listed.

- 3 Click *Add* to create a new document storage area.

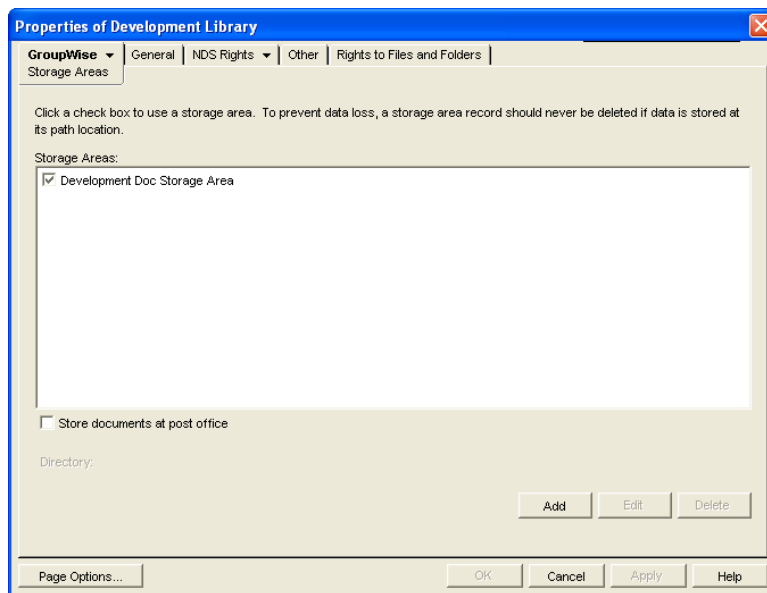


- 4 Provide a description for the document storage area.
- 5 Specify the UNC path to the directory where you want to create the document storage area.
If the directory does not exist, it will be created as the document storage area is set up.
As an alternative, you can specify an AppleTalk zone to store documents on an Apple computer, or you can specify a Linux path to store documents on a Linux server. The POA that will service the library must have direct access to the location you specify.
- 6 Click **OK** to create the new document storage area and add it to the list of storage areas for the library.
If you have multiple document storage areas selected in the *Storage Areas* list, new and modified documents could be added to any one of them.
- 7 If you want to stop storing documents in the previous document storage area, deselect it in the *Storage Areas* list.
- 8 Click **OK** to save the document storage area information.

Moving a Document Storage Area

You might choose to move a document storage area if it is close to exceeding the available disk space at its current location and you do not want to create an additional document storage area.

- 1 Stop the POA that services the library.
- 2 Copy the document storage area directory and all of its contents to the desired location.
- 3 Make sure that the POA has access to the new location so that it can read and write documents in the document storage area.
- 4 In ConsoleOne, browse to and right-click the Library object, then click *Properties*.
- 5 Click *GroupWise > Storage Areas* to display the Storage Areas page.



Existing document storage areas are listed.

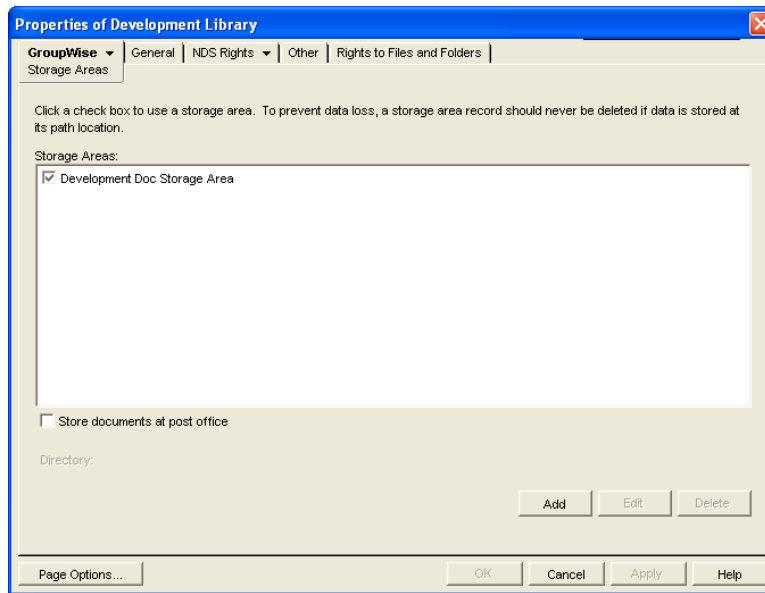
- 6 Select a document storage area, then click Edit.
- 7 Provide the new location for the document storage area, then click OK twice to save the new document storage information.
- 8 Restart the POA.

Deleting a Document Storage Area

When you delete a document storage area, any documents in the document storage area are moved to other valid document storage areas for the library. If you want to move documents to a specific location before deleting the document storage area, see [Section 23.1.3, “Managing Groups of Documents,”](#) on page 361.

To delete a document storage area:

- 1 In ConsoleOne, browse to and right-click the Library object that owns the document storage area, then click *Properties*.
- 2 Click *GroupWise > Storage Areas* to display the Storage Areas page.



- 3 Select a document storage area, then click *Delete*.
- 4 Click *OK* to close the Storage Areas page

If the above steps are not successful in deleting a document storage area, perhaps because one or more documents were in use during the deletion process, you can use the *Analyze/Fix Library* action of *Mailbox/Library Maintenance*, with the *Remove Deleted Storage Areas* and *Move Documents First* options selected, to finish cleaning up the deleted document storage area. For more information, see [Chapter 28, "Maintaining Library Databases and Documents,"](#) on page 415.

22.6.3 Managing Library Access

Access to libraries is controlled by the rights users have to the Library object. By default, when a new library is created, all of the following rights are granted:

Public Right	Description
Add	Allows users to add new documents to the library.
Change	Allows users to make changes to existing documents in the library.
Delete	Allows users to delete documents, regardless of who created them or has rights to the documents. However, to be able to delete a document, users must also have rights to locate and modify the document (View and Change rights), in addition to the Delete right.
View	By itself, this right allows searching, viewing, or copying documents, but does not permit editing them. Copies can be edited, because a copy is saved as a separate document. Therefore, editing a copy does not affect the original document or any of its versions.
Designate Official Version	Allows any version of a document to be designated as the official version. The official version, which is not necessarily the most recently edited version, is the one located in searches. The official version is usually determined by the creator or author of the document. However, the official version can be designated by the last user to edit the document (if the user has this right). A user also needs the Change right to the document to be able to designate an official version.

Public Right	Description
Reset In-Use Flag	<p>The In-Use flag protects against data loss by preventing multiple users from concurrently opening the same document. The purpose of the Reset In-Use Flag right is to allow a user or librarian to reset a document's status when the document is in use by someone else or when it is erroneously flagged as in use.</p> <p>In the GroupWise client the document properties Status field displays the current In-Use flag setting for a document. The Status field is automatically set to In Use when a document is opened and reset to Available when a document is closed. There can also be other values, such as Checked Out. A document cannot be checked out when its status is In Use.</p>

There are a variety of reasons for which you might want to restrict certain library rights, including:

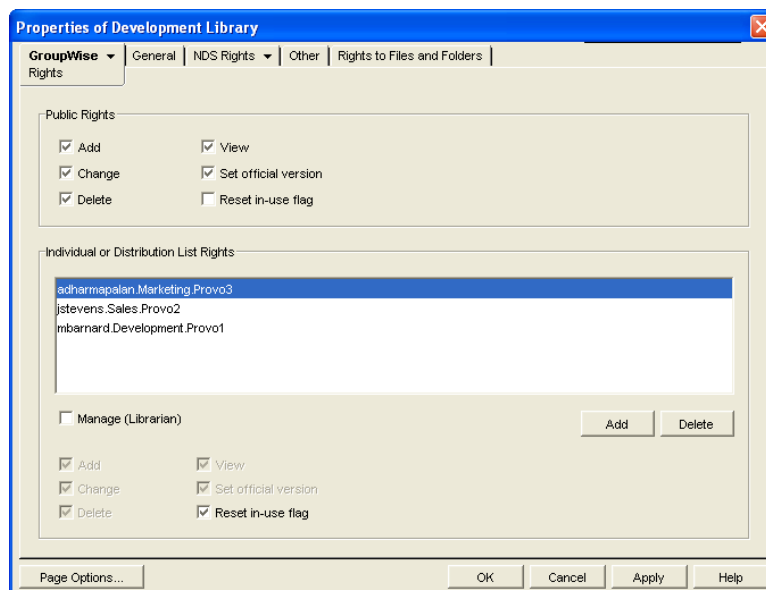
- ◆ Your libraries are specialized by department and you want to restrict access to sensitive libraries, such as a payroll library.
- ◆ Your libraries are distributed across multiple post offices and you want to restrict the scope of user searches to only the libraries they should use, thereby speeding up searches.
- ◆ Your libraries are distributed across multiple servers and you want to minimize network traffic.
- ◆ You have some users who should have more rights than other users to certain libraries.

To restrict public rights while granting individual rights:

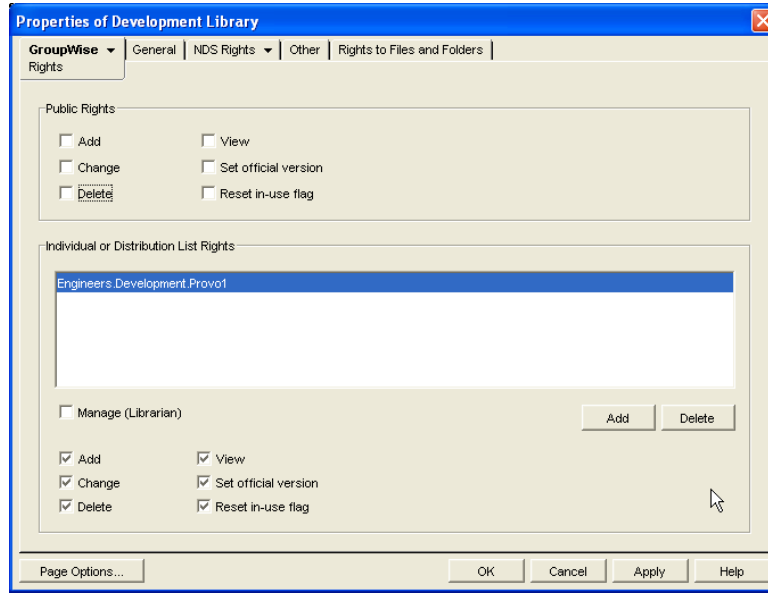
- 1 In ConsoleOne, browse to and right-click the Library object, then click *Properties*.
- 2 Click *GroupWise > Rights* to display the Rights page.
- 3 In the *Public Rights* box, deselect the rights that you want to remove from all users.
- 4 Click *Add*, then browse to and select the users who need to have rights to the library.

If the number is large, you might find it easier to create a distribution list for users who need rights. Then you can select one distribution list rather than multiple users. See [Chapter 18, "Creating and Managing Distribution Lists,"](#) on page 285

- 5 In the *Individual or Distribution List Rights* box, select the users or distribution lists to grant rights to.
- 6 Below the list, select the rights that you want to grant.



In the first example, only one user is granted the Reset In-Use Flag right.



In the second example, only members of the Engineers group are granted any rights to the Development Library.

7 Click *OK* to save the updated library rights information.

22.6.4 Adding and Training Librarians

When you first create a library, you might for convenience assign yourself as the initial librarian. As library activity increases you can add librarians, and if desired, remove yourself as a librarian.

- ♦ [“Understanding the Role of the Librarian” on page 350](#)
- ♦ [“Setting Up a Librarian GroupWise Account \(Optional\)” on page 353](#)
- ♦ [“Assigning Librarians” on page 353](#)

Understanding the Role of the Librarian

Keep in mind the following when assigning librarians:

- ♦ [“Librarian Identity” on page 350](#)
- ♦ [“Librarian Functions” on page 351](#)
- ♦ [“Librarian Rights” on page 351](#)

Librarian Identity

Any GroupWise user with access to a library can be a librarian for the library. You can have multiple librarians for a single library. You can also assign a single user as a librarian for multiple libraries. Because being a librarian entails additional functions and rights in the library, you should choose responsible users as librarians.

Librarian Functions

A librarian can perform the following actions:

- ◆ Check out a document without a copy.
- ◆ Modify the properties of any document in the library.
- ◆ Copy documents to another library.
- ◆ Delete both documents and properties.
- ◆ Reassign document creators and authors to handle orphaned documents
- ◆ Reset a document's status (change the In-Use flag).
- ◆ View all activity log records of any document in the library.
- ◆ Restore document BLOBs from backup.
- ◆ Perform mass operations, such as moving, deleting, archiving, and changing properties.
- ◆ Perform searches (but not full-text searches) on documents that are not available for searching by regular users.
- ◆ Use GroupWise third-party APIs to generate reports on all library documents.

All operations available to a normal user are also available to a librarian, as long as the security requirement discussed under "[Librarian Rights](#)" on page 351 is not compromised. The intention is that librarians can modify their own documents and document properties.

All actions taken by a librarian are written to a document's activity log.

Unless the librarian's own GroupWise user ID is in the *Author* or *Security* fields, a librarian cannot perform the following functions:

- ◆ Open a document
- ◆ View a document
- ◆ Save a document
- ◆ Check out a document with a copy

To help new librarians get started, you should explain these librarian functions to them. You can also refer new librarians to the "librarian users" topic in the GroupWise client help.

Librarian Rights

In addition to the six public rights, libraries also have a Manage right. When you grant the Manage right to a GroupWise user, you designate that user as a librarian. The Manage right gives the librarian full access to the properties of every document in the library. However, the Manage right does *not* grant the librarian direct access to the content of any document.

Because a librarian has full access to document properties, the librarian could add his or her own personal GroupWise user ID to the Author or Security field of a document, thus gaining access to the document's content. However, a high-priority email notification would automatically be sent to the original person listed in the Author field informing him or her of the action by the librarian. Therefore, document privacy is maintained.

The following table lists the various librarian functions, and whether an email notification is sent if the function is performed.

Librarian Function	Notification?
Modify the Author or Security fields	High-priority email to the author
Copy a document	High-priority email to the author
Delete a document	High-priority email to the author
Replace a document with a copy from backup	High-priority email to the author
Perform a mass document operation (copy, move, delete, or archive documents; modify document properties)	Mass operation emails
Reset a document's status (In-Use flag)	None
Check out a document without a copy	None
View the activity log of any document	None
Generate reports on any documents (using GroupWise third-party APIs)	None

Mass operation notifications do not specify what action was taken by the librarian; they only specify that an action was taken.

The following table lists the document property fields that the librarian has rights to modify, and whether an email notification is sent if the field is modified.

Property Field	Notification?
Subject	No
Author	Yes
Security (sharing list)	Yes
Document Type	No
Version Description	No
Custom Fields	No
File Extension	No
Official Version	No
Current Version	No

If you remove the Manage right from a user, you must manually deselect any rights that the user gained from being made a librarian that the user did not previously have.

Setting Up a Librarian GroupWise Account (Optional)

The Manage right is always in effect for those users who have been assigned as librarians. However, there might be times librarians want to act on their own accord without the possibility of seeing or modifying documents that belong to other users.

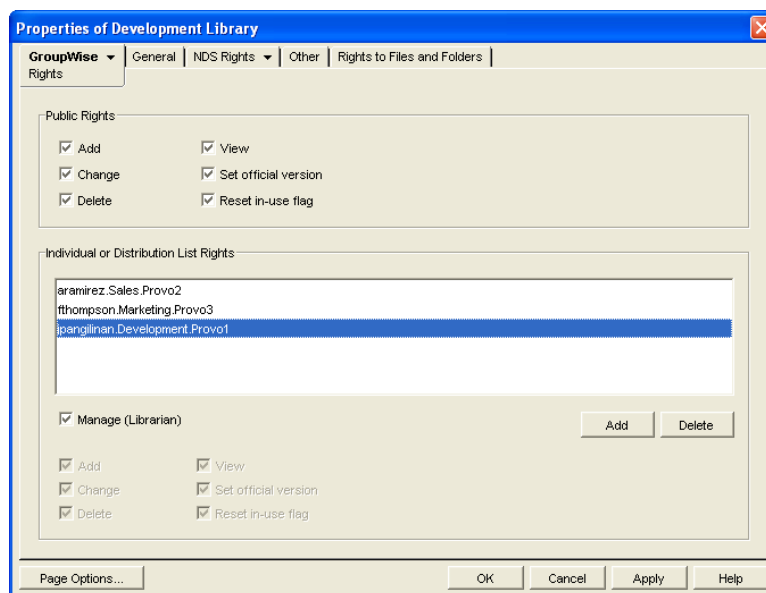
To allow users assigned as librarians to act as normal GroupWise users, you could create a single librarian account for a library and have users who need to perform librarian tasks log in using the librarian GroupWise account and password instead of their own.

If users assigned as librarians log in under a librarian GroupWise account, they do not have access to any documents they would normally have access to under their own accounts, except by altering the Author or Security fields.

Assigning Librarians

To add librarians to a library:

- 1 In ConsoleOne, browse to and right-click the Library object, then click *Properties*.
- 2 Click *GroupWise > Rights* to display the Rights page.
- 3 Click *Add*, browse to and select the users that you want to assign as librarians, then click *OK* to return to the Rights page.



- 4 In the *Individual or Distribution List Rights* box, select the librarian users, select *Manage (Librarian)*, then click *OK* to save the library rights changes.

22.6.5 Maintaining Library Databases

The Mailbox/Library Maintenance feature of ConsoleOne offers database maintenance features to keep your library and document databases in good condition. See [Chapter 28, “Maintaining Library Databases and Documents,” on page 415](#). It also helps you manage the disk space occupied by library and document databases and document storage areas. See [Section 30.4, “Reducing the Size of Libraries and Document Storage Areas,” on page 428](#).

When document creators or authors are removed from your GroupWise system, orphaned documents might be left behind. See [Section 23.4.3, “Handling Orphaned Documents,” on page 385](#).

To supplement your library maintenance procedures, you should back up your libraries and documents regularly. See [Section 31.3, “Backing Up a Library and Its Documents,” on page 432](#).

22.6.6 Moving a Library

You cannot move a Library object from one location to another in the eDirectory tree. To accomplish the equivalent, you can create a new library in the desired location, make yourself a librarian in both libraries, use a mass move operation in the GroupWise client to move the library’s documents from the old library into the new library, and then delete the old library. For instructions for these tasks, see:

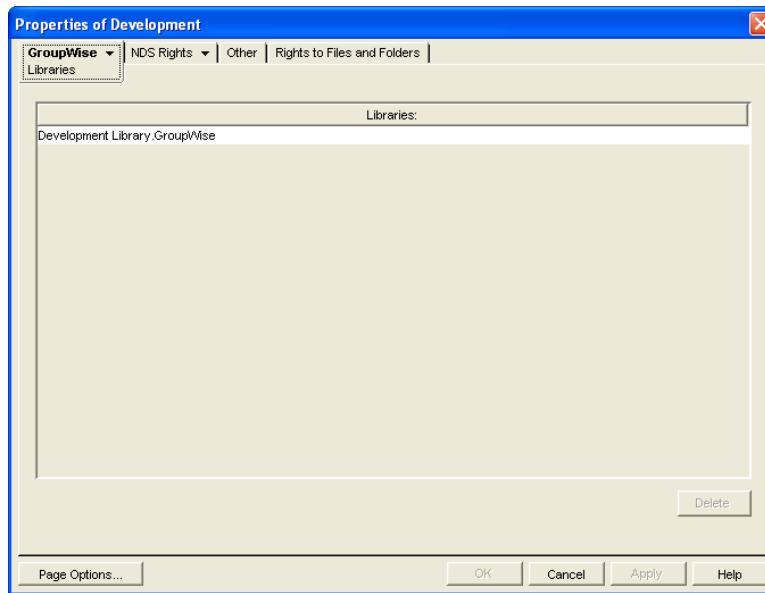
- ♦ [Section 22.2, “Setting Up a Basic Library,” on page 326](#)
- ♦ [Section 22.6, “Managing Libraries,” on page 342](#)
- ♦ [“Managing Groups of Documents” in “Document Management” in the *GroupWise 2012 Windows Client User Guide*](#)

As an alternative to moving the library, you can move just its document storage areas. See [“Moving a Document Storage Area” on page 346](#).

22.6.7 Deleting a Library

You should not delete a library until you make sure that all documents still in the library are no longer needed.

- 1 In ConsoleOne, browse to and right-click the Post Office object that owns the library to delete, then click *Properties*.
- 2 Click *GroupWise > Libraries* to display the Libraries page.



- 3 Select the library to delete, then click *Delete*.
All document storages areas and documents are deleted along with the library.
- 4 Click *OK* to close the Libraries page and complete the deletion of the library.

22.7 Library Worksheets

- ♦ [Section 22.7.1, “Basic Library Worksheet,” on page 355](#)
- ♦ [Section 22.7.2, “Full-Service Library Worksheet,” on page 356](#)

22.7.1 Basic Library Worksheet

For instructions on how to use this worksheet, see [Section 22.1, “Planning a Basic Library,” on page 324](#).

Item	Explanation
1) eDirectory Container:	<p>Specify the eDirectory container where you will create the Library object. This could be the same container as the post office that the library is assigned to. The Library object cannot later be moved to a different location.</p> <p>For more information, see Section 22.1.2, “Determining the Context for the Library Object,” on page 324.</p>
2) Library Name:	<p>Specify a name for the new library. Choose the name carefully. After the library is created, it cannot be renamed.</p> <p>For more information, see Section 22.1.3, “Choosing the Library Name,” on page 324.</p>
3) Post Office:	<p>Indicate which post office the library will belong to. A library cannot later be assigned to a different post office.</p> <p>For more information, see Section 22.1.1, “Selecting the Post Office That the Library Will Belong To,” on page 324.</p>

Item	Explanation
4) Store Documents at the Post Office?	Mark No unless you are absolutely certain you will never need to move the documents stored at the post office
<ul style="list-style-type: none"> ◆ No ◆ Yes 	For more information, see Section 22.1.4, "Deciding Where to Store Documents," on page 325.
5) Document Storage Area Description:	Provide a brief description for the document storage area, including such information as to which post office it belongs, its current capacity in megabytes, and the types of documents that might be stored in it.
	For more information, see Section 22.1.4, "Deciding Where to Store Documents," on page 325.
6) Document Storage Area Path:	If you are not storing documents at the post office, specify the document storage area for the library.
	For more information, see Section 22.1.4, "Deciding Where to Store Documents," on page 325.
7) Library Description:	Provide a description for the library to help you identify its function in the system.
	For more information, see Section 22.1.3, "Choosing the Library Name," on page 324.
8) Display Name:	Specify the library name you want users to see in the GroupWise client, if it is different from the Library object name.
	For more information, see Section 22.1.3, "Choosing the Library Name," on page 324.

22.7.2 Full-Service Library Worksheet

For instructions on how to use this worksheet, see [Section 22.3, "Planning Full-Service Libraries," on page 328.](#)

Item	Explanation
1) eDirectory Container:	Specify the name of the eDirectory container where you will create the Library object. This could be the same container as for the post office that owns the library. The Library object cannot later be moved to a different context.
	For more information, see Section 22.3.3, "Determining the Contexts for Library Objects," on page 332.
2) Library Name:	Specify a name for the new library. Choose the name carefully. After the library is created, it cannot be renamed.
	For more information, see Section 22.3.4, "Choosing Library Names," on page 332.

Item	Explanation
3) Post Office:	<p>Specify the post office that the library will belong to. A library cannot later be assigned to a different library.</p> <p>If you will using a centralized library configuration and you have not yet created the DMS post office, follow the instructions in Chapter 11, “Creating a New Post Office,” on page 173 before you begin creating libraries.</p> <p>For more information, see Section 22.3.1, “Deciding Which Libraries to Create,” on page 328.</p>
<p>4) Document Usage Estimate:</p> <p>a) Number of DMS users:</p> <p>b) Average number of documents per user:</p> <p>c) Average document size (bytes):</p> <p>d) Average number of versions per document:</p> <p>e) Total: (multiply a times b times c times d)</p>	<p>Calculate how much disk space the new library will need in order to help you select a location where you will store documents.</p> <p>For more information, see Section 22.3.5, “Deciding Where to Store Documents,” on page 333.</p>
5) Document Storage Area Description:	<p>Provide a brief description for the document storage area, including such information as which library it belongs to, its current capacity in megabytes, and the types of documents stored in it.</p> <p>For more information, see Section 22.3.5, “Deciding Where to Store Documents,” on page 333.</p>
6) Document Storage Area Path:	<p>Specify the UNC path to the location where you want to create the initial document storage area for the post office.</p> <p>For more information, see Section 22.3.5, “Deciding Where to Store Documents,” on page 333.</p>
7) Library Description:	<p>Provide a brief description for the new library, including what post office it belongs to, what types of documents will be stored in it, and so on.</p> <p>For more information, see Section 22.3.1, “Deciding Which Libraries to Create,” on page 328.</p>
8) Start Version Number:	<p>Select 0 or 1.</p> <ul style="list-style-type: none"> ◆ 0 ◆ 1 <p>For more information, see Section 22.3.6, “Setting Document Version Options,” on page 335.</p>
9) Maximum Archive Size:	<p>Specify the maximum number of bytes to allow per archive directory. Use a size that conforms with your backup strategy and backup medium requirements.</p> <p>For more information, see Section 22.3.7, “Figuring Maximum Archive Directory Size,” on page 335.</p>
10) Display Name:	<p>Specify the library name you want users to see in the GroupWise client, if it is different from the Library object name.</p> <p>For more information, see Section 22.3.4, “Choosing Library Names,” on page 332.</p>

Item	Explanation
11) Restrict Public Library Rights: <ul style="list-style-type: none"> ◆ Add ◆ Change ◆ Delete ◆ View ◆ Designate Official Version ◆ Reset In-Use Flag 	Cross out any public library rights you do not want all users to have. For more information, see Section 22.3.1, “Deciding Which Libraries to Create,” on page 328 or Section 22.3.6, “Setting Document Version Options,” on page 335.
12) Librarians:	List any users you want to have full rights to all documents in the library. For more information, see Section 22.3.8, “Designating Initial Librarians,” on page 336.
13) Dedicated POA for Indexing <ul style="list-style-type: none"> ◆ Yes ◆ No 	Mark whether or not you want to configure and run a separate POA dedicated to indexing documents. For more information, see Section 22.3.10, “Determining Your Indexing Needs,” on page 338.
14) Set Up Integrations <ul style="list-style-type: none"> ◆ Yes ◆ No 	Mark whether or not you need to manually set up integrations. For more information, see Chapter 24, “Integrations,” on page 387.

23 Creating and Managing Documents

GroupWise Document Management Services (DMS) lets Windows client users create documents with integrated applications, save them, then easily locate a specific document later without knowing the application, a specific document name, or the document's physical location. Windows client users can create, share, locate, edit, view, and check out documents that are created under the management of GroupWise DMS.

- ♦ [Section 23.1, "Adding Documents to Libraries," on page 359](#)
- ♦ [Section 23.2, "Organizing Documents in Libraries," on page 362](#)
- ♦ [Section 23.3, "Indexing Documents in Libraries," on page 374](#)
- ♦ [Section 23.4, "Managing Documents in Libraries," on page 383](#)

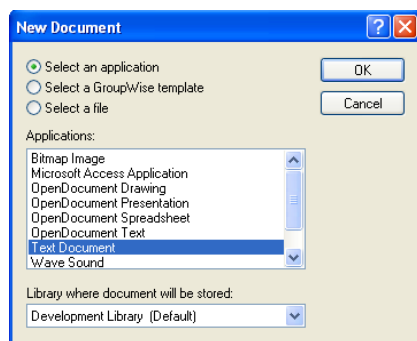
23.1 Adding Documents to Libraries

After you set up one or more libraries, users can add new documents to any library to which they have rights. They can also import existing documents into the GroupWise DMS system.

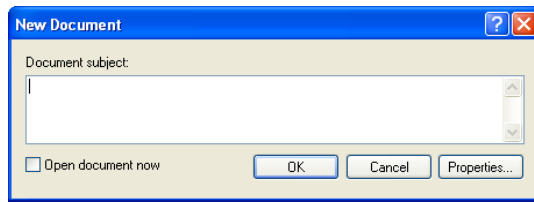
- ♦ [Section 23.1.1, "Creating New Documents in the GroupWise Windows Client," on page 359](#)
- ♦ [Section 23.1.2, "Importing Existing Documents into the GroupWise DMS System," on page 360](#)
- ♦ [Section 23.1.3, "Managing Groups of Documents," on page 361](#)

23.1.1 Creating New Documents in the GroupWise Windows Client

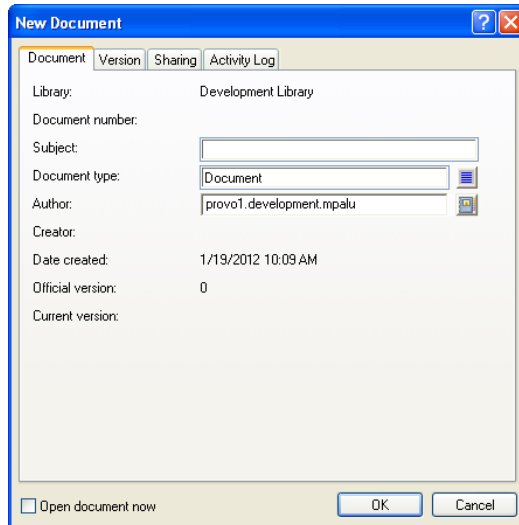
- 1 Click *File > New > Document*.



- 2 Select the program you want to use to create the document, select the library where you want to store the document, then click *OK*.
- 3 In the New Document dialog box, type a brief description of the document.



4 To set document properties, click *Properties*.



5 Set the document properties as needed, then click *OK*.

The selected program starts so you can create a new document.

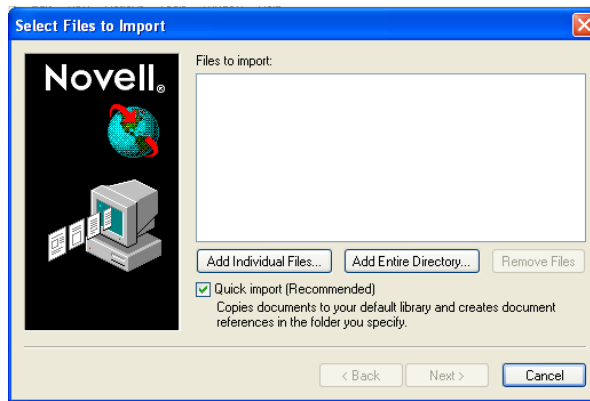
For more detailed information about creating documents in the GroupWise client, see “[Creating Documents](#)” in “[Document Management](#)” in the *GroupWise 2012 Windows Client User Guide*. You can also look up “documents” in the GroupWise client help.

23.1.2 Importing Existing Documents into the GroupWise DMS System

Some users might have existing documents that they want to manage by adding them to a GroupWise library.

To import documents using the GroupWise Windows client:

- 1 Click *File > Import/Export > Import Documents*.



2 Click *Add Individual Documents*, browse to and select the documents to add, then click *OK*.

or

Click *Add Entire Directory*, browse to and select a directory containing documents to import, then click *OK*.

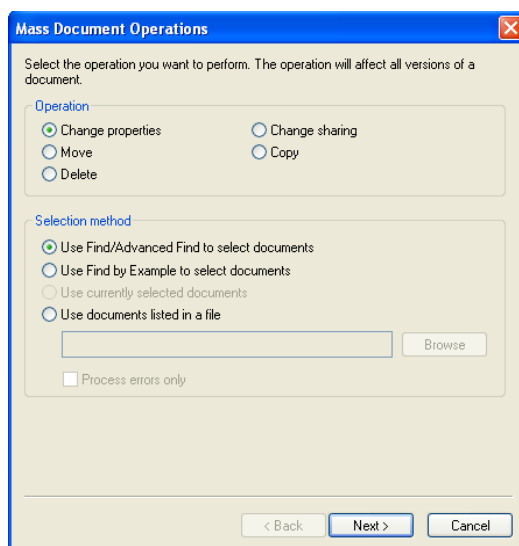
For additional instructions about creating documents in the GroupWise client, see [“Importing Documents into a GroupWise Library”](#) in [“Document Management”](#) in the *GroupWise 2012 Windows Client User Guide*. You can also look up “import documents” in the GroupWise client help.

23.1.3 Managing Groups of Documents

As users add documents and your GroupWise DMS system grows, your librarians might need to assist users in managing large groups of documents. If you have not yet assigned librarians to your GroupWise libraries, see [Section 22.6.4, “Adding and Training Librarians,”](#) on page 350.

To manage large groups of documents in the GroupWise Windows client:

1 Click *Tools > Mass Document Operations*.



2 Select the operation to perform on the group of documents:

- ◆ Change properties
- ◆ Move

- ◆ Delete
 - ◆ Change sharing
 - ◆ Copy
- 3 Select the method for identifying the group of documents to perform the operation on:
- ◆ Use Find/Advanced Find to select documents
 - ◆ Use Find by Example to select documents
 - ◆ Use currently selected documents
 - ◆ Use documents listed in a file.

For additional instructions about creating documents in the GroupWise client, see [“Managing Groups of Documents”](#) in [“Document Management”](#) in the *GroupWise 2012 Windows Client User Guide*. You can also look up [“mass document operations”](#) in the GroupWise client help.

IMPORTANT: You must be in Online mode in the GroupWise Windows client in order to perform mass document operations.

23.2 Organizing Documents in Libraries

Because documents are stored in a database structure, information can be associated with each document that is not part of the document itself. This additional information is stored as document properties.

- ◆ [Section 23.2.1, “Customizing Document Properties,”](#) on page 362
- ◆ [Section 23.2.2, “Defining Related Document Properties,”](#) on page 371

NOTE: Document properties cannot be set in ConsoleOne on Linux. However, you can use ConsoleOne on Windows to set document properties for libraries that are located on Linux.

23.2.1 Customizing Document Properties

For a summary of document properties, see [Section 21.3.1, “Document Properties,”](#) on page 318. To review, the following document properties are provided by default:

Author
Creator
Current Version Number
Date Created
Document Number
Document Type
Official Version Number
Subject

The default document property types cannot be deleted. Except for the Document Type property, they cannot be modified. However, you can add custom document types as needed.

- ◆ [“Customizing the Default Document Type Property”](#) on page 363
- ◆ [“Planning Custom Document Properties”](#) on page 364
- ◆ [“Adding Custom Document Properties”](#) on page 366

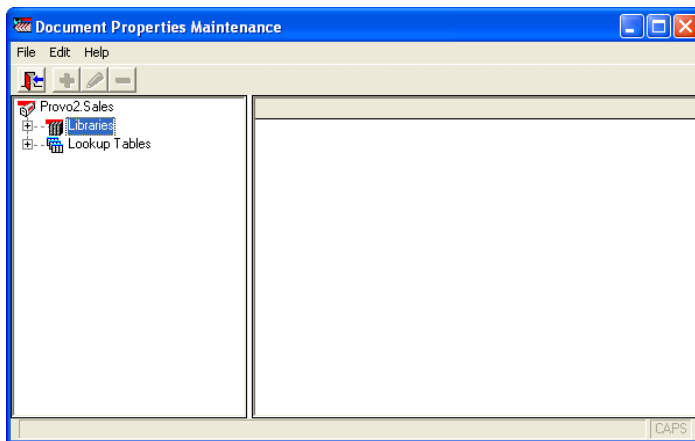
- ♦ “Planning Custom Lookup Tables for Custom Document Properties” on page 368
- ♦ “Adding Custom Lookup Tables” on page 369

Customizing the Default Document Type Property

The Document Type property is the only default document property that you can modify. For a review of document types, see [Section 21.3.2, “Document Types,” on page 319](#). You must have at least one document type, because it is a required document property field.

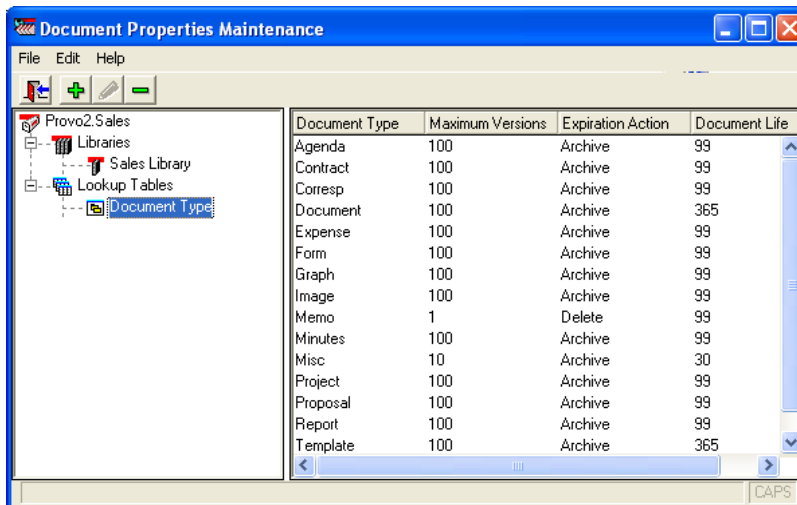
To modify the Document Type property for all libraries in a post office:

- 1 In ConsoleOne on Windows, browse to and select the post office that has libraries where you want to modify the Document Type property.
- 2 Click *Tools > GroupWise Utilities > Document Properties Maintenance*.



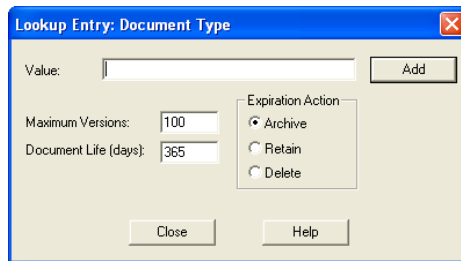
If you expand Libraries and select each library, you see that each library has the Document Type property. It is required.

- 3 Expand Lookup Tables, then select *Document Type*.

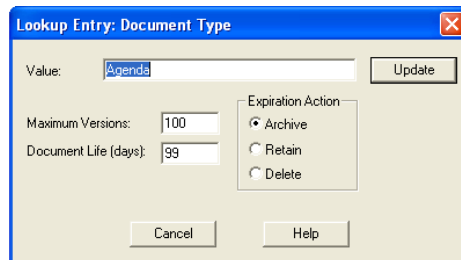


The lookup table defines the list of choices offered to users when they select a document type, no matter which library in the post office they are creating the document in.

- To add a new document type, click *Edit > Add*. In the *Value* field, type the new document type, click *Add*, then click *Close*.



- To edit an existing document type, click *Edit > Edit*. Change the settings as needed, click *Update*, then click *Close*.



For more details about the fields associated with the Document Type property, see [Section 21.3.2, “Document Types,” on page 319](#).

- To delete a document type, select the document type, click *Edit*, then click *Delete*.

Planning Custom Document Properties

When you need to add custom document properties, print the [“Custom Document Properties Worksheet” on page 365](#). One copy of the worksheet accommodates three new document properties.

The following table describes the fields and values associated with custom document properties:

Document Property Field	Field Values
<i>Property Field:</i>	The document property field is the label that GroupWise client users see in the document Properties dialog box. When you create a new document property, you can provide a description as well. However, the description displays only in ConsoleOne, not in the GroupWise client.
<i>Read-Only?</i>	Yes: The document property field displays information, but it is not accessible to users. No: Users can type in the document property field.
<i>Required?</i>	Yes: The user must supply a value for the document property. No: The user can leave the document property field blank.
<i>Hidden?</i>	Yes: The document property field is not displayed in the GroupWise client interface. No: The document property field is displayed in the GroupWise client interface.

Document Property Field	Field Values
<i>Lookup Table:</i>	A lookup table is required for a custom document property only when you want to offer the user a list of choices, rather than having the user type in the setting. The lookup table guarantees that the user provides a valid setting. For more information, see “Planning Custom Lookup Tables for Custom Document Properties” on page 368 .
<i>Related Property:</i>	A related property is required for a custom document property only when you create a lookup table that references a related lookup table. For more information, see Section 23.2.2, “Defining Related Document Properties,” on page 371 .
<i>Data Type:</i>	<p>Binary: An Object API reads and writes this information</p> <p>Date: Displayed in the Windows format selected by the user</p> <p>Number: Numerical only</p> <p>String: Alphanumeric</p>
<i>Maximum Length:</i>	For the String data type, you can specify the maximum number of characters allowed in the string. The longest possible string is 65535 alphanumeric characters.
<i>Case:</i>	For the String data type, you can control how the user's input is handled: <p>Upper: Forces entries to display in uppercase</p> <p>Lower: Forces entries to display in lowercase</p> <p>Mixed: Allows alphabetical characters to be displayed as typed</p>
<i>Minimum Value:</i>	For the Number data type, you can specify a minimum acceptable value.
<i>Maximum Value:</i>	For the Number data type, you can specify a maximum acceptable value.
<i>Parent:</i>	If the new document property is related to an existing document property in a parent-child relationship, you must specify the parent document property. For more information, see Section 23.2.2, “Defining Related Document Properties,” on page 371 .

Use copies of the [“Custom Document Properties Worksheet” on page 365](#) to plan the custom document properties you want to add to libraries.

If you need to create one or more lookup tables for your custom document properties, follow the instructions in [“Planning Custom Lookup Tables for Custom Document Properties” on page 368](#) and [“Adding Custom Lookup Tables” on page 369](#). Lookup tables used by new document properties should exist before you create custom document properties.

Then continue with [“Adding Custom Document Properties” on page 366](#).

Custom Document Properties Worksheet

For instructions on how to use this worksheet, see [“Planning Custom Document Properties” on page 364](#).

Item	Custom Document Property	Custom Document Property	Custom Document Property
1) Post Office:			
2) Libraries:			

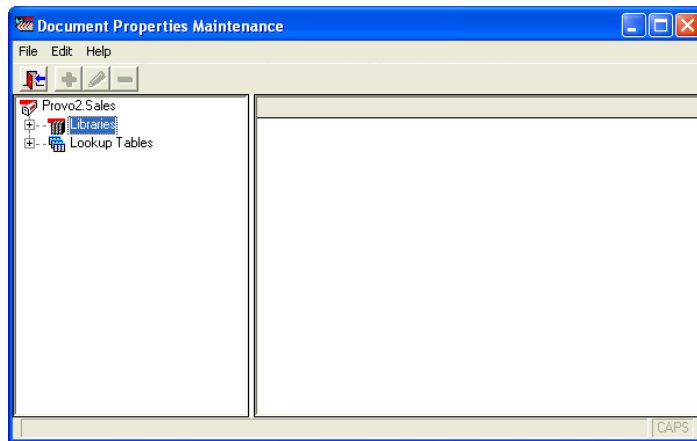
Item	Custom Document Property	Custom Document Property	Custom Document Property
3) Property Label:			
4) Description:			
5) Read-Only?			
	♦ Yes		
	♦ No		
6) Required?			
	♦ Yes		
	♦ No		
7) Hidden?			
	♦ Yes		
	♦ No		
8) Lookup Table:			
9) Data Type:			
	♦ Binary		
	♦ Date		
	♦ Number		
	♦ String		
10) Maximum Length:			
11) Case:			
	♦ Mixed		
	♦ Upper		
	♦ Lower		
12) Minimum Value:			
13) Maximum Value:			
14) Parent:			

Adding Custom Document Properties

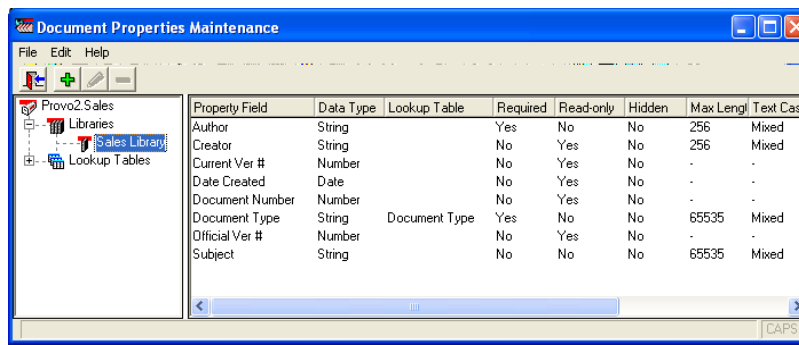
After you have determined what new document properties will meet the needs of your DMS system, as described in [“Planning Custom Document Properties” on page 364](#), and if necessary you have created lookup tables for your new document properties, as described in [“Planning Custom Lookup Tables for Custom Document Properties” on page 368](#) and [“Adding Custom Lookup Tables” on page 369](#), you are ready to add new custom document properties.

To add new custom document properties:

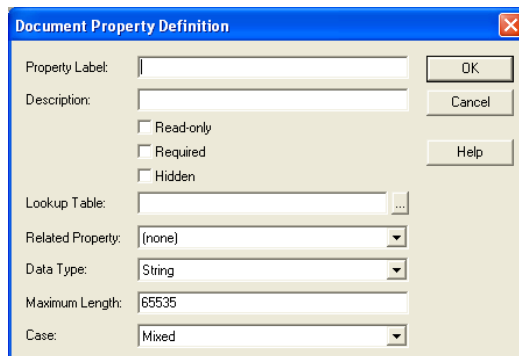
- 1 In ConsoleOne on Windows, browse to and select the Post Office object that owns the library for which you are creating custom document properties ([worksheet item 1](#)).
- 2 Click *Tools > GroupWise Utilities > Document Properties Maintenance*.



- Expand Libraries, then select the library for which you are creating custom document properties (worksheet item 2).



- Click *Edit > Add* to display the Document Property Definition dialog box.



Fields vary according to data type.

- Fill in the fields (worksheet items 3 through 14).
- Click *OK* to create the new custom document property.

In the Document Properties Maintenance window, the new document property is listed in alphabetical order. In the GroupWise client, custom document properties are listed after default document properties, in the order in which they are added to the library.

- Repeat [Step 4](#) through [Step 6](#) for each new custom document property.

When users next create documents in the library, the new custom document properties will be available to them.

Planning Custom Lookup Tables for Custom Document Properties

A lookup table is required for a custom document property only when you want to offer the user a list of choices, rather than having the user type in the setting. The lookup table guarantees that the user provides a valid setting.

Lookup tables are defined for the post office, so that multiple libraries in the post office can reference the same lookup tables.

When you need to provide lookup tables for custom document properties, print the “[Custom Lookup Tables Worksheet](#)” on page 369. One copy of the worksheet accommodates three new lookup tables.

The following table describes the fields and values associated with lookup tables:

Lookup Table Field	Field Values
<i>Lookup Table Name:</i>	<p>The lookup table name identifies the lookup table when you are assigning it to a property field.</p> <p>If the lookup table pertains to only one document property, you can name the lookup table the same as the document property. For example, the default property Document Type uses a lookup table named Document Type.</p> <p>However, lookup tables can be used by multiple document properties. For example, you could have a lookup table named Project used by document properties named Primary Project and Secondary Project.</p> <p>When you create a new lookup table, you can provide a description as well. If the lookup table name does not match a document property, you could indicate what document properties use the lookup table.</p>
<i>Related Table:</i>	<p>A related table is required for a lookup table only when you want to define related properties. For more information, see Section 23.2.2, “Defining Related Document Properties,” on page 371.</p>
<i>Data Type:</i>	<p>Binary: An Object API reads and writes this information</p> <p>Date: Displayed in the Windows format selected by the user</p> <p>Number: Numerical only</p> <p>String: Alphanumeric</p>
<i>Maximum Length:</i>	<p>For the String data type, you can specify the maximum number of characters allowed in the string. The longest possible string is 65535 alphanumeric characters.</p>
<i>Case:</i>	<p>For the String data type, you can control how the user’s input is handled:</p> <p>Upper: Forces entries to display in uppercase</p> <p>Lower: Forces entries to display in lowercase</p> <p>Mixed: Allows alphabetical characters to be displayed as typed</p>
<i>Minimum Value:</i>	<p>For the Number data type, you can specify a minimum acceptable value.</p>
<i>Maximum Value:</i>	<p>For the Number data type, you can specify a maximum acceptable value.</p>
<i>Lookup Table Entries:</i>	<p>The lookup table entries are the settings that users will choose from when they set the custom document property.</p>

Use copies of the [“Custom Lookup Tables Worksheet” on page 369](#) to plan the lookup tables you need in order to provide values for new custom document properties. If you need to use related properties, follow the instructions in [Section 23.2.2, “Defining Related Document Properties,” on page 371](#). Then continue with [“Adding Custom Lookup Tables” on page 369](#).

Custom Lookup Tables Worksheet

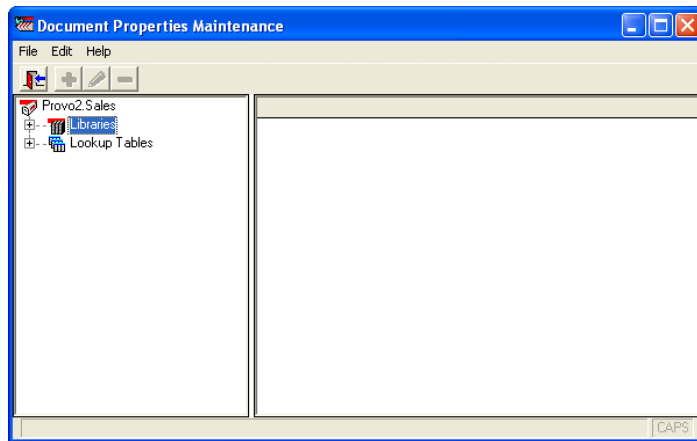
For instructions on how to use this worksheet, see [“Planning Custom Lookup Tables for Custom Document Properties” on page 368](#).

Item	Custom Lookup Table	Custom Lookup Table	Custom Lookup Table
1) Post Office:			
2) Property Label:			
3) Lookup Table Name:			
4) Description:			
5) Related Table:			
6) Data Type:			
♦ Binary			
♦ Date			
♦ Number			
♦ String			
7) Maximum Length:			
8) Case:			
♦ Mixed			
♦ Upper			
♦ Lower			
9) Minimum Value:			
10) Maximum Value:			
11) Lookup Table Entries:			

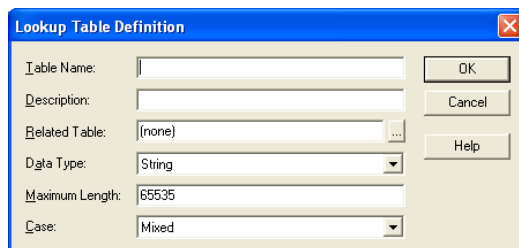
Adding Custom Lookup Tables

After you have determined what new lookup tables and lookup table entries you need to accommodate your new custom document properties, as described in [“Planning Custom Lookup Tables for Custom Document Properties” on page 368](#), you are ready to add new lookup tables.

- 1 In ConsoleOne on Windows, browse to and select the Post Office object that owns the libraries for which you are creating lookup tables ([worksheet item 1](#)).
- 2 Click *Tools > GroupWise Utilities > Document Properties Maintenance*.

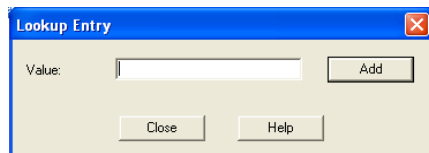


- 3 Select *Lookup Tables*, then click *Edit > Add* to display the Lookup Table Definition dialog box.



Fields vary depending on data type.

- 4 Fill in the fields ([worksheet items 3 through 10](#)).
- 5 Click *OK* to create the new lookup table.
- 6 Select the new lookup table, then click *Edit > Add* to display the Lookup Entry dialog box.



- 7 In the *Value* field, type one of the document property settings you want to offer to users ([worksheet item 11](#)), then click *Add*.
- 8 Repeat [Step 7](#) for all the lookup table entries listed on your worksheet for this lookup table, then click *Close*.
- 9 Click *OK* to create the custom lookup table.

23.2.2 Defining Related Document Properties

When document properties are related, your choice for the first property determines the settings you are offered for the second property. The user's selection in the first field determines what choices were offered in the second field.

Related document properties are set up by creating related lookup tables. Complete the following tasks to set up related document properties:

- ♦ [“Planning Related Document Properties” on page 371](#)
- ♦ [“Creating Related Lookup Tables” on page 373](#)
- ♦ [“Setting Up Related Document Properties” on page 373](#)

Planning Related Document Properties

Related document properties use a parent-child relationship. A parent property can have multiple child properties, but a child property can belong to only one parent. The relationship can include only two levels. A parent property cannot function as a child and a child property cannot function as a parent. The default document properties cannot participate as related properties.

In the Development Library example above, the Product document property would be the parent property and the Component document property would be the child property. If the Development Library belonged to Novell, products would include GroupWise, Open Enterprise Server, ZENworks, and so on. When users selected GroupWise as the product, listed components could include the GroupWise client, the agents, GroupWise system administration, and so on. Or you could let users type in whatever components they wanted.

When you need to set up related document properties, print the [“Related Document Properties Worksheet” on page 372](#). One copy of the worksheet accommodates one pair of related property fields, one parent lookup table, and one child lookup table (optional).

The following table describes the document properties and lookup tables that are required in order to set up related document properties:

Properties and Tables	Description
Parent Document Property	The parent document property is the user's first selection. In the Development Library example above, the parent document property is Product.
Child Document Property	The child document property is the user's second selection, based on the first selection. In the Development Library example above, the child document property is Component.
Parent Lookup Table	The entries in the parent lookup table provide the choices offered to the user in the parent document property field. In the Development Library example above, the user could select from GroupWise, Open Enterprise Server, and ZENworks in the Product field.
Child Lookup Table	The entries in the child lookup table provide the choices offered to the user after a choice from the parent lookup table has been selected. In the Development Library example above, if the user selected GroupWise in the Product field, the child lookup table would provide choices such as Agents, Client, and Admin in the Component field. The child lookup table is not required if you want to allow the user to type in anything they want in the child document property field.

Use copies of the [“Related Document Properties Worksheet”](#) on page 372 to plan the related document properties you want to use. One copy of the worksheet accommodates one pair of related properties. Continuing with the Development Library example, a filled-in worksheet might look like this:

Item	Setting	Item	Setting
1) Parent Document Property	Property Name: Product	4) Child Document Property	Property Name: Component
2) Parent Lookup Table	Table Name: Product	5) Child Lookup Table	Table Name: Component
3) Parent Lookup Entries	(required) Parent Entry: GroupWise Parent Entry: Open Enterprise Server Parent Entry: ZENworks	6) Child Lookup Entries	(optional) Child Entries: Admin Agents Client Child Entries: eDirectory Servers Child Entries: Desktops Servers

When you have finished planning related properties and their associated lookup tables, you should print and fill in a worksheet for each for each new related property, as described in [“Planning Custom Document Properties”](#) on page 364, and for each new lookup table, as described in [“Planning Custom Lookup Tables for Custom Document Properties”](#) on page 368.

Then you are ready to continue with [“Creating Related Lookup Tables”](#) on page 373.

Related Document Properties Worksheet

For instructions on how to use this worksheet, see [“Planning Related Document Properties”](#) on page 371.

Item	Setting	Item	Setting
1) Parent Document Property	Name:	4) Child Document Property	Name:
2) Parent Lookup Table	Name:	5) Child Lookup Table	Name:
3) Parent Lookup Entries	(required) Entry: Entry: Entry:	6) Child Lookup Entries	(optional) Entries: Entries: Entries:

Creating Related Lookup Tables

If you are supplying the choices for both related fields, you need both a parent lookup table and a child lookup table. If you are going to have users type information into the child property field, then you only need to create the parent lookup table. You should create lookup tables before creating the document properties that use them.

- ♦ [“Creating the Parent Lookup Table” on page 373](#)
- ♦ [“Creating the Child Lookup Table \(Optional\)” on page 373](#)

Creating the Parent Lookup Table

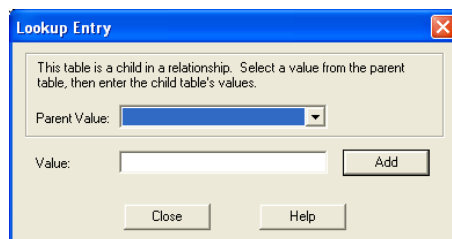
- 1 Create a new lookup table, as described in [Step 1](#) through [Step 5](#) in [“Adding Custom Lookup Tables” on page 369](#). Use [worksheet item 2](#) in the Table Name field. Leave the Related Table field set to (none).
- 2 Add entries to the new lookup table, as described in [Step 6](#) through [Step 8](#) in [“Adding Custom Lookup Tables” on page 369](#). Use the entries listed under [worksheet item 3](#) in the Value field.
- 3 Continue with [“Creating the Child Lookup Table \(Optional\)” on page 373](#).

or

If you are going to have users type information into the child property field, rather than selecting from a predefined list, skip to [“Setting Up Related Document Properties” on page 373](#)

Creating the Child Lookup Table (Optional)

- 1 Create a new lookup table, as described in [Step 1](#) through [Step 5](#) in [“Adding Custom Lookup Tables” on page 369](#). Use [worksheet item 5](#) in the Table Name field. Use [worksheet item 2](#) in the Related Table field to link the child table to the parent table.
- 2 Select the new lookup table, click *Edit*, then click *Add* to display the Lookup Entry dialog box.



- 3 Select a Parent value.
- 4 In the *Value* field, type one of the child lookup table entries for the selected parent value ([worksheet item 6](#)), then click *Add*.
- 5 Repeat [Step 4](#) for each entry listed under [worksheet item 6](#).
- 6 Repeat [Step 3](#) through [Step 5](#) for each parent value listed under [worksheet item 3](#).
- 7 Continue with [“Setting Up Related Document Properties” on page 373](#).

Setting Up Related Document Properties

After you have created related lookup tables, you are ready to set up the related document properties that use them. A few document property fields are required settings in the context of related properties:

- ♦ *Read-Only* must be set to No.

- ♦ *Hidden* must be set to No.
- ♦ *Required* must be set the same on the child property as it is on the parent property.

To set up related document properties:

- 1 Create the parent document property as described in [“Adding Custom Document Properties” on page 366](#). Use [worksheet item 1](#) in the Property Label field. Use [worksheet item 2](#) in the Lookup Table field. Leave the Related Property field set to (none).
- 2 Create the child document property using the same procedure. Use [worksheet item 4](#) in the Property Label field. Use [worksheet item 5](#) in the Lookup Table field. The Related Property field should automatically display as [worksheet item 1](#), showing that the child property is related to the parent property.

23.3 Indexing Documents in Libraries

Documents stored in GroupWise libraries need to be indexed so users can locate documents using the Find feature in the GroupWise Windows client. Your organization might need dedicated indexing to minimize performance degradation and network congestion. You might also need dedicated indexing so users can have prompt access to newly created documents.

- ♦ [Section 23.3.1, “Understanding DMS Indexing,” on page 374](#)
- ♦ [Section 23.3.2, “Determining Your Indexing Needs,” on page 381](#)
- ♦ [Section 23.3.3, “Implementing Indexing,” on page 383](#)

23.3.1 Understanding DMS Indexing

Before determining if you will need dedicated indexing, you should have a basic understanding of how indexing works in GroupWise.

- ♦ [“Index Storage” on page 374](#)
- ♦ [“Index Content” on page 375](#)
- ♦ [“Indexing Performed by the POA” on page 375](#)
- ♦ [“Indexing Cycle” on page 375](#)
- ♦ [“Bandwidth Considerations” on page 376](#)
- ♦ [“Indexer Configurations” on page 376](#)

Index Storage

When documents are indexed, the information is stored in QuickFinder indexes, which are located in a library’s [index](#) subdirectory. A library’s QuickFinder index is partitioned into ten *.idx files. Additionally, temporary *.inc (incremental) files are created that contain each day’s new index information. The *.inc files are combined once per day into the *.idx files (usually at midnight).

In a system with multiple libraries, each library has its own set of QuickFinder index files. Depending on how many libraries belong to a post office, and how many post offices with libraries are in your GroupWise system, there can be many sets of QuickFinder index files.

Index Content

Indexing can include a document's full text (depending on its document type), and always includes the document's property sheet information (subject, author, version descriptions, and so on). Both newly edited and newly created documents are indexed, which means indexing volume is determined by how many existing documents are edited as well as how many new documents are created.

Newly-created documents must be indexed before users can search for them. In setting up your indexing strategy, you must know how quickly users will need access to newly-created documents.

The standard search is limited to the QuickFinder indexes in the user's default library. But users can choose to search for documents in other libraries to which they have access.

Indexing Performed by the POA

Indexing is among the many functions of the Post Office Agent (POA). To learn more about POA functions, see [Section 35.5, "Role of the Post Office Agent,"](#) on page 477.

You can configure the POA for a post office to meet basic indexing needs. See [Section 39.1, "Regulating Indexing,"](#) on page 573.

To support greater indexing needs, you can set up an additional POA that is dedicated to indexing. See [Section 39.5, "Configuring a Dedicated Indexing POA \(Windows Only\),"](#) on page 577.

Not all libraries need dedicated POAs for indexing documents because indexing needs vary widely:

- ♦ In a small GroupWise system that has only one post office and one library, indexing can easily be done by the one POA.
- ♦ In a post office with heavy DMS usage, one or more additional POAs can be dedicated to indexing the documents.
- ♦ In a large system that has a DMS post office housing all libraries in the GroupWise system, indexing can be done by the DMS post office's POAs.

A library can have more than one POA dedicated to indexing its documents. Because the library's QuickFinder index is partitioned into ten separate *.idx files, an organization that is extremely document-intensive can boost indexing performance by using up to ten POAs dedicated to indexing. These POAs do not conflict with each other in performing indexing because the *.idx and *.inc files are locked during the indexing process.

You can temporarily use multiple indexing POAs for importing documents to speed up importing time.

Indexing Cycle

The frequency of indexing is determined by the POA QuickFinder Interval setting. The default is once every 24 hours at 8:00 p.m. This might be often enough in an organization where document usage is minimal, or where searching for newly-created documents is not mission-critical.

You can specify the QuickFinder Interval setting in one-hour increments. For example, a setting of 1 would allow users to find documents created as recently as an hour ago. Whether you should use a dedicated indexer at this frequency would depend on the volume (per hour) of documents that get queued for indexing.

You can set the QuickFinder Interval to 0 (zero) for continuous indexing. This is recommended for organizations where document usage is intensive, or where users routinely need to find documents that have just been created. If document usage is intensive in your organization, you might need a separate indexer server dedicated to continuous indexing because the post office server's performance could become unacceptably slow if continuous indexing is performed on it.

Bandwidth Considerations

A primary factor in network speed is bandwidth. This is the amount of data that can be passed through the network per second. If a network's bandwidth is not sufficient for handling heavy traffic, intensive document indexing can degrade network performance.

A number of elements affect network bandwidth, including cable types, transmission protocols, and hardware. Ethernet networks are susceptible to wide fluctuations in transmission speed during periods of heavy traffic. WANs can benefit from reduced network traffic.

If you locate a post office in close proximity to its users, you have less traffic through routers, bridges, and other network hardware. Running GroupWise in client/server access mode also reduces network traffic.

GroupWise users can add heavy messaging traffic to your existing network. DMS usage adds document indexing traffic as well. These factors can create much more network bandwidth usage than you have previously experienced.

Indexer Configurations

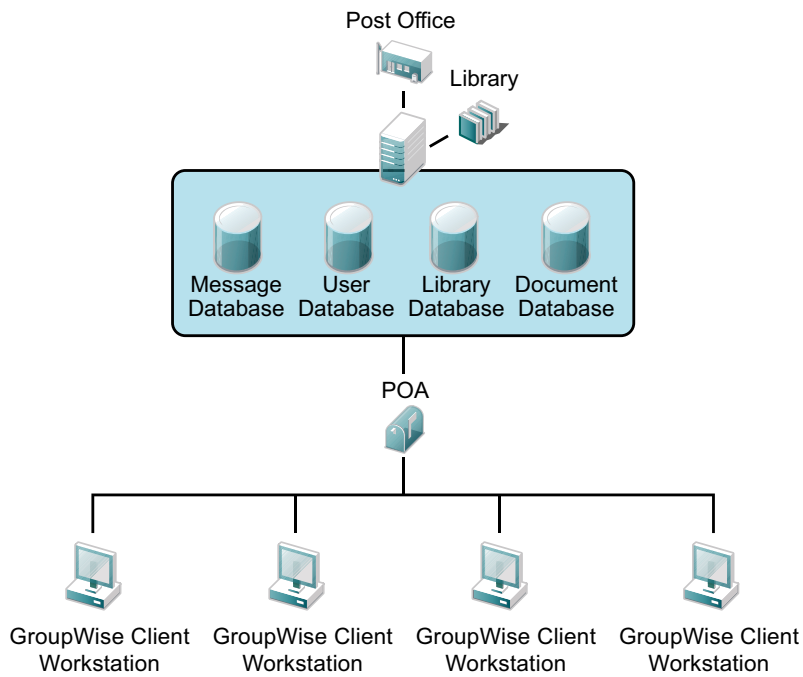
Following are five basic examples of how dedicated indexers can be configured. The examples do not cover all possibilities. You can combine elements from these configurations to customize indexing for your organization.

In all configuration examples, the post office can contain multiple libraries, although the Single Server with One POA configuration is best suited to only one library. In the other configuration examples, one or more POAs can be set up for indexing documents for all libraries in the post office.

- ♦ [“Single Server with One POA” on page 376](#)
- ♦ [“Single Server with Multiple POAs” on page 377](#)
- ♦ [“Dedicated Indexer Server” on page 378](#)
- ♦ [“Dedicated Indexer Server on an Isolated Network Segment” on page 379](#)
- ♦ [“Dedicated DMS Post Office” on page 380](#)

Single Server with One POA

One POA runs on the post office server and performs all POA functions for the post office and its libraries. This basic configuration is best suited for a small system, or a decentralized library configuration with small post offices that each have a library. For more information, see [“Centralized vs. Decentralized Library Configurations” on page 328](#).



Advantages

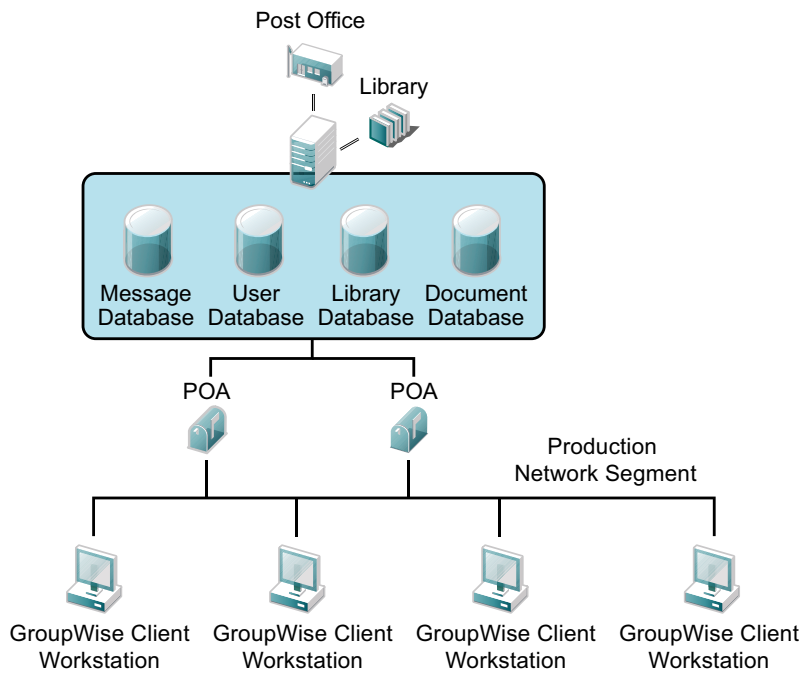
- ◆ Default configuration; no additional setup is required.
- ◆ Troubleshooting is limited to a single server.

Disadvantages

- ◆ All operations are performed on one server, which can cause performance degradation if your organization does enough DMS operations.
 - ◆ If you increase QuickFinder intervals to lessen the load on the POA, you lengthen the time users must wait to search for new files, or find modified information through new searching keywords.
-

Single Server with Multiple POAs

It is possible to run more than one POA for the same post office on the same server.



Advantages

None.

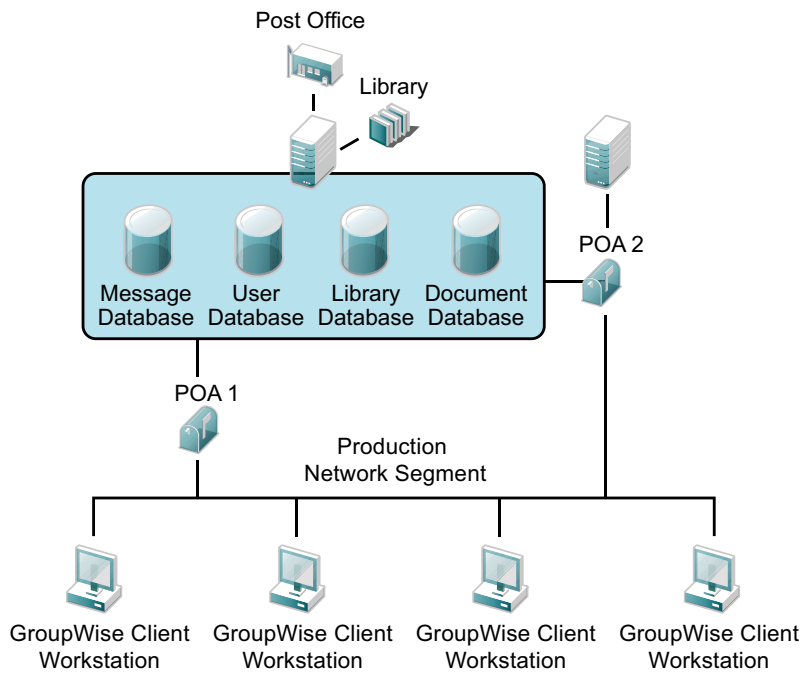
Disadvantages

- ◆ Many processes running on one server can slow it down.
 - ◆ A single point of failure can cause the server to shut down when a problem is encountered.
-

There are no advantages to running multiple POAs on the same server. If you need more than one POA, run it on a separate server, as described in [“Dedicated Indexer Server” on page 378](#)

Dedicated Indexer Server

You can have the post office on one server and a POA dedicated to indexing DMS documents on another server. This configuration is useful for systems of any size with heavy DMS usage.



Advantages

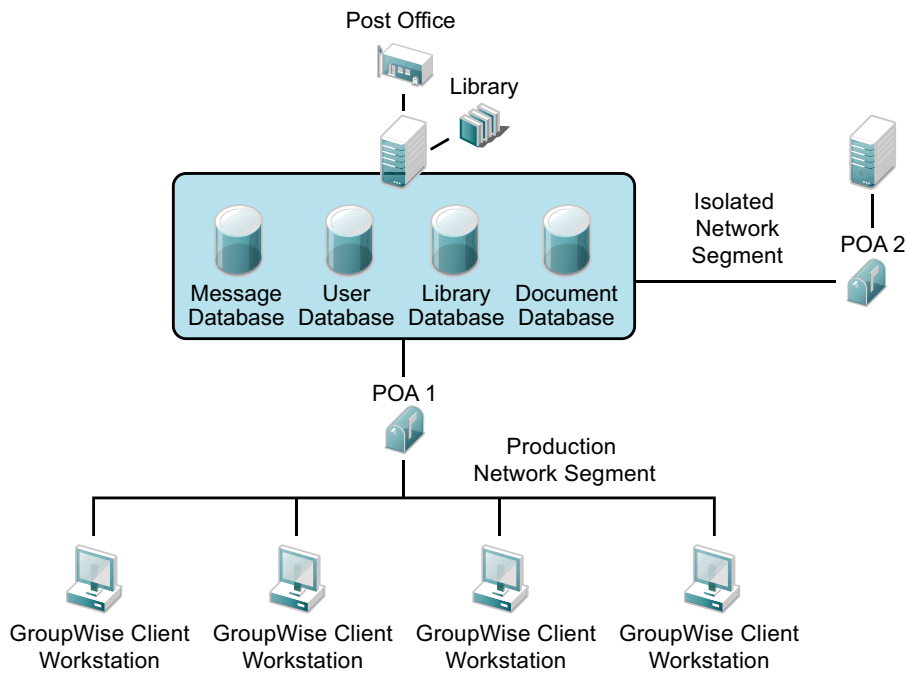
- ◆ A dedicated server for quicker DMS indexing. This is useful for organizations that are document-intensive.
- ◆ The messaging post office is not hampered by DMS indexing.

Disadvantages

- ◆ Network traffic can increase significantly during periods of intense indexing.
 - ◆ Multiple server hardware is required.
-

Dedicated Indexer Server on an Isolated Network Segment

You can have the post office on one server and a POA dedicated to indexing documents on another server that is on an isolated network segment. This configuration minimizes bandwidth congestion for the production network segment.



Advantages

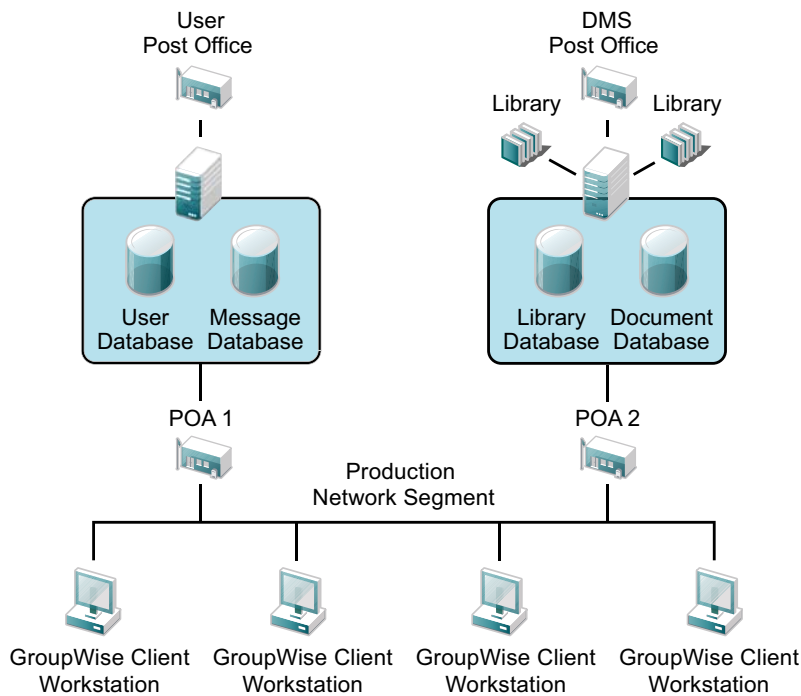
- ◆ Dedicated server for quicker DMS indexing. This is useful for organizations that are document-intensive.
- ◆ The messaging post office is not hampered by DMS indexing.
- ◆ The large amount of information that is passed between the post office server and the indexing server does not congest the bandwidth of the production network segment.

Disadvantages

- ◆ Multiple server hardware is required.
 - ◆ A dedicated network segment is required (including second network interface card that is directly linked to the indexer server).
 - ◆ For multiple indexing servers, a dedicated hub might be needed.
-

Dedicated DMS Post Office

You can have one post office that is dedicated to messaging and another to DMS. This configuration is useful for post offices that have heavy DMS usage. For a review of this configuration, see [“Centralized Libraries” on page 329](#).



Advantages	Disadvantages
<ul style="list-style-type: none"> ◆ A dedicated POA for quicker DMS indexing. This is useful for organizations that are document-intensive. ◆ The messaging post office is not hampered by DMS traffic and indexing. ◆ Logical separation of messaging and DMS databases. Processes such as backing up databases are easier. ◆ This configuration is ideal for creating a centralized library configuration. 	<ul style="list-style-type: none"> ◆ High-end hardware is required for DMS server. ◆ An additional post office and POA to be maintained. ◆ Client/server is required for searching and accessing documents. ◆ Remote access is required for users who cannot use client/server mode. This ensures that the slower store-and-forward process is used for remote searching and accessing of documents.

23.3.2 Determining Your Indexing Needs

The following table presents some indexing considerations and suggests an indexing configuration based on how the considerations pertain to your indexing needs:

Consideration	Single Server with One POA	Dedicated Indexer Server	Dedicated Indexer Server on an Isolated Network Segment	Dedicated DMS Post Office
Does the post office own multiple libraries?	No	Yes or No	Yes or No	Yes
What is the expected indexing volume (per hour)?	Light	Light or Moderate	Moderate or Heavy	Heavy

Consideration	Single Server with One POA	Dedicated Indexer Server	Dedicated Indexer Server on an Isolated Network Segment	Dedicated DMS Post Office
Is hardware available for a dedicated indexer server?	No	Yes	Yes	Yes
Could bandwidth congestion be a problem?	No	Maybe	Maybe or Yes	Yes

Use the “[Indexing Worksheet](#)” on page 382 to estimate the indexing needs of the libraries in your GroupWise system. Each worksheet accommodates three libraries.

Identify each library ([worksheet items 1 and 2](#)). Estimate the impact of each consideration in each library ([worksheet items 3 through 6](#)). Then compare your estimates for each library to the values in the table above to determine the indexing configuration for each library ([worksheet item 7](#)).

Indexing Worksheet

For instructions on how to use this worksheet, see [Section 23.3.2, “Determining Your Indexing Needs,”](#) on page 381.

	Library	Library	Library
1) Library:			
2) Library's Post Office:			
3) Multiple Libraries per Post Office?			
♦ Yes			
♦ No			
4) Expected Indexing Volume (per hour):			
♦ Light			
♦ Moderate			
♦ Heavy			
5) Additional Server Available?			
♦ Yes			
♦ No			
6) Bandwidth Congestion Possible?			
♦ Yes			
♦ Maybe			
♦ No			

7) Indexer Configuration:

- ◆ Single server with one POA
 - ◆ Dedicated indexer server
 - ◆ Dedicated indexer server on an insulated network segment
 - ◆ Dedicated DMS post office
-

23.3.3 Implementing Indexing

For libraries where a single POA running on the post office server can provide adequate indexing support for the post office's libraries, follow the instructions in [Section 39.1, "Regulating Indexing," on page 573](#) to implement indexing.

For libraries where additional POAs running on separate servers are required to support the indexing needs of the post office's libraries, follow the instructions in [Section 39.5, "Configuring a Dedicated Indexing POA \(Windows Only\)," on page 577](#) to implement indexing.

23.4 Managing Documents in Libraries

As more and more documents are added to your GroupWise libraries, you must manage the disk space occupied by libraries and respond to various changes in your GroupWise system.

- ◆ [Section 23.4.1, "Archiving and Deleting Documents," on page 383](#)
- ◆ [Section 23.4.2, "Backing Up and Restoring Archived Documents," on page 383](#)
- ◆ [Section 23.4.3, "Handling Orphaned Documents," on page 385](#)

See also [Section 22.6.2, "Managing Document Storage Areas," on page 345](#).

23.4.1 Archiving and Deleting Documents

The Document Type property determines what happens to documents whose document life in your GroupWise system has expired. For a review of the document types and document life, see [Section 21.3.2, "Document Types," on page 319](#).

You can use the Mailbox/Library Maintenance feature in ConsoleOne to archive and delete documents on demand, as described in [Section 30.4, "Reducing the Size of Libraries and Document Storage Areas," on page 428](#).

You can also configure the POA to archive and delete documents on a regular schedule, as described in [Section 36.4.2, "Scheduling Disk Space Management," on page 520](#).

23.4.2 Backing Up and Restoring Archived Documents

When documents are archived, they are physically moved to a directory in the post office, where disk space can be limited. You should move archived documents to your backup medium regularly.

- ◆ ["Moving Archived Documents to Backup" on page 384](#)
- ◆ ["Restoring Archived Documents" on page 384](#)

Moving Archived Documents to Backup

When documents are archived, they are placed in automatically created archive directories. Each library has a set of archive directories. For example, `gwdms` (GroupWise Document Management Services) is one of the post office's directories. The library directories exist under it, named `lib0001-ff`. Under each library directory is an archive directory, under which are the sequentially-numbered archival directories, named `arnnnnnn` (where `nnnnnn` is an integer with leading zeros). Each `arnnnnnn` directory is an archive set. To view the `gwdms` directory, see [“Post Office Directory”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

To move archived documents to backup:

- 1 Make sure you have a backup medium (such as tape, CD, or DVD) operating with your system.
- 2 Make sure you have already archived documents that have reached their expiration dates. Documents that have not been archived cannot be removed to a backup medium.
- 3 Start the software for your backup medium.
- 4 When the backup software asks for the location of your archive files, give the full path.

Example:

```
j:\post_office\gwdms\lib0\archive\ar000001
```

If users need the backed-up documents in the future, see [“Restoring Archived Documents”](#) on page 384.

Restoring Archived Documents

When a user tries to access a document that has been archived, one of two things happens:

- ♦ If the document is in the post office archive set, and has not yet been physically moved from the archive location, the document opens normally. The user does not realize it was archived. The document is unarchived from the archive set at that time; that is, it is moved back to the library document directory from which it was archived. It is also given a new archive date according to the document type.
- ♦ The user sees a message indicating the document cannot be opened. In this case, the archive set containing the document has been physically moved to a backup medium. Therefore, the document cannot be automatically unarchived. In this case, the user might contact you, asking you to locate or recover the document. You can restore either the document's BLOB or the archive set that contains the BLOB. After the document is restored to its archive directory, the user will be able to open the document normally.

To restore archived documents from a backup medium:

- 1 Obtain the Document Number for the document the user was trying to access.
- 2 In the GroupWise Windows client, click *Tools > Find*.
- 3 Specify the Document Number, then click *OK*.
- 4 Right-click the document in the *Find Results* listing, then click *Properties > Version*.
- 5 Note the archive directory in the path listed in the *Current Location* field.
The subdirectory listed after the `..\archive` directory is the archive set containing the document, for example, `\ar000001`.
- 6 If you have the ability to recover individual files from your backup medium, also note the BLOB file name listed in the *Current Filename* field.

- 7 Determine where you backed up the archive set, then copy either the archive set or the individual BLOB file to the archive directory specified in the Current Location field that you noted earlier.
- 8 You can now notify the user that the requested document is available.
- 9 When you are sure the user has opened the document (causing it to be unarchived), you should delete any files remaining in that archive directory because you have already backed them up.

23.4.3 Handling Orphaned Documents

If you remove public rights for a library, some documents might become inaccessible. For example, if a user who has been denied access to the library is the only user who had access to certain documents, those documents become orphaned. No other user can access or search for those orphaned documents. This is because document security is controlled by the user listed in the Author and Creator fields in the document's properties. In other words, if the author or creator no longer has access to a document, neither does anyone else.

However, orphaned documents can be reassigned to another author so that someone can access them again. This can be done in one of two ways:

- ♦ In ConsoleOne, the Analyze/Fix Library action in Mailbox/Library Maintenance can reassign orphaned documents to a specified user. Then, the new user has access to all orphaned documents in that library. For more information, see [Section 28.2, "Analyzing and Fixing Library and Document Information,"](#) on page 416.
- ♦ A librarian has the ability to alter the Author field of documents. Therefore, a librarian can replace the previous user's GroupWise ID with his or her own ID. In doing so, the librarian becomes the new author of the document. This can also be done as a mass operation for multiple documents with varying user IDs in the Author field. For more information, see [Section 22.6.4, "Adding and Training Librarians,"](#) on page 350.

24 Integrations

Document-producing applications can be integrated with GroupWise Document Management Services (DMS) to allow GroupWise management control over files produced by the integrated applications. Integrations provide code specifically designed to allow function calls, such as Open or Save, to be redirected to the GroupWise Windows client. This allows GroupWise dialog boxes to be displayed instead of the application's normal dialog boxes for the integrated functions.

GroupWise DMS includes standard integrations for the following applications:

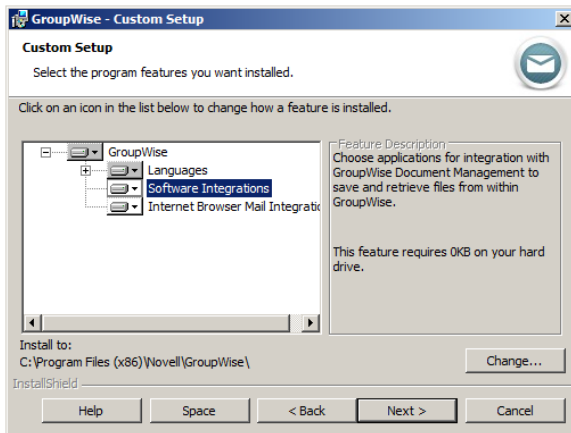
- ♦ Corel Presentations 7.x through 10.x
- ♦ Corel Quattro Pro 7.x and 8.x
- ♦ Corel WordPerfect 6.1 through 10.x
- ♦ Lotus Word Pro 96 and 97
- ♦ Microsoft Binder 97
- ♦ Microsoft Excel 95, 97, 2000, and 2002
- ♦ Microsoft PowerPoint 97, 2000, and 2002
- ♦ Microsoft Word 95, 97, 2000, and 2002
- ♦ Microsoft Office 2007
- ♦ OpenOffice.org (Novell version)

Other applications can be integrated manually using the `gwappint.inf` file.

- ♦ [Section 24.1, "Setting Up Integrations during Windows Client Installation," on page 387](#)
- ♦ [Section 24.2, "Setting Up Integrations Using the gwappint.inf File," on page 388](#)
- ♦ [Section 24.3, "Controlling Integrations in the GroupWise Windows Client," on page 393](#)

24.1 Setting Up Integrations during Windows Client Installation

The GroupWise Windows client Setup program can offer users the opportunity to integrate their document-producing applications during client installation.



This dialog box lists the applications that can be integrated with GroupWise that are currently installed on users' workstations. Therefore, it is important to make sure that the applications to integrate are installed *before* the GroupWise client is installed. However, it does not matter whether GroupWise and the applications are installed to run from the network or from the users' workstations. The integrations work with any combination of installation choices.

After selecting applications to integrate during GroupWise client integration, users can manage their integrations in the GroupWise client, as described in [“Integrating GroupWise with Your Applications”](#) in [“Document Management”](#) in the *GroupWise 2012 Windows Client User Guide*.

If users need to install and integrate applications *after* installing the GroupWise client, they can install the new applications, then reinstall the GroupWise client so that they can select the new applications during GroupWise client installation. If reinstalling the GroupWise client is not an option, you might need to assist them in setting up additional integrations, as described in [Section 24.2, “Setting Up Integrations Using the gwappint.inf File,”](#) on page 388.

24.2 Setting Up Integrations Using the gwappint.inf File

The `gwappint.inf` file controls how document-producing applications are integrated with the GroupWise Windows client. During client installation, the `gwappint.inf` file is installed in the following directory:

```
c:\Program Files\Novell\GroupWise
```

It is a text file that can be viewed and modified in a text editor such as Notepad. However, a regular Windows user does not have sufficient rights to edit the `gwappint.inf` file in its default location. Therefore, when a user accesses integration settings in the GroupWise Windows client by using *Tools > Options > Documents > Integrations*, a copy of the `gwappint.inf` file is created in the following directory:

```
Windows XP: c:\Documents and Settings\user_name\Application Data\Novell\GroupWise
```

```
Windows Vista: c:\Users\user_name\AppData\Local\Novell\GroupWise
```

```
Windows 7: c:\Users\user_name\AppData\Roaming\Novell\GroupWise
```

In that location, the GroupWise client user has sufficient rights to edit the file. The GroupWise Windows client always checks the user-editable location first.

You might want to print the `gwappint.inf` file from a user workstation to help you understand how integrations have been set up for your users during GroupWise client installation.

- ♦ [Section 24.2.1, “Understanding the Three Levels of Integration,” on page 389](#)
- ♦ [Section 24.2.2, “Understanding the gwappint.inf File,” on page 390](#)
- ♦ [Section 24.2.3, “Editing the gwappint.inf File,” on page 392](#)

24.2.1 Understanding the Three Levels of Integration

The `gwappint.inf` file provides for three different levels of integration, to meet the needs of different types of document-producing applications:

- ♦ [“ODMA Integration” on page 389](#)
- ♦ [“Point-to-Point Integration” on page 389](#)
- ♦ [“No Integration” on page 389](#)

ODMA Integration

The Open Document Management API (ODMA) is an industry standard for applications and document management programs to use in achieving seamless integration. ODMA is platform-independent. GroupWise DMS is 32-bit ODMA-compliant, and can automatically integrate with all 32-bit ODMA-compliant applications. Applications that are not 32-bit ODMA-compliant must have integrations created for them to be used with GroupWise DMS.

Point-to-Point Integration

This integration involves applications that are not 32-bit ODMA-compliant. Novell has written macros for various applications, such as Microsoft Word, which allow them to be integrated with GroupWise. This provides the same functionality as for 32-bit ODMA-integrated applications. These applications can be selected for integration when the GroupWise client is installed.

Integration macros are written in the macro language of the application being integrated with GroupWise. Macro calls are made to GroupWise dialog boxes to replace access of the application's own dialog boxes (for example, Open and Save).

No Integration

Non-integrated applications rely on Windows associations. When a reference icon is selected in GroupWise, the file's extension is examined to determine which application to use. The application is launched and the file is opened.

Functions performed in a non-integrated application are not managed by GroupWise. So, if the file is renamed or saved to a different location, the file is not part of a GroupWise library. When the file is opened later, a message is displayed reminding the user that the file is not under management of GroupWise. However, if you simply edit the file and re-save it without changing the name or location, GroupWise continues to provide management of the file.

24.2.2 Understanding the gwappint.inf File

The gwappint.inf file is located in the c:\Program Files\Novell\GroupWise subdirectory. It includes the following sections and lines:

- ♦ [executable_name] sections
 - Integration= line
 - DualExe= line
 - AppName= line
 - AppKey= line
- ♦ [ODMA Application Extensions] section
- ♦ [Integration State] section
- ♦ [Non-Integrated Defaults] section
 - WaitInterval= line
 - ShowMessage= line

[executable_name] Sections

The gwappint.inf file contains one [executable_name] section for each integrated application. It supplies the name of the executable for the program being integrated.

Integration= Line

Each [executable_name] section must have an Integration= line, where digits identify the type of integration employed for the executable:

```
Integration = 0 (No Integration)
Integration = 1 (Point-to-Point Integration)
Integration = 2 (ODMA Integration)
```

DualExe= Line

Some programs, such as Lotus Word Pro, use a small startup executable that, in turn, calls the main program. Use the DualExe= line to specify the name of the main executable. You can specify the full path to the main executable, or you can specify the path relative to the startup executable.

AppName= Line

The AppName= line assigns the application an arbitrary name for use in the [ODMA Application Extensions] and [Integration State] sections.

AppKey= Line

The AppKey= line is used only with point-to-point integrations (Integration=1). It specifies a value used by GroupWise to pass information to and from the integrated application. The value must be unique among the point-to-point integrations defined in the gwappint.inf file.

Examples Based on Standard Integrations

The table below shows how the standard integrations are implemented in the gwappint.inf file:

Application	Executable	Version	Comments
Corel Presentations	prwin.exe	3	If it is already installed on the workstation, GroupWise installation changes the Integrations= line to 0 and the application is available for selection as a non-integrated application.
		7	For ODMA integration, change the DualExe= line to system\prwin70.exe and the Integrations= line to 2.
		8, 9, 10	For ODMA integration, change the Integrations= line to 2.
Corel Quattro Pro	qpw.exe	6.1	If it is already installed on the workstation, the GroupWise client installation changes the Integrations= line to 0 and the application is available for selection as a non-integrated application.
		7	For ODMA integration, change the Integrations= line to 2
Corel WordPerfect	wpwin.exe	6.1	If it is already installed on the workstation, the GroupWise client installation changes the Integrations= line to 0 and the application is available for selection as a non-integrated application.
		7	For ODMA integration, change the DualExe= line to system\wpwin7.exe and the Integrations= line to 2.
		8, 9, 10	For ODMA integration, no DualExe= line is needed. Change the Integrations= line to 2.
Lotus Word Pro	wordpro.exe	96	This application is 32-bit ODMA-compliant. Therefore, if it is installed before GroupWise, it is available for selection as an ODMA-integrated application.
		97	For ODMA integration, change the DualExe= line to system\wordpro.exe and the Integrations= line to 2.
Microsoft Binder	binder.exe	97	This application is 32-bit ODMA-compliant. Therefore, if it is installed before GroupWise, it is available for selection as an ODMA-integrated application.
Microsoft Excel	excel.exe	95, 97, 2000, 2002	The Integrations= line is set to 1 for both versions.
Microsoft PowerPoint	powerpnt.exe	97, 2000, 2002	This application is 32-bit ODMA-compliant. Therefore, if it is installed before GroupWise, it is available for selection as an ODMA-integrated application.
Microsoft Word	winword.exe	95	If it is already installed on the workstation, GroupWise installation changes the Integrations= line to 1 and the application is available for selection for point-to-point integration.
		97, 2000, 2002	For ODMA integration, change the Integrations= line to 2.

[ODMA Application Extensions] Section

The [ODMA Application Extensions] section lists the file extensions GroupWise associates with particular document-producing applications. Examples include:

Application	File Extension
Corel WordPerfect	.wpd
Microsoft Excel	.xls
Microsoft PowerPoint	.ppt
Microsoft Word	.doc

[Integration State] Section

The [Integration State] section records whether the user has turned integrations on or off for integrated applications.

[Non-Integrated Defaults] Section

The [Non-Integrated Defaults] section provides two configuration settings that apply to all non-integrated applications:

- ◆ [WaitInterval= line](#)
- ◆ [ShowMessage= line](#)

WaitInterval= Line

The `WaitInterval=` line specifies a number of milliseconds for the GroupWise client to wait before it attempts to communicate with a non-integrated process. The wait interval allows the application to start completely before GroupWise contacts it. The default wait interval is 1000 milliseconds (one second).

The default setting supplied in the [Non-Integrated Defaults] section can be overridden for specific applications by including a `WaitInterval=` line in the application's [\[executable_name\]](#) section.

ShowMessage= Line

The `ShowMessage=` line indicates whether or not to display a message to the GroupWise client user if GroupWise cannot contact a non-integrated application. Use `ShowMessage=1` to display the message or `ShowMessage=0` to suppress the message.

The default setting supplied in the [Non-Integrated Defaults] section can be overridden for specific applications by including a `ShowMessage=` line in the application's [\[executable_name\]](#) section.

24.2.3 Editing the gwappint.inf File

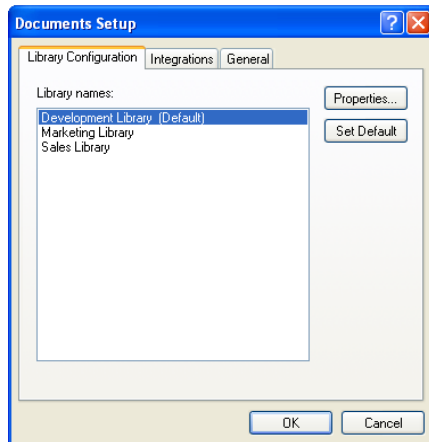
The `gwappint.inf` file is a text file that can be modified using any text editor (Notepad, for example). By editing the `gwappint.inf` file, you can add integrations for applications for which Novell has not provided integrations. It is located in the `c:\Program Files\Novell\GroupWise` subdirectory.

24.3 Controlling Integrations in the GroupWise Windows Client

For the convenience of GroupWise Windows client users, some settings in the `gwappint.inf` file can be modified from the client.

In the GroupWise client:

- 1 Click *Tools > Options > Documents > Integrations*.

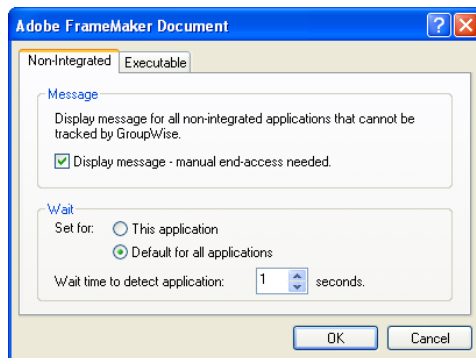


The *Integrations* tab of the Documents Setup dialog box lets users turn integrations on and off for the listed registered applications.

If the application that users want to integrate is does not appear in the registered applications list, users must first make sure the application is installed on their workstations. Then they can either reinstall the GroupWise client or modify the `gwappint.inf` file as described in [Section 24.2, “Setting Up Integrations Using the gwappint.inf File,” on page 388](#).

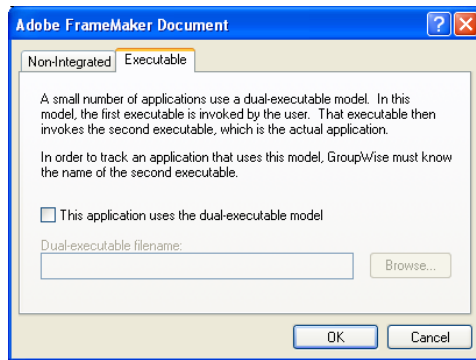
The users’ selections on the Integrations tab are recorded in the [\[Integration State\]](#) section of the `gwappint.inf` file.

- 2 Select an application to configure integration for, then click *Advanced*.



The *Non-Integrated* tab enables users to set values for the `ShowMessage=` and `WaitInterval=` lines in the `gwappint.inf` file.

- 3 Click *Executable*.



The *Executable* tab enables users to set the `DualExe=` line in the `gwappint.inf` file.

- 4 Click *OK* twice to save the updated integration information.

If users check the contents of the `gwappint.inf` file in the Windows `system32` subdirectory, they see their integration configuration changes reflected there.

VIII Databases

- ♦ Chapter 25, “Understanding GroupWise Databases,” on page 397
- ♦ Chapter 26, “Maintaining Domain and Post Office Databases,” on page 401
- ♦ Chapter 27, “Maintaining User/Resource and Message Databases,” on page 409
- ♦ Chapter 28, “Maintaining Library Databases and Documents,” on page 415
- ♦ Chapter 29, “Synchronizing Database Information,” on page 419
- ♦ Chapter 30, “Managing Database Disk Space,” on page 423
- ♦ Chapter 31, “Backing Up GroupWise Databases,” on page 431
- ♦ Chapter 32, “Restoring GroupWise Databases from Backup,” on page 433
- ♦ Chapter 33, “Retaining User Messages,” on page 441
- ♦ Chapter 34, “Stand-Alone Database Maintenance Programs,” on page 447

For additional assistance in managing your GroupWise system, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

25 Understanding GroupWise Databases

Your GroupWise system includes numerous databases where vital information is stored.

- ♦ [Section 25.1, “Domain Databases,” on page 397](#)
- ♦ [Section 25.2, “Post Office Databases,” on page 398](#)
- ♦ [Section 25.3, “User Databases,” on page 398](#)
- ♦ [Section 25.4, “Message Databases,” on page 398](#)
- ♦ [Section 25.5, “Library Databases,” on page 399](#)
- ♦ [Section 25.6, “Guardian Databases,” on page 399](#)

NOTE: The maximum size for all types of GroupWise databases is 4 GB. Domains, post offices, and mailboxes consist of multiple databases, so there are no physical size limits for domains, post offices, and mailboxes. However, there are feasibility limitations based on potentially time-consuming activities such as backup/restore procedures.

25.1 Domain Databases

The domain database ([wpdomain.db](#)) in each domain contains all administrative information for the domain, including:

- ♦ Address information about all GroupWise objects (such as users and resources), post offices, and gateways in the domain
- ♦ System configuration and linking information for the domain’s MTA
- ♦ Address and message routing information to other domains

The first domain you create is the primary domain. In the primary domain, the `wpdomain.db` file contains all administrative information for your entire GroupWise system (all domains, post offices, users, and so on). Because the `wpdomain.db` file in the primary domain is so crucial, you should back it up regularly and keep it secure. See [Section 31.1, “Backing Up a Domain,” on page 431](#).

You can re-create your entire GroupWise system from the primary domain `wpdomain.db` file; however, if the primary domain `wpdomain.db` file becomes unusable, you can no longer make administrative updates to your GroupWise system.

Every domain you create after the primary domain is a secondary domain. The contents of secondary domains are automatically synchronized with the primary domain.

For the location of the domain database, see [“Domain Directory” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*](#). For additional domain information, see [Section 41.3, “Information Stored in the Domain,” on page 622](#).

The database version for GroupWise 2012 domain databases is 1200.

25.2 Post Office Databases

The post office database (`wphost.db`) in each post office contains all administrative information for the post office, including a copy of the GroupWise Address Book. This information is necessary for users to send messages to others in the GroupWise system.

For the location of the post office database, see “Post Office Directory” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*. For more post office information, see Section 35.3, “Information Stored in the Post Office,” on page 472.

The database version for GroupWise 2012 post office databases is 1200.

25.3 User Databases

Each member of the post office has a personal database (`userxxx.db`) that represents the user’s mailbox. The user database contains the following:

- ♦ Message header information
- ♦ Pointers to messages
- ♦ Personal groups
- ♦ Personal address books
- ♦ Rules

When a member of another post office shares a folder with one or more members of the local post office, a “prime user” database (`puxxxxx.db`) is created to store the shared information. The prime user is the owner of the shared information.

Local user databases and prime user databases are stored in the `ofuser` directory in the post office.

Because resources are addressable just like users, resources also have user databases.

For the location of user databases in the post office, see “Post Office Directory” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*. For more post office information, see Section 35.3, “Information Stored in the Post Office,” on page 472.

25.4 Message Databases

Each member of the post office is assigned to a message database (`msgnnn.db`) where the body portions of messages are stored. Many users in a post office share a single message database. There can be as many as 255 message databases in the post office (numbered from 0 to 254). Message databases are stored in the `ofmsg` directory in the post office.

Outgoing messages from local senders are stored in the message database assigned to each sender. Incoming messages from users in other post offices are stored in the message database with the same name as the message database assigned to the sender in his or her own post office. In each case, only one copy of the message is stored in the post office, no matter how many members of the post office it is addressed to.

For the location of message databases in the post office, see “Post Office Directory” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*. For more post office information, see Section 35.3, “Information Stored in the Post Office,” on page 472.

25.5 Library Databases

A library is a collection of documents and document properties stored in a database system that can be managed and searched. You do not need to set up libraries unless you are using GroupWise Document Management Services (DMS). See [Part VII, “Libraries and Documents,”](#) on page 313.

The databases for managing libraries are stored in the `gwdms` directory and its subdirectories in the post office.

The `dmsh.db` file is a database shared by all libraries in the post office. It contains information about where each library in the post office is located.

Each library has its own subdirectory in the `gwdms` directory. In each library directory, the `dmxxxnn01-FF.db` files contain information specific to that library, such as document properties and what users have rights to access the library.

For the location of library databases in the post office, see [“Post Office Directory”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*. For more post office information, see [Section 35.3, “Information Stored in the Post Office,”](#) on page 472.

The actual documents in a library are not kept in the library databases. They are kept in a document storage area, which consists of a series of directories for storing documents. Documents are encrypted and stored in BLOBs (binary large objects) to make document management easier. A document, its versions, and related objects are stored together in the same BLOB.

A document storage area might be located in the post office itself, or in some other location where more storage space is available. If it is located in the post office, the document storage area can never be moved. Therefore, storing documents in the post office directory structure is not usually recommended. If it is stored outside the post office, a document storage area can be moved when additional disk space is required.

See [Chapter 22, “Creating and Managing Libraries,”](#) on page 323 and [Chapter 23, “Creating and Managing Documents,”](#) on page 359 for more information about Document Management Services.

25.6 Guardian Databases

The guardian database (`ngwguard.db`) serves as the master copy of the data dictionary information for the following subordinate databases in the post office:

- ◆ User databases (`userxxx.db`)
- ◆ Message databases (`msgnnn.db`)
- ◆ Prime user databases (`puxxxxx.db`)
- ◆ Library databases (`dmsh.db` and `dmxxxnn01-FF.db`)

The guardian database is vital to GroupWise functioning. Therefore, the POA has an automated back-up and roll-forward process to protect it. The POA keeps a known good copy of the guardian database called `ngwguard.fbk`. Whenever it modifies the `ngwguard.db` file, the POA also records the transaction in the roll-forward transaction log called `ngwguard.rfl`. If the POA detects damage to the `ngwguard.db` file on startup or during a write transaction, it goes back to the `ngwguard.fbk` file (the “fall back” copy) and applies the transactions recorded in the `ngwguard.rfl` file to create a new, valid and up-to-date `ngwguard.db`.

In addition to the POA back-up and roll-forward process, you should still back up the `ngwguard.db`, `ngwguard.fbk`, and `ngwguard.rfl` files regularly to protect against media failure. Without a valid `ngwguard.db` file, you cannot access your email. With current `ngwguard.fbk` and `ngwguard.rfl` files, a valid `ngwguard.db` file can be rebuilt should the need arise.

The [ngwguard.dc](#) file is the structural template for building the guardian database and its subordinate databases. Also called a dictionary file, the `ngwguard.dc` file contains schema information, such as data types and record indexes. If this dictionary file is missing, no additional databases can be created in the post office.

26 Maintaining Domain and Post Office Databases

Occasionally, it is necessary to perform maintenance tasks on domain databases ([wpdomain.db](#)) or post office databases ([wphost.db](#)). The frequency depends on the reliability of your network and your own experience of how often problems are likely to occur. The following tasks help you maintain the integrity of your domain and post office databases:

- ♦ [Section 26.1, “Validating Domain or Post Office Databases,” on page 401](#)
- ♦ [Section 26.2, “Recovering Domain or Post Office Databases,” on page 402](#)
- ♦ [Section 26.3, “Rebuilding Domain or Post Office Databases,” on page 405](#)
- ♦ [Section 26.4, “Rebuilding Database Indexes,” on page 407](#)

NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

To further protect your GroupWise system against loss of domain and post office information, see:

- ♦ [Chapter 31, “Backing Up GroupWise Databases,” on page 431](#)
- ♦ [Chapter 32, “Restoring GroupWise Databases from Backup,” on page 433](#)

To ensure that the same information exists in all domain and post office databases throughout your GroupWise system, see:

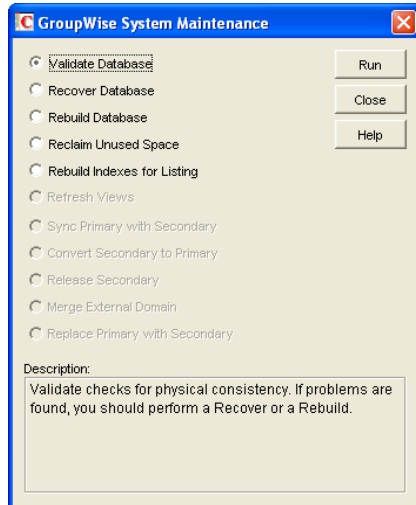
- ♦ [Section 29.5, “Synchronizing the Primary Domain from a Secondary Domain,” on page 422](#)
- ♦ [Section 29.4, “Synchronizing a Secondary Domain,” on page 421](#)
- ♦ [Section 29.2, “Synchronizing a Post Office,” on page 420](#)

26.1 Validating Domain or Post Office Databases

You can validate the data in the domain and post office databases at any time without interrupting normal GroupWise operation. The frequency can vary depending on the size of your system and the number of changes you make to users, resources, and distribution lists.

- 1 Make sure you have full administrative rights to the domain and post office database directories you are validating.
- 2 In ConsoleOne, browse to and select the Domain object or Post Office object where you want to validate the database.

3 Click *Tools > GroupWise Utilities > System Maintenance*.



4 Click *Validate Database > Run*.

5 When prompted, make sure the *Path to Database* is correct. If an incorrect path is displayed, browse to and select the path to the database being validated. Click *OK*.

You are notified if there are any physical problems, so you can then recover or rebuild the database.

See [Section 26.2, “Recovering Domain or Post Office Databases,”](#) on page 402 and [Section 26.3, “Rebuilding Domain or Post Office Databases,”](#) on page 405.

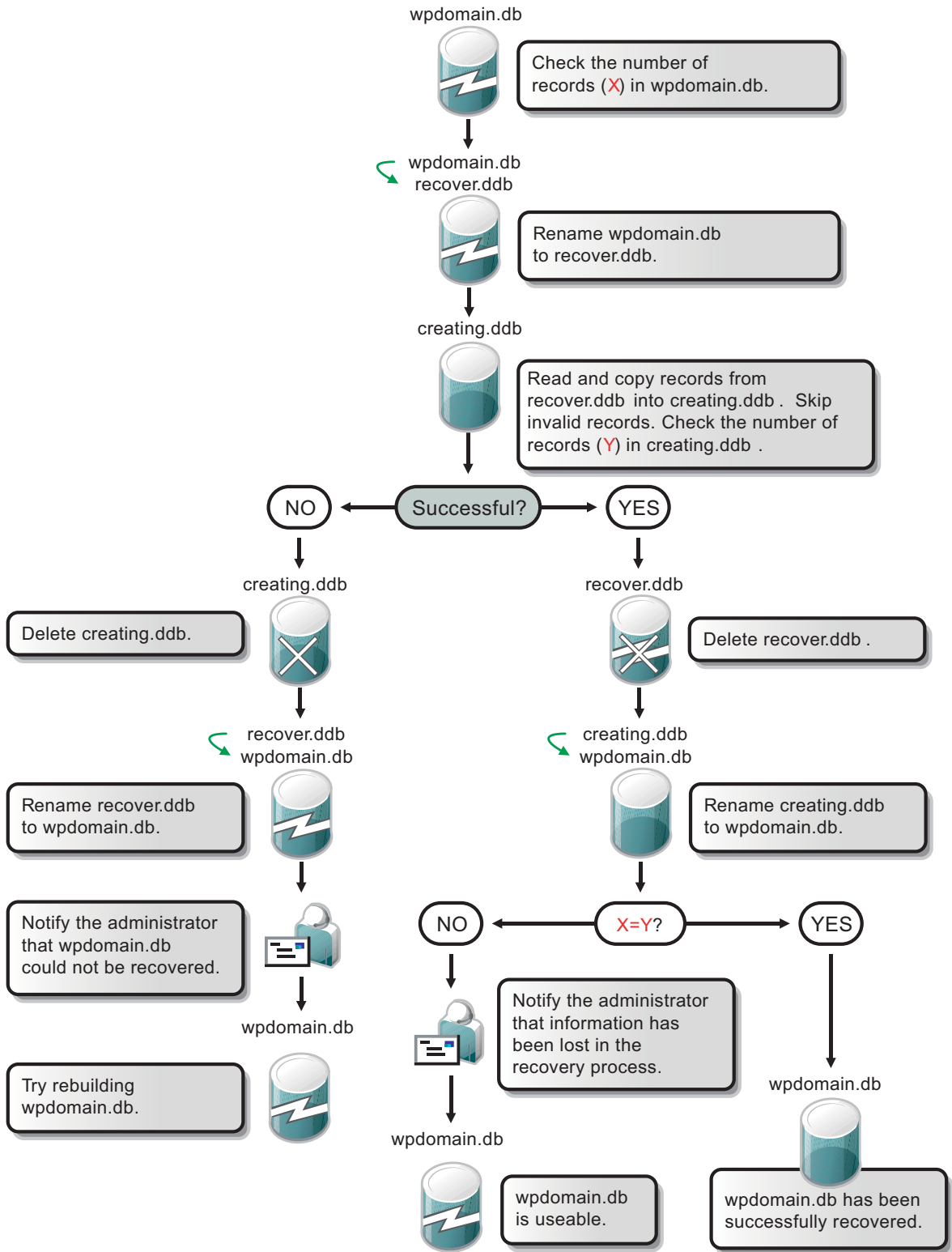
26.2 Recovering Domain or Post Office Databases

The database recover process corrects physical problems in the database structure, but does not update incorrect information contained in the database.

If you receive an administrative message informing you that an internal database error has occurred, or if you detect database damage and don't want to take users out of GroupWise, you can recover the database. If no errors are reported after the recover process, you do not need to take further action.

The recover process is run against a copy of the domain database (`wpdomain.db`) or post office database (`wphost.db`). Therefore, while the recover process is running, you can continue to access the database through ConsoleOne and you do not need to stop the MTA or the POA.

As the copy of the database is created, the recover process skips invalid records. If the number of records in the original `wdomain.db` file or `wphost.db` file is different from the number in the new, valid copy, GroupWise sends an administrative message informing you that data has been lost. When the recover process is completed, the backup database is deleted.



For convenience, the agents are configured by default to automatically recover domain and post office databases whenever a physical problem is encountered. See [“Recovering the Domain Database Automatically or Immediately” on page 667](#) and [“Recovering the Post Office Database Automatically or Immediately” on page 535](#).

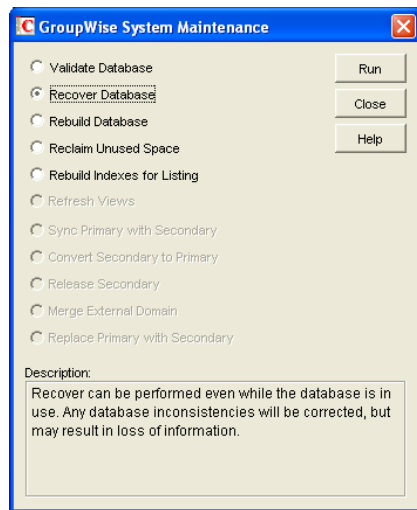
To recover a specific database in ConsoleOne:

- 1 Make sure you have network access to the domain or post office directory for the database you are recovering.

If you have administration rights in the primary domain, you can recover the primary domain database, the post office databases in the primary domain, and any secondary domain databases.

From a secondary domain, you can recover the secondary domain database and the post office databases in the secondary domain.

- 2 Make sure you have sufficient disk space for the copy of the database that is created during recovery.
- 3 In ConsoleOne, browse to and select the Domain object or Post Office object where you want to recover the database.
- 4 Click *Tools > GroupWise Utilities > System Maintenance*.



- 5 Click *Recover Database > Run*.
- 6 When prompted, make sure the *Path to Database* is correct. If an incorrect path is displayed, browse to and select the path to the database being validated. Click *OK*.

If recovery is successful, the backup database is deleted, and the new domain database is renamed to `wpdomain.db`, or the new post office database is renamed to `wphost.db`.

If recovery fails for any reason, the backup database is copied back to `wpdomain.db` or `wphost.db`. If any data was lost, you are notified by an administrative message.

You have several options for retrieving lost data from other sources:

- ♦ If data has been lost from the primary domain, you can synchronize it with a secondary domain that is known to contain current information. See [Section 29.5, “Synchronizing the Primary Domain from a Secondary Domain,” on page 422](#).

- ♦ If data has been lost from a secondary domain, you can synchronize it with the primary domain. See [Section 29.4, “Synchronizing a Secondary Domain,”](#) on page 421.
- ♦ You can also rebuild the database at a later time when you have exclusive access to the database where the data has been lost. See [Section 26.3, “Rebuilding Domain or Post Office Databases,”](#) on page 405.

26.3 Rebuilding Domain or Post Office Databases

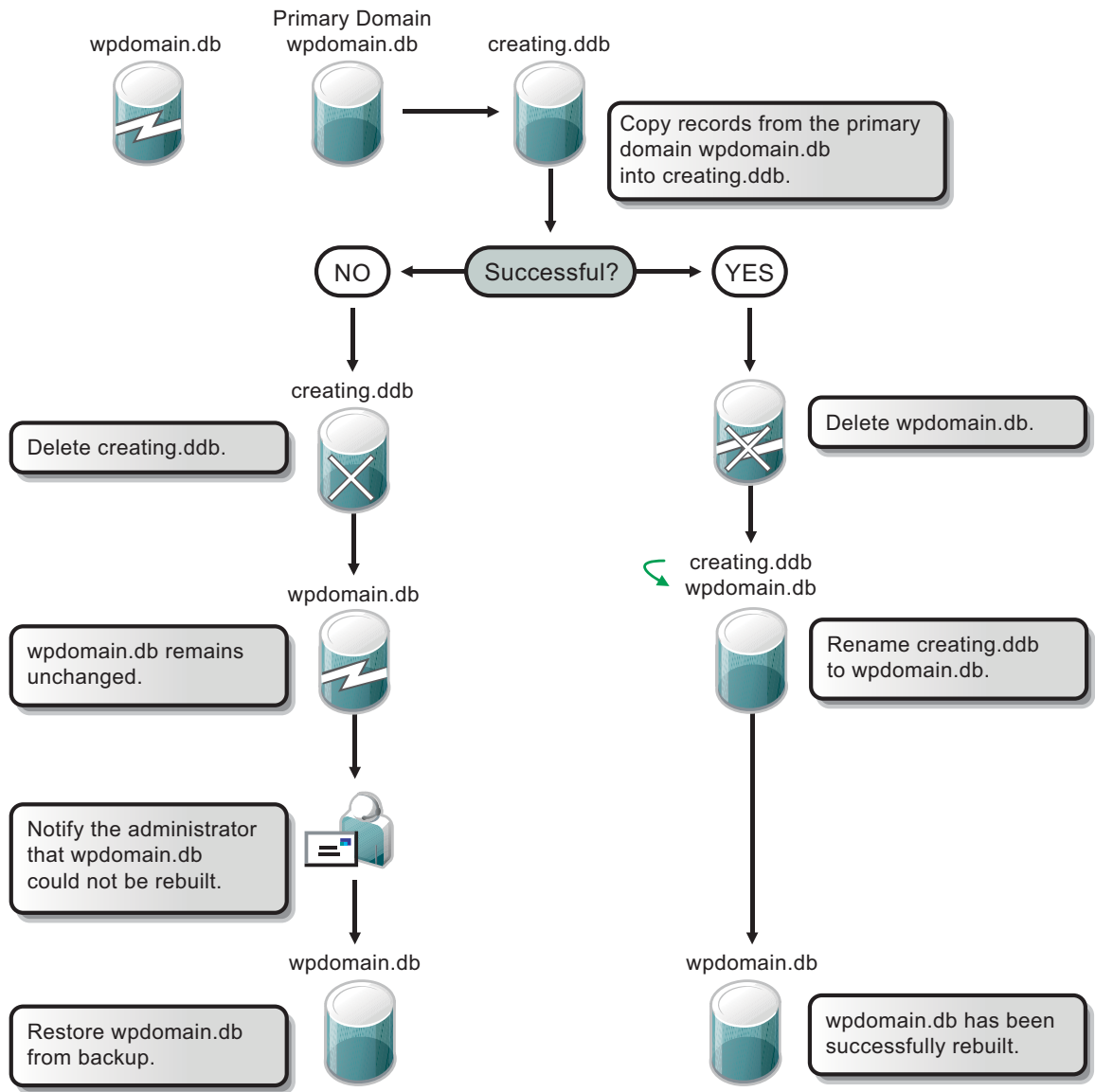
In addition to correcting the physical problems resolved by the database recover process, the rebuild process updates user and object information in a domain database (`wpdomain.db`) or post office database (`wphost.db`). However, the process requires that no users or GroupWise agents (MTA or POA) have access to the database during the rebuild process.

You should rebuild a domain or post office database if you encounter any of the following conditions:

- ♦ Objects are not being replicated between domains.
- ♦ The agent that writes to the database went down unexpectedly.
- ♦ The server where the database resides went down unexpectedly.
- ♦ You receive an administrative message informing you that an internal database error has occurred or there is database damage and you think there might be data loss.
- ♦ You ran the recover database process and received a notification of data loss.

When you rebuild a secondary domain database, information is retrieved from the primary domain. When you rebuild a post office database, information is retrieved from the domain it belongs to.

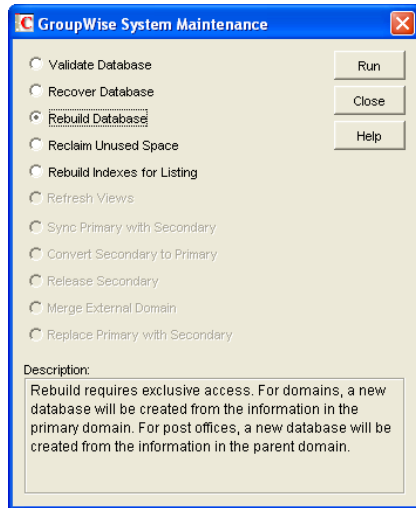
During the rebuild process, a backup of the domain or post office database is created as well as a new `wdomain.db` or `wphost.db`. The records from the primary domain database are copied into the new `wdomain.db`. There should not be any data loss. When the rebuild process is complete, the temporary database and the backup database are deleted.



To rebuild a database:

- 1 Stop all GroupWise agents that might access the database during the rebuild, as described in [“Stopping the MTA” on page 663](#) and [“Stopping the POA” on page 530](#).
- 2 (Conditional) If you are rebuilding a post office database, have all users exit GroupWise, then disable the post office before the rebuild, as described in [Section 12.9, “Disabling a Post Office,” on page 212](#).
- 3 Make sure you have sufficient disk space for the copy of the database that is created during the rebuild process.

- 4 In ConsoleOne:
 - 4a (Conditional) If you are rebuilding a domain database, connect to the primary domain.
or
 - 4b (Conditional) If you are rebuilding a post office database, connect to the domain that owns the post office.
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, "Select Domain,"](#) on page 69.
- 5 Browse to and select the Domain object or Post Office object where you want to rebuild the database.
- 6 Click *Tools > GroupWise Utilities > System Maintenance*.



- 7 Click *Rebuild Database > Run*.
- 8 When prompted, make sure the Path to Database is correct. If an incorrect path is displayed, browse to and select the path to the database being rebuilt. Click OK.

26.4 Rebuilding Database Indexes

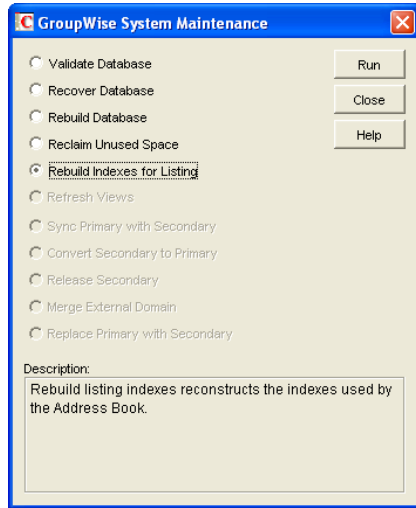
Each domain database (`wpdomain.db`) and post office database (`wphost.db`) contains three indexes that are used to determine the order of the Address Book: the system index, the domain index, and the post office index. When you display the GroupWise Address Book, the system index is used. When you display a domain-level Address Book, the domain index is used, and when you display the Address Book for a post office, the post office index is used.

The GroupWise client uses the post office database to list users. If you are in the GroupWise client and the indexes for listing system, domain, and post office users are different than the domain database indexes, you should rebuild the post office database indexes. The most common cause of incorrect indexes in a post office is that the post office database was closed when you set up the list information.

To rebuild a database index:

- 1 Make sure you have administrative rights to the database whose indexes you are rebuilding.
- 2 In ConsoleOne, browse to and select the Domain object or Post Office object where you want to rebuild the database index.

3 Click *Tools > GroupWise Utilities > System Maintenance*.



4 Select *Rebuild Indexes for Listing*, then click *Run*.

5 When prompted, make sure the *Path to Database* is correct. If an incorrect path is displayed, browse to and select the path to the database being whose indexes are being rebuilt. Click *OK*.

27 Maintaining User/Resource and Message Databases

It is sometimes necessary to perform maintenance tasks on user and resource databases (`userxxx.db`) and message databases (`msgnnn.db`). The frequency depends on the reliability of your network and your own experience of how often problems are likely to occur. The following tasks help you maintain the integrity of your user and message databases.

- ♦ [Section 27.1, “Analyzing and Fixing User and Message Databases,”](#) on page 409
- ♦ [Section 27.2, “Performing a Structural Rebuild of a User Database,”](#) on page 411
- ♦ [Section 27.3, “Re-creating a User Database,”](#) on page 412

NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

To further protect your GroupWise users against loss of mailbox contents, see [Chapter 31, “Backing Up GroupWise Databases,”](#) on page 431 and [Chapter 32, “Restoring GroupWise Databases from Backup,”](#) on page 433.

To ensure that the same information exists for users and messages throughout your GroupWise system, see [Section 29.1, “Synchronizing Individual Users or Resources,”](#) on page 419.

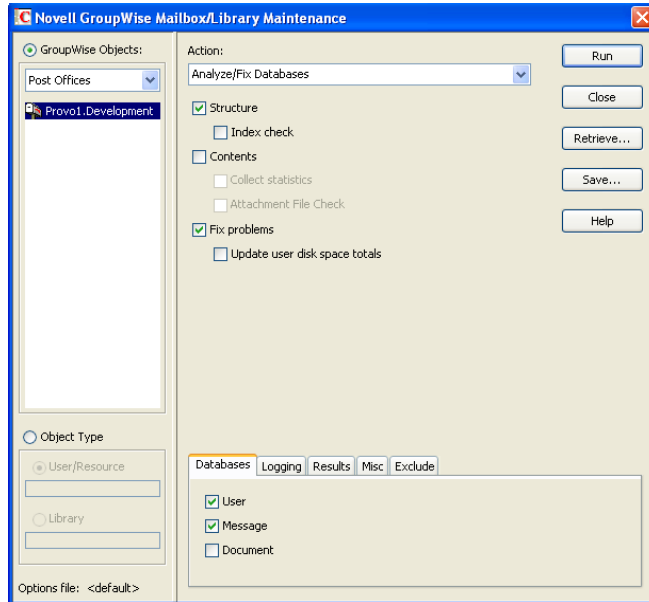
27.1 Analyzing and Fixing User and Message Databases

The Analyze/Fix option of Mailbox/Library Maintenance looks for problems and errors in user and resource databases (`userxxx.db`) and/or message databases (`msgnnn.db`) and then fixes them if you select the *Fix Problems* option. You can analyze databases individually or you can analyze all user, resource, and/or message databases in one or more post offices.

To analyze and repair user, resource, and/or message databases:

- 1 In ConsoleOne, browse to and select one or more User or Resource objects to check individual users or resources.
or
Browse to and select one or more Post Office objects to select all user and/or message databases in the post office.

2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



3 From the *Action* drop-down menu, select *Analyze/Fix Databases*.

4 Select from the following options:

Structure: When a user experiences a problem that is related to the user, message, or library databases, you should perform a structure check. The structure check verifies the integrity of the databases and reports the amount of space that could be recovered. If there is a structural problem, the databases are rebuilt with free space reclaimed.

Index Check: If you select *Structure*, you can also select *Index Check*. You should run an index check if a user tries to open a message and gets a read error, or when sent items that show a delivered status in the Properties window do not appear in the recipient's mailbox. An index check can be time-consuming.

Contents: The user databases (located in the `ofuser` directory) do not contain user messages. Messages are contained in the message databases under the `ofmsg` directory. However, the message databases do not contain the message attachments; these are located in the `offiles` directory. A contents check analyzes references to other items. For example, in the user database, Mailbox/Library Maintenance verifies that any referenced messages actually exist in the message database. In the message database, it verifies that any attachments that are referenced actually exist in the attachment directories. A contents check also restores system folders (Mailbox, Sent Items, Calendar, Cabinet, and Trash to their default locations if any of them have been moved into a subfolder.

Collect Statistics: If you selected *Contents*, the *Collect Statistics* option is available to collect and display statistics about the post office, such as the number of messages and appointments in the post office and the average number per user. In addition, you can display any user mailboxes that have more than a specified number of items. This can help determine if some users are using an excessive amount of disk space. If this is a problem, you might want to encourage users to delete unneeded items or to use the Archive feature in the GroupWise client to store messages on their local drives. You can also limit the amount of disk space each user can have. See [Section 12.3, "Managing Disk Space Usage in the Post Office,"](#) on page 196.

Attachment File Check: Files that are attached to messages are stored under the offiles subdirectory in the post office. When Mailbox/Library Maintenance performs an attachment file check, it reads each attachment file, verifying the file structure. If you skip the attachment file check, Mailbox/Library Maintenance verifies that the attachment file exists but it does not process the file in any way.

Fix Problems: This option tells Mailbox/Library Maintenance to fix any problems it finds. Otherwise, Mailbox/Library Maintenance just reports the problems.

Update User Disk Space Totals: Recalculates the total disk space a GroupWise user is using by reading the selected user mailboxes and updating the poll record used for disk space management. Because disk space is user-specific, the program calculates the amount of disk space in use by the user in the user databases, in any of the message databases, and in the attachment directory. Disk space limitations do not take into account the disk space used in document libraries. This option is usually run if the user totals are not being reflected correctly.

- 5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

[“Databases” on page 452](#)

[“Logging” on page 453](#)

[“Results” on page 453](#)

[“Misc” on page 453](#)

[“Exclude” on page 454](#)

Selected options can be saved for repeated use. See [“Saving Mailbox/Library Maintenance Options” on page 454](#).

- 6 Click Run to perform the Analyze/Fix operation.

Analyze/Fix can also be run using the stand-alone GroupWise Check program. See [Section 34.1, “GroupWise Check,” on page 447](#). It can also be scheduled to run on a regular basis by properly configuring the POA. See [Section 36.4.1, “Scheduling Database Maintenance,” on page 517](#).

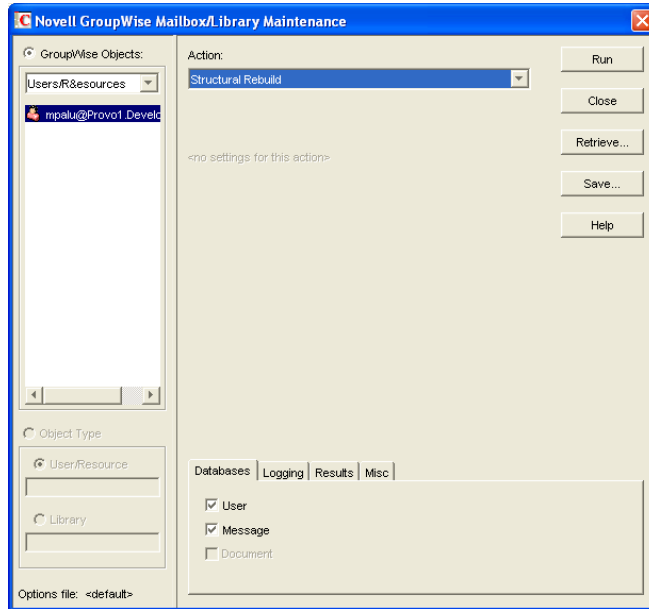
27.2 Performing a Structural Rebuild of a User Database

The Structural Rebuild option of Mailbox/Library Maintenance rebuilds the structure of a user or resource database (`userxxx.db`) and reclaims any free space. It does not re-create the contents of the database. If you need to recover database contents as well as structure, see [Section 27.3, “Re-creating a User Database,” on page 412](#).

To rebuild a user database:

- 1 In ConsoleOne, browse to and select one or more User or Resource objects whose database needs to be rebuilt.

- 2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



- 3 From the *Action* drop-down list, select *Structural Rebuild*.
- 4 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

[“Databases” on page 452](#)

[“Logging” on page 453](#)

[“Results” on page 453](#)

[“Misc” on page 453](#)

Selected options can be saved for repeated use. See [“Saving Mailbox/Library Maintenance Options” on page 454](#).

- 5 Click *Run* to perform a structural rebuild of the user database.

27.3 Re-creating a User Database

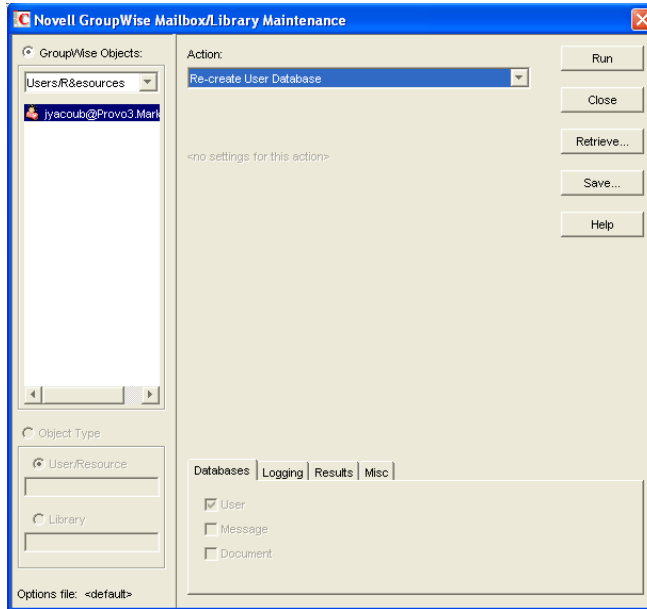
The *Re-create User Database* option of Mailbox/Library Maintenance rebuilds a user or resource database (*userxxx.db*) and recovers any information it can. Some information is lost, such as the folder assignments.

You should never need to select this option for regular database maintenance. It is designed for severe problems, such as replacing a user database that has been accidentally deleted and for which you have no backup copy. A substantial amount of information is lost in the re-creation process, as listed in [“User Databases” on page 473](#). Because folder assignments are lost, all items are placed into the Cabinet folder. The user must then reorganize all the items in his or her mailbox. Using filters and searching can facilitate this process, but it is not a desirable experience. It is, however, preferable to losing everything.

To re-create a user database:

- 1 In ConsoleOne, browse to and select one or more User or Resource objects that need the user database re-created.

2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



3 From the *Action* drop-down list, select *Re-create User Database*.

4 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

[“Databases” on page 452](#)

[“Logging” on page 453](#)

[“Results” on page 453](#)

[“Misc” on page 453](#)

Selected options can be saved for repeated use. See [“Saving Mailbox/Library Maintenance Options” on page 454](#).

5 Click *Run* to re-create the user database.

28 Maintaining Library Databases and Documents

GroupWise Document Management Services (DMS) uses libraries as repositories for documents. For a review of library database structure, see [Section 25.5, “Library Databases,”](#) on page 399.

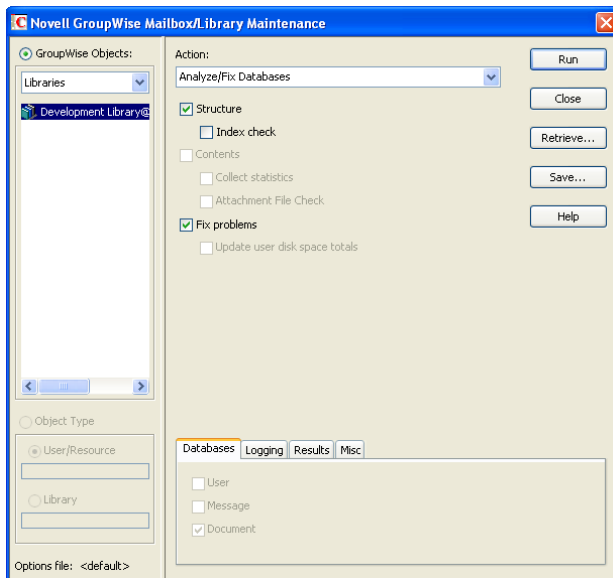
- ♦ [Section 28.1, “Analyzing and Fixing Databases for Libraries and Documents,”](#) on page 415
- ♦ [Section 28.2, “Analyzing and Fixing Library and Document Information,”](#) on page 416

NOTE: Unfortunately, damage to databases cannot be prevented. A power outage can occur in the middle of a write to a database. A hard drive can fail. However, the GroupWise tools for repairing damaged databases are very effective and should be able to resolve most damage to GroupWise databases.

28.1 Analyzing and Fixing Databases for Libraries and Documents

For libraries, the *Analyze/Fix Databases* option of Mailbox/Library Maintenance looks for problems and errors in library and document databases and then fixes them if you select the *Fix Problems* option.

- 1 In ConsoleOne, browse to and select one or more Library objects.
- 2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



3 From the *Action* drop-down menu, select *Analyze/Fix Databases*.

4 Select from the following options:

Structure: When a user experiences a problem that is related to the library databases, you should perform a structure check. The structure check verifies the integrity of the databases and reports the amount of space that could be recovered. If there is a structural problem, the databases are rebuilt with free space reclaimed.

Index Check: If you select *Structure*, you can also select *Index Check*. An index check can be time-consuming.

Contents: The library database (located in the `gwdms` directory of the post office) does not contain documents. Documents are stored in the `lib0000-FF` directories. A contents check analyzes references from libraries to documents.

Collect Statistics: If you selected *Contents*, the *Collect Statistics* option is available to collect and display statistics about the library, such as the number and size of documents.

Attachment File Check: Files that are attached to messages are stored under the `offiles` subdirectory in the post office. When Mailbox/Library Maintenance performs an attachment file check, it reads each attachment file, verifying the file structure. If you skip the attachment file check, Mailbox/Library Maintenance verifies that the attachment file exists but it does not process the file in any way.

Fix Problems: This option tells Mailbox/Library Maintenance to fix any problems it finds. Otherwise, Mailbox/Library Maintenance just reports the problems.

5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

[“Databases” on page 452](#)

[“Logging” on page 453](#)

[“Results” on page 453](#)

[“Misc” on page 453](#)

Selected options can be saved for repeated use. See [“Saving Mailbox/Library Maintenance Options” on page 454](#).

6 Click *Run* to perform the *Analyze/Fix Databases* operation on the library.

Analyze/Fix Databases can also be run using the stand-alone GroupWise Check program. See [Section 34.1, “GroupWise Check,” on page 447](#). It can also be scheduled to run on a regular basis by properly configuring the POA. See [Section 36.4.1, “Scheduling Database Maintenance,” on page 517](#).

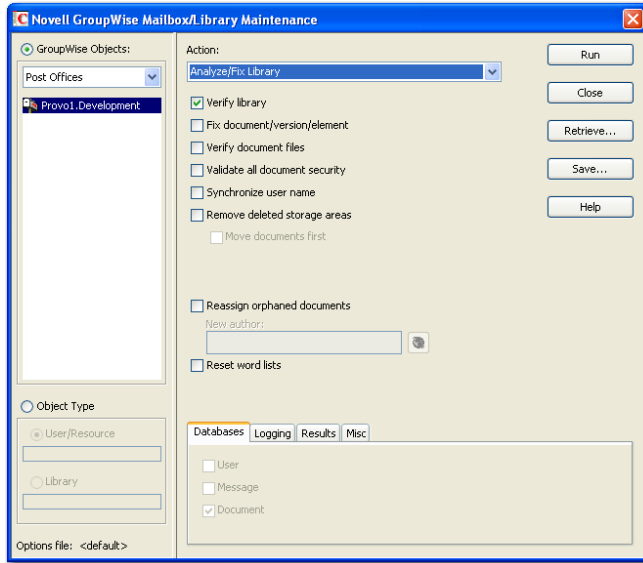
28.2 Analyzing and Fixing Library and Document Information

The *Analyze/Fix Library* option of Mailbox/Library Maintenance performs more library-specific functions than *Analyze/Fix Databases*. For all options except *Verify Library*, all documents in each of the selected library databases are checked. This can be a time-consuming process. Therefore, if you intend to select more than one of the *Analyze/Fix Library* options, you can save time by selecting each of them before clicking *Run*. This causes all selected options to be run against each document, which is faster than running each option individually against all documents.

To validate library databases:

1 In ConsoleOne, browse to and select one or more Post Office objects where you want to validate libraries.

2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



3 From the *Action* drop-down menu, select *Analyze/Fix Library*.

4 Select from the following options:

Verify Library: This is a post office-level check. It verifies that all libraries are on the libraries list. It also checks the schema and guarantees its integrity. If there is a problem with the schema, it resets to a default schema to reclaim any missing items. For example, if you deleted the Document Type property, you could recover it using this option.

Fix Document/Version/Element: This performs an integrity check to verify the following:

- ◆ Each document has one or more versions linked to it.
- ◆ Each version has one or more elements linked to it.
- ◆ All versions are linked to a document.
- ◆ All elements are linked to a version.

If there are any missing links, the missing documents or versions are created from the information contained in the existing version or element for which the link is missing. For example, if a version is found that shows no link to a document, a document is created from the information contained in the version and the link is reestablished. Of course, any information in the lost document that might have been newer than the information contained in the old version is lost.

Verify Document Files: This determines if the BLOB exists for a document and the document is accessible. If not, an error is logged for that document. The log message does not indicate why a file is missing or inaccessible. You can recover a file by restoring it from backup.

Possible errors that would be logged include:

- ◆ If the file system on the network becomes corrupted, this tells you which documents cannot be opened or which BLOB files are missing.
- ◆ If a file was marked by someone as Read Only or Hidden, this option logs an error indicating that the file is inaccessible.

Validate All Document Security: This option validates document security for the Author, Creator and Security (document sharing) fields. The validation replaces the results of selecting the *Validate Author/Creator Security* option, and is more thorough. Therefore, you only need to select one option or the other.

Synchronize User Name: The *Author* and *Creator* fields display users' full names, not unique IDs. If a user's name is changed, such as for marriage, this option verifies that the user's name on document and version records is the same as the user's current display name. In other words, the *Author* and *Creator* fields in documents and versions are updated to the user's newer name.

Remove Deleted Storage Areas: When you delete a document storage area in the Storage Areas page of a library's details dialog box, the document storage area and the documents stored there remain on the system. Deleting the storage area from the library only means that new documents are not stored there. The documents there continue to be available to users.

If you want to also remove the document storage area from the system, you have two options: delete the storage area and its documents, or first move the documents and then delete the storage area. The first option is not advisable, but exists so that if you have moved all of the documents that can be moved, but some corrupted documents are left behind, you can force the document storage area to be deleted.

You should normally select *Move Documents First* so that users continue to have access to those documents from a different document storage area. With this option, all BLOBs in the library are checked to see which documents are in the area being deleted.

Reassign Orphaned Documents: Documents can occasionally become orphaned (unattached to a user). For example, this can happen when a user leaves your organization and the user object is removed. All documents belonging to that user are no longer available in GroupWise searches and cannot be accessed by anyone (document security is controlled by the user listed in the *Author* and *Creator* fields). This option lets you reassign these documents to another user. You must select a new author from the browser menu after checking this option. The new author you designate has access to all orphaned documents in this library.

Reset Word Lists: Documents stored in a library are indexed and inserted into a generated word list. This allows users to search for a document by keywords as well as any word contained within a document. The document library word list might become outdated and if this occurs, the word list must be regenerated. This option allows the program to regenerate the document library word list the next time an index operation is performed.

- 5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

["Databases" on page 452](#)

["Logging" on page 453](#)

["Results" on page 453](#)

["Misc" on page 453](#)

Selected options can be saved for repeated use. See ["Saving Mailbox/Library Maintenance Options" on page 454](#).

- 6 Click *Run* to perform the Analyze/Fix Library operation.

Analyze/Fix Library can also be run using the stand-alone GroupWise Check program. See [Section 34.1, "GroupWise Check," on page 447](#). It can also be scheduled to run on a regular basis by properly configuring the POA. See [Section 36.4.1, "Scheduling Database Maintenance," on page 517](#).

29 Synchronizing Database Information

In general, synchronization of object information throughout your GroupWise system occurs automatically. Whenever you add, delete, or modify a GroupWise object, the information is automatically replicated to all appropriate databases. Ideally, each domain database (`wpdomain.db`) in your system contains original records for all objects it owns and accurately replicated records for all objects owned by other domains. However, because unavoidable events such as power outages and hardware problems can disrupt network connectivity, information in various databases might get out of sync.

If you think you have a synchronization problem, especially soon after adding, deleting, or modifying objects, it is wise to check Pending Operations to make sure your changes have been processed. See [Section 4.5, “Pending Operations,” on page 80](#). When waiting for replication to take place, patience is a virtue.

When information differs between the original record and a replicated record, the original record is considered correct. If you perform synchronization from the owning domain, the owning domain notifies the primary domain of the correct information, then the primary domain broadcasts the correct information to all secondary domains. Therefore, the best place to perform synchronization is from the domain that owns the object that is out of sync. The next best place to perform synchronization is from the primary domain, because the primary domain sends a request to the owning domain for the correct information, then broadcasts the correct information to all secondary domains.

Any GroupWise object can be synchronized:

- ♦ [Section 29.1, “Synchronizing Individual Users or Resources,” on page 419](#)
- ♦ [Section 29.2, “Synchronizing a Post Office,” on page 420](#)
- ♦ [Section 29.3, “Synchronizing a Library,” on page 421](#)
- ♦ [Section 29.4, “Synchronizing a Secondary Domain,” on page 421](#)
- ♦ [Section 29.5, “Synchronizing the Primary Domain from a Secondary Domain,” on page 422](#)

29.1 Synchronizing Individual Users or Resources

Most often, you will notice a synchronization problem when a user has trouble sending a message. Symptoms include:

- ♦ The sender receives a “user is undeliverable” message.
- ♦ A new user or resource created in ConsoleOne does not appear in the Address Book in some or all post offices.
- ♦ User or resource information is incorrect in the Address Book but correct in ConsoleOne.
- ♦ A user or resource is listed in the Address Book as belonging to one post office but actually belongs to another.

To synchronize individual User and/or Resource objects:

- 1 In ConsoleOne, connect to the domain that owns the users and/or resources.
or
Connect to the primary domain.
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,” on page 69](#).
- 2 Browse to and right-click one or more User or Resource objects to synchronize, then click *Properties*.
- 3 Make sure the correct information appears on the object’s Identification page, then click *Cancel*.
- 4 Repeat [Step 2](#) and [Step 3](#) for each user or resource you need to synchronize.
- 5 Select each User or Resource object, then click *Tools > GroupWise Utilities > Synchronize*.
- 6 When you are asked whether to proceed, click *Yes*.

Current, correct information is then replicated throughout your GroupWise system.

If many User or Resource objects are being synchronized, you can check progress by viewing pending operations. See [Section 4.5, “Pending Operations,” on page 80](#).

After synchronization is complete, you can verify that it was successful by checking the synchronized objects in Address Books and several post offices in your GroupWise system.

If there are indications that a large number of User or Resource objects need to be synchronized, rebuilding the post office database (`wphost.db`) can be preferable to synchronizing individual objects. However, this process requires exclusive access to the post office database. See [Section 26.3, “Rebuilding Domain or Post Office Databases,” on page 405](#).

Occasionally, GroupWise user information can get out of sync with Novell eDirectory user information. This requires a different type of synchronization process. See [Section 42.4.1, “Using eDirectory User Synchronization,” on page 652](#).

29.2 Synchronizing a Post Office

If information for a particular post office does not display the same throughout your GroupWise system, you can synchronize the post office.

- 1 In ConsoleOne, connect to the domain that owns the post office, as described in [Section 9.1, “Connecting to a Domain,” on page 145](#).
or
Connect to the primary domain.
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,” on page 69](#).
- 2 Browse to and right-click the Post Office object to synchronize, then click *Properties*.
- 3 Make sure the correct information appears on the post office Identification page, then click *Cancel*.
- 4 Select the Post Office object, then click *Tools > GroupWise Utilities > Synchronize*.
- 5 When you are asked whether to proceed, click *Yes*.

Current, correct post office information is then replicated throughout your GroupWise system.

After synchronization is complete, you can verify that it was successful by checking the post office information when connected to different domains in your GroupWise system.

See also [Section 26.3, “Rebuilding Domain or Post Office Databases,”](#) on page 405.

29.3 Synchronizing a Library

If information for a library does not display the same throughout your GroupWise system, you can synchronize the library.

- 1 In ConsoleOne, connect to the domain that owns the library.

or

Connect to the primary domain.

If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,”](#) on page 69.

- 2 Browse to and right-click the Library object to synchronize, then click *Properties*.
- 3 Make sure the correct information appears on the library Identification page, then click *Cancel*.
- 4 Select the Library object, then click *Tools > GroupWise Utilities > Synchronize*.
- 5 When you are asked whether to proceed, click *Yes*.

Current, correct library information is then replicated throughout your GroupWise system.

After synchronization is complete, you can verify that it was successful by checking the library information when connected to different domains in your GroupWise system.

See also [Section 28.2, “Analyzing and Fixing Library and Document Information,”](#) on page 416.

29.4 Synchronizing a Secondary Domain

If information for a particular secondary domain does not display the same throughout your GroupWise system, you can synchronize the secondary domain.

- 1 In ConsoleOne, connect to the primary domain.

If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,”](#) on page 69.

- 2 If there is any doubt about the correctness of that secondary domain’s information as stored in the primary domain database, synchronize the primary domain with the secondary domain before proceeding, as described in [Section 29.5, “Synchronizing the Primary Domain from a Secondary Domain,”](#) on page 422.
- 3 Browse to and right-click the Domain object to synchronize, then click *Properties*.
- 4 Make sure the correct information appears on the domain Identification page, then click *Cancel*.
- 5 Select the Domain object, then click *Tools > GroupWise Utilities > Synchronize*.
- 6 When you are asked whether to proceed, click *Yes*.

Current, correct domain information for the secondary domain is then replicated throughout your GroupWise system.

After synchronization is complete, you can verify that it was successful by checking the domain information when connected to different domains in your GroupWise system.

See also [Section 26.3, “Rebuilding Domain or Post Office Databases,”](#) on page 405.

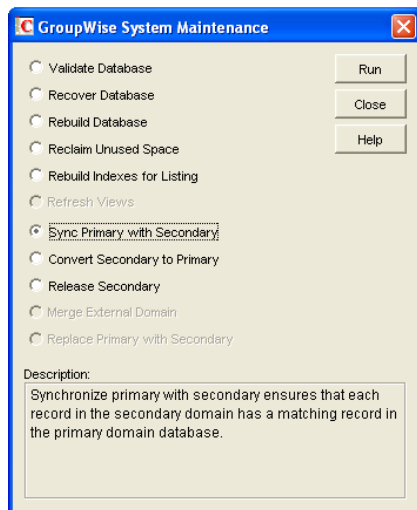
29.5 Synchronizing the Primary Domain from a Secondary Domain

Information about a secondary domain stored in the secondary domain database is considered more current and correct than information about that secondary domain stored in the primary domain database. If the primary domain database contains out-of-date information, you can synchronize the primary domain from the secondary domain.

When you synchronize the primary domain database from a secondary domain database, any records the secondary domain owns, such as post offices or users added to the secondary domain, are replicated from the secondary domain database to the primary domain database.

To synchronize the primary domain from a secondary domain:

- 1 You must have administrative rights to the primary domain directory and the secondary domain directory from which the primary domain is being synchronized.
- 2 In ConsoleOne, connect to the primary domain.
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,”](#) on page 69.
- 3 Browse to and select the Domain object of the secondary domain whose database you want to use to synchronize the primary domain database.
- 4 Click *Tools > GroupWise Utilities > System Maintenance*.



- 5 Select *Sync Primary with Secondary*, then click *Run*.
- 6 When prompted, make sure the *Path to Database* is correct. If an incorrect path is displayed, browse to and select the path to the database being validated. Click *OK*.

To make sure the primary domain database is totally up-to-date, repeat the procedure for each secondary domain in your system.

30 Managing Database Disk Space

One of the most common maintenance issues in a growing system is running out of disk space. In addition to sending messages, users tend to use GroupWise for all sorts of communication, such as transferring large files. Library documents created with Document Management Services (DMS) can use huge amounts of disk space. Archived library documents can also quickly use up disk space assigned to the post office, where space is usually limited.

You should let your users know about the archive and auto-delete features of GroupWise mail, or set client options in ConsoleOne to automatically archive or delete. See [Chapter 76, “Setting Defaults for the GroupWise Client Options,”](#) on page 1025.

- ♦ [Section 30.1, “Gathering Mailbox Statistics,”](#) on page 423
- ♦ [Section 30.2, “Reducing the Size of User and Message Databases,”](#) on page 425
- ♦ [Section 30.3, “Reclaiming Disk Space in Domain and Post Office Databases,”](#) on page 427
- ♦ [Section 30.4, “Reducing the Size of Libraries and Document Storage Areas,”](#) on page 428

See also [Section 12.3, “Managing Disk Space Usage in the Post Office,”](#) on page 196.

30.1 Gathering Mailbox Statistics

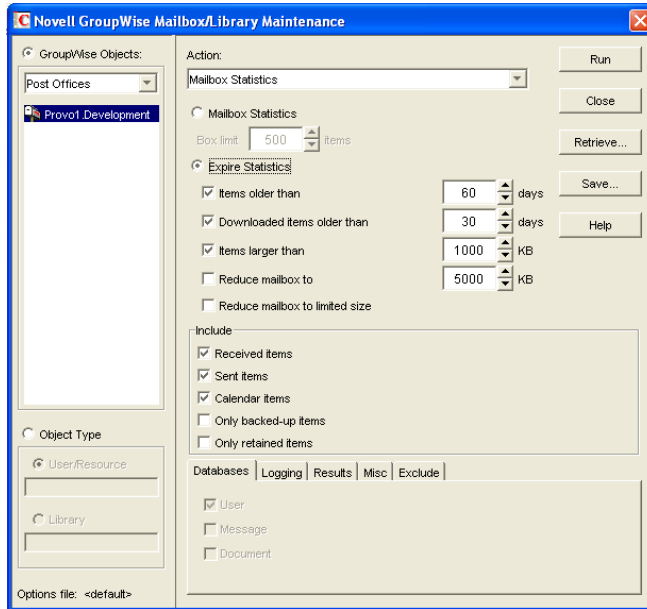
If you have some users who don't like to throw anything away, you might want to monitor the size of their mailboxes and, where appropriate, suggest voluntary cleanup. You can assess email retention by the number of messages, age of messages, or size of user databases.

The Mailbox Statistics option in Mailbox/Library Maintenance collects and displays statistics about the post office, such as the number of messages and appointments in the post office and the average number per user. It is valid only for user databases. In addition, you can display any user mailboxes that have more than a specified number of items. This can help determine which users might be using an excessive amount of file server disk space.

To gather mailbox statistics:

- 1 In ConsoleOne, browse to and select one or more User or Resource objects or one or more Post Office objects.

2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



3 From the *Action* drop-down menu, select *Mailbox Statistics*.

4 Select *Mailbox Statistics*.

Mailbox Statistics: Specify a maximum number of items to see a report showing each user whose mailbox has more items in it than the number you specify.

or

Select *Expire Statistics*.

Expire Statistics: Select one of the following:

- ◆ **Items Older Than:** Shows how many items are older than the number of days you specify.
- ◆ **Downloaded Items Older Than:** Shows how many items have been downloaded to users' GroupWise Caching or Remote mailboxes that are older than the number of days you specify. This does not include items that have been downloaded to non-GroupWise mailboxes (for example, POP and IMAP accounts).
- ◆ **Items Larger Than:** Shows how many items are larger than the size you specify.
- ◆ **Reduce Mailbox To:** Shows how many items need to be expired before the mailbox would be reduced to the size you specify. Older, larger items are expired before newer, smaller items.
- ◆ **Reduce Mailbox to Limited Size:** Shows how many items need to be expired before the mailbox is the size specified using the Disk Space Management feature under Client Options, as described in [Section 12.3.3, "Setting Mailbox Size Limits,"](#) on page 198.

When items meet your selected expire criteria, they are subject to being removed from the mailbox when you the *Expire/Reduce Messages* action as described in [Section 30.2, "Reducing the Size of User and Message Databases,"](#) on page 425.

5 In the *Include* box, select *Received Items*, *Sent Items*, *Calendar Items*, *Only Backed-Up Items*, and/or *Only Retained Items* to specify the types of items to gather statistics for.

The *Only Backed-Up Items* option interacts with the *Do Not Purge Items Until They Are Backed Up* setting under *Tools > GroupWise Utilities > Client Options > Environment Options > Cleanup*. If items are not allowed to be deleted before they are backed up, then they cannot be deleted during an Expire/Reduce operation. For more information, see [“Environment Options: Cleanup” on page 1039](#).

The *Only Retained Items* option interacts with third-party messages retention application, as described in [Chapter 33, “Retaining User Messages,” on page 441](#).

- 6 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

[“Databases” on page 452](#)

[“Logging” on page 453](#)

[“Results” on page 453](#)

[“Misc” on page 453](#)

[“Exclude” on page 454](#)

Selected options can be saved for repeated use. See [“Saving Mailbox/Library Maintenance Options” on page 454](#).

By default, the mailbox statistics are sent to the domain administrator, as designated in [Section 43.7, “Notifying the Domain Administrator,” on page 682](#).

- 7 If you want to send the statistics to one or more other users, click *Results*, select *Individual Users*, specify the email addresses of the users in the *CC* field, then click *Message* if you want to include explanatory text.
- 8 Click *Run* to gather the mailbox statistics and email the results to the specified users.

30.2 Reducing the Size of User and Message Databases

When users archive and empty messages in their mailboxes, the messages are marked for removal from the database (“expired”), but the disk space that the expired messages occupied in the databases is retained and used again for new messages. As a result, archiving and deleting messages does not affect the overall size of the databases.

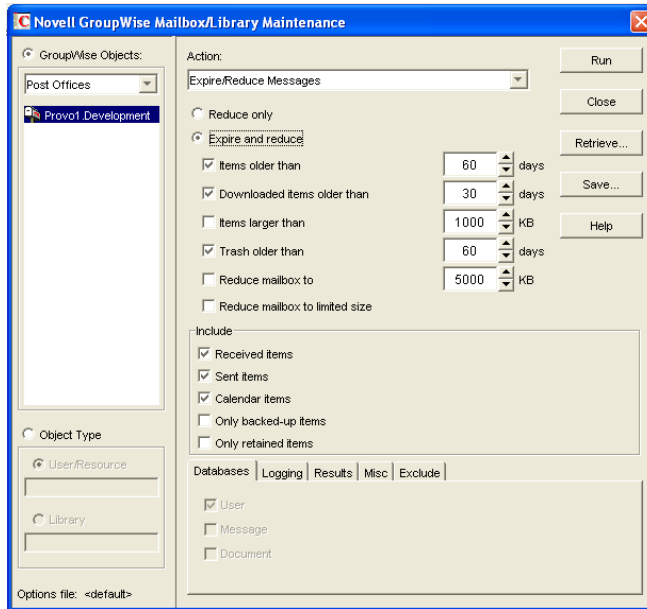
The Expire/Reduce Messages option of Mailbox/Library Maintenance enables you to expire additional messages and reduce the size of the databases by reclaiming the free space in the databases that is created when messages are expired. You can expire/reduce messages for one or more users or resources, or for all users and resources in one or more post offices. You should inform users before you run this process so they have a chance to archive or delete messages. Unread messages are not expired.

- 1 In ConsoleOne, browse to and select one or more User or Resource objects to expire/reduce messages for the selected users and resources.

or

Browse to and select one or more Post Office objects to expire/reduce messages for all users and resources in each selected post office.

2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



3 From the *Action* drop-down menu, select *Expire/Reduce Messages*.

4 Click *Reduce Only* to delete items that have already expired (that is, items that have been archived or deleted by users).

or

Click *Expire and Reduce* to expire items in addition those that users have already archived or deleted, based on the criteria you select.

Expire and Reduce: Select one or more of the following:

- ◆ **Items Older Than:** Expires items that are older than the number of days you specify.
 - ◆ **Downloaded Items Older Than:** Expires items that have been downloaded to users' GroupWise Caching or Remote mailboxes that are older than the number of days you specify. It does not expire items that have been downloaded to non-GroupWise mailboxes (for example, POP and IMAP accounts).
 - ◆ **Items Larger Than:** Expires items that are larger than the size you specify.
 - ◆ **Trash Older Than:** Expires items in the Trash that are older than the number of days you specify.
 - ◆ **Reduce Mailbox To:** Expires items until the mailbox is reduced to the size you specify. Older, larger items are expired before newer, smaller items.
 - ◆ **Reduce Mailbox to Limited Size:** Expires items until the mailbox is the size specified using the Disk Space Management feature under Client Options, as described in [Section 12.3.3, "Setting Mailbox Size Limits,"](#) on page 198.
- 5 In the *Include* box, select *Received Items*, *Sent Items*, *Calendar Items*, *Only Backed-Up Items*, and/or *Only Retained Items*. You might want to notify users of the types of items that will be deleted.

The *Only Backed-Up Items* option interacts with the *Do Not Purge Items Until They Are Backed Up* setting under *Tools > GroupWise Utilities > Client Options > Environment Options > Cleanup*. If items are not allowed to be deleted before they are backed up, then they cannot be deleted during an *Expire/Reduce* operation. For more information, see ["Environment Options: Cleanup"](#) on page 1039.

The *Only Retained Items* option interacts with third-party messages retention application, as described in [Chapter 33, “Retaining User Messages,”](#) on page 441.

- 6 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

“Databases” on page 452

“Logging” on page 453

“Results” on page 453

“Misc” on page 453

“Exclude” on page 454

Selected options can be saved for repeated use. See “[Saving Mailbox/Library Maintenance Options](#)” on page 454.

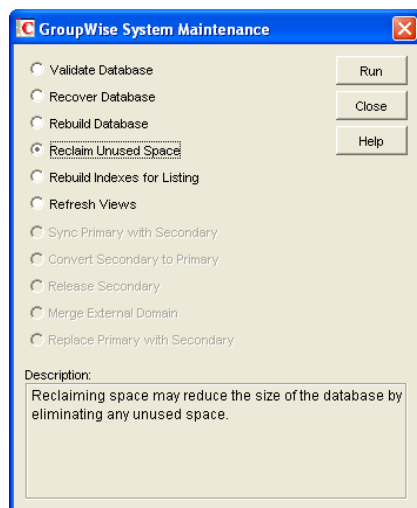
- 7 Click *Run* to perform the Expire/Reduce Messages operation.

For additional disk space management assistance, see [Section 12.3, “Managing Disk Space Usage in the Post Office,”](#) on page 196.

30.3 Reclaiming Disk Space in Domain and Post Office Databases

As you add information to your system, the domain databases (`wppdomain.db`) and post office databases (`wppost.db`) increase in size. If you delete information, the space created in the databases for the information is not immediately recovered. GroupWise uses the free space before requiring more disk space; however, if you have deleted a large amount of information, you might want to reclaim unused database space. If you have frequent changes to your users, especially deletions, you should occasionally reclaim disk space.

- 1 In ConsoleOne, browse to and select the Domain object or Post Office object where you want to reclaim disk space.
- 2 Click *Tools > GroupWise Utilities > System Maintenance*.



- 3 Select *Reclaim Unused Space*, then click *Run*.
- 4 When prompted, make sure the *Path to Database* is correct. If an incorrect path is displayed, browse to and select the path to the database where you want to reclaim disk space. Click *OK*.

30.4 Reducing the Size of Libraries and Document Storage Areas

The amount of disk space you allow at each post office for your library databases varies according to the GroupWise features they use.

If you are using GroupWise Document Management Services, you must determine storage requirements for your documents. If you feel your current disk space usage by documents is not representative of your long-term requirements, you can estimate the disk space users need for documents by multiplying an average document size by the average number of documents per user by the total number of users in the post office.

For example, the typical document size is 50 KB. Each user owns about 50 documents and there are 100 users on your post office.

Sample Calculation:

```
    50 KB (document size)
x   50 documents (per user)
x  100 users
-----
    2.5 GB of disk space
```

Be sure to allow your libraries room to grow.

When room to grow is no longer available, the following tasks help you make the best use of available disk space:

- ♦ [Section 30.4.1, “Archiving and Deleting Documents,” on page 428](#)
- ♦ [Section 30.4.2, “Deleting Activity Logs,” on page 429](#)

See also [Section 23.4.2, “Backing Up and Restoring Archived Documents,” on page 383](#).

30.4.1 Archiving and Deleting Documents

Documents can be archived, retained indefinitely, or simply deleted. The document type property determines a document’s disposition (archive, delete, or retain). The document life property determines when it can be archived or deleted. When you run the *Archive/Delete Documents* option of Mailbox/Library Maintenance, documents in the selected libraries that have reached their document life dates are either deleted or archived.

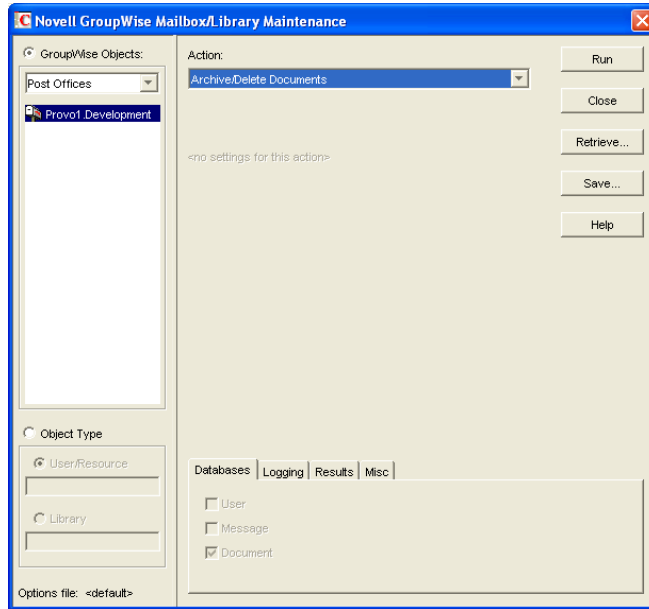
Documents that have reached their document life and been marked for deletion in the document type are simply deleted from the library, after which the document and its property information can no longer be found by any search. You can recover deleted documents from database backups.

When documents are archived, their BLOBs are moved to archive directories. These directories are named *arnnnnnn* (where *nnnnnn* is an incremented integer with leading zeros), and are automatically created as needed. They are sometimes referred to as archive sets. The archive directories are located at `post_office_directory\gwdms\lib01-FF\archive`. When a document is archived, GroupWise determines if the document BLOB fits in the current archive directory. If the BLOB does not fit, another archive directory is created and the BLOB is archived there.

To archive/delete documents from one library or all libraries in the selected post offices:

- 1 In ConsoleOne, select one or more Library objects or Post Office objects for the documents you want to archive/delete.

- 2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



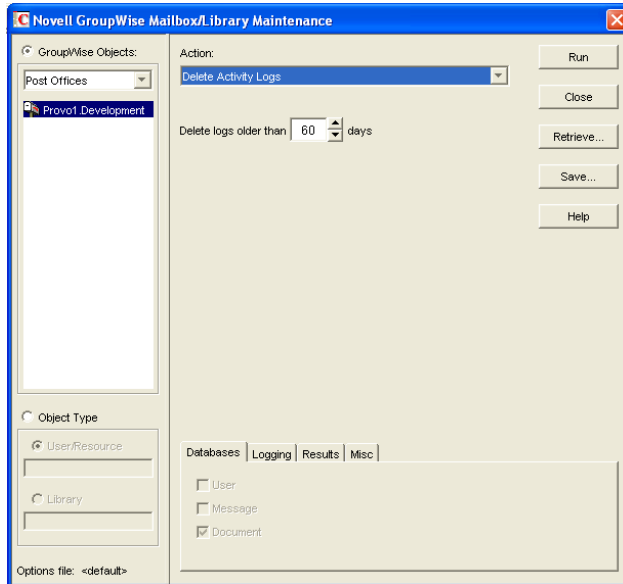
- 3 From the *Action* drop-down menu, select *Archive/Delete Documents*.
- 4 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:
 - [“Databases” on page 452](#)
 - [“Logging” on page 453](#)
 - [“Results” on page 453](#)
 - [“Misc” on page 453](#)Selected options can be saved for repeated use. See [“Saving Mailbox/Library Maintenance Options” on page 454](#).
- 5 Click *Run* to perform the Archive/Delete Documents operation.

30.4.2 Deleting Activity Logs

To free up disk space by deleting the activity logs for one or more libraries:

- 1 In ConsoleOne, select one or more Library objects or Post Office object where you want to delete activity logs.

2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.



- 3 From the *Action* drop-down menu, select *Delete Activity Logs*.
- 4 Specify the number of days in the *Delete Activity Logs Older Than* field. The default is 60 days.
- 5 Using the tabs at the bottom of the Mailbox/Library Maintenance dialog box, set the following options:

“Databases” on page 452

“Logging” on page 453

“Results” on page 453

“Misc” on page 453

Selected options can be saved for repeated use. See “Saving Mailbox/Library Maintenance Options” on page 454.

- 6 Click *Run* to delete unneeded activity logs.

31 Backing Up GroupWise Databases

You should back up GroupWise databases regularly so that if a database sustains damage that cannot be repaired using the GroupWise database maintenance tools, you can still recover with minimum data loss.

Use your backup software of choice to back up GroupWise databases to a secure location. For a list of compatible products, see the [Partner Product Guide \(http://www.novell.com/partnerguid\)](http://www.novell.com/partnerguid). You can also use the GroupWise Database Copy utility (DBCOPY) and the GroupWise Time Stamp utility (GWTMSTMP) to assist with backups. For details about how to use these utilities, see [Section 34, "Stand-Alone Database Maintenance Programs,"](#) on page 447.

- [Section 31.1, "Backing Up a Domain,"](#) on page 431
- [Section 31.2, "Backing Up a Post Office,"](#) on page 431
- [Section 31.3, "Backing Up a Library and Its Documents,"](#) on page 432
- [Section 31.4, "Backing Up Individual Databases,"](#) on page 432

31.1 Backing Up a Domain

All critical domain-level information is stored in the domain database (`wppdomain.db`). Use your backup software of choice to back up each domain database to a secure location. If your backup software cannot handle open files, stop the MTA for the domain while the backup of the domain database takes place or copy the domain directory to a temporary location and back up the static copy.

See also [Section 32.1, "Restoring a Domain,"](#) on page 433.

31.2 Backing Up a Post Office

Critical post office-level information is stored in many different databases. The table below summarizes the databases and their locations:

Database	Location
<code>wpphost.db</code>	<code>\post_office_directory</code>
<code>ngwguard.db</code>	<code>\post_office_directory</code>
<code>msgnnn.db</code>	<code>\post_office_directory\ofmsg</code>
<code>userxxx.db</code>	<code>\post_office_directory\ofuser</code>
<code>puxxxxx.db</code>	<code>\post_office_directory\ofuser</code>
<code>*.idx</code> and <code>*.inc</code>	<code>\post_office_directory\ofuser\index</code>

Database	Location
fd0-F6	\post_office_directory\offiles
dmsb.db	\post_office_directory\gwdms
dmsxxxn01-FF.db	\post_office_directory\gwdms\lib0000-FF
fd0-FF	\post_office_directory\gwdms\lib0000-FF\docs
*.idx and *.inc	\post_office_directory\gwdms\lib0000-FF\index

To view a post office directory structure diagram, see “Post Office Directory” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

Use your backup software of choice to back up all databases in each post office to a secure location. If your backup software cannot handle open files, stop the POA for the post office while the backup of the domain database takes place or copy the post office directory to a temporary location and back up the static copy.

See also [Section 32.2, “Restoring a Post Office,”](#) on page 433.

31.3 Backing Up a Library and Its Documents

If the document storage area for a library is physically located in a post office, the library and documents are backed up along with the rest of the data in the post office. However, document storage areas are frequently located outside of the post office directory structure because of disk space considerations. Therefore, remote document storage areas must be backed up separately. A post office can have multiple libraries and each library can have multiple document storage areas, so make sure you have identified all document storage areas in your library/document backup procedure.

After you have initially performed a full backup of your document storage areas, you can perform incremental backups by backing up to the same location to shorten the backup process.

To ensure consistency between the backups of post office databases and document storage areas:

- 1 Use your backup software of choice to back up your document storage areas.
- 2 Back up the post office, as described in [Section 31.2, “Backing Up a Post Office,”](#) on page 431.
- 3 Perform an incremental backup of your document storage areas to pick up all new documents and document modifications that occurred while backing up the post office.

You should need to restore data in a document storage area only if files have been damaged or become inaccessible due to a hard disk failure.

See also [Section 32.3, “Restoring a Library,”](#) on page 434.

31.4 Backing Up Individual Databases

If you need to back up individual databases separately from backing up a post office, you can use your backup software of choice.

See also [Section 32.4, “Restoring an Individual Database,”](#) on page 434.

32 Restoring GroupWise Databases from Backup

Database damage can usually be repaired using the database maintenance tools provided with GroupWise. Only very occasionally should you need to restore databases from backup.

- ♦ [Section 32.1, “Restoring a Domain,” on page 433](#)
- ♦ [Section 32.2, “Restoring a Post Office,” on page 433](#)
- ♦ [Section 32.3, “Restoring a Library,” on page 434](#)
- ♦ [Section 32.4, “Restoring an Individual Database,” on page 434](#)
- ♦ [Section 32.5, “Restoring Deleted Mailbox Items,” on page 435](#)
- ♦ [Section 32.6, “Recovering Deleted GroupWise Accounts,” on page 438](#)

32.1 Restoring a Domain

Typically, damage to the domain database (`wpdomain.db`) can be repaired using the database maintenance tools provided in ConsoleOne, as described in [Chapter 26, “Maintaining Domain and Post Office Databases,” on page 401](#).

If damage to the domain database is so severe that rebuilding the database is not possible:

- 1 Stop the MTA for the domain.
- 2 Use the backup software for your platform, as listed in [Section 31.1, “Backing Up a Domain,” on page 431](#), to restore the domain database into the domain directory.
- 3 Restart the MTA for the domain.
- 4 To update the restored domain database with administrative changes made since it was backed up, synchronize the restored domain database with the primary domain database, as described in [Section 29.4, “Synchronizing a Secondary Domain,” on page 421](#).

If the restored domain database is for the primary domain, see [Section 29.5, “Synchronizing the Primary Domain from a Secondary Domain,” on page 422](#).

32.2 Restoring a Post Office

Typically, damage to databases in a post office can be repaired using the database maintenance tools provided in ConsoleOne or using GroupWise Check (GWCheck). See [Chapter 26, “Maintaining Domain and Post Office Databases,” on page 401](#), [Chapter 27, “Maintaining User/Resource and Message Databases,” on page 409](#), and [Section 34.1, “GroupWise Check,” on page 447](#).

If damage to the post office was so severe that rebuilding databases is not possible:

- 1 Stop the POA for the post office.

- 2 Use the backup software for your platform, as listed in [Section 31.2, “Backing Up a Post Office,” on page 431](#), to restore the various databases into their proper locations in the post office directory.
- 3 Time-stamp the restored user databases so that old items are not automatically purged during nightly maintenance:
 - 3a In ConsoleOne, browse to and select the Post Office object, then click *Tools > GroupWise Utilities > Backup/Restore Mailbox*.
 - 3b On the *Backup* tab, select *Restore*, then click *Yes*.
- 4 To update the restored post office database (*wphost.db*) with the most current information stored in the domain database, rebuild the post office database, as described in [Section 26.3, “Rebuilding Domain or Post Office Databases,” on page 405](#).
- 5 To update other restored databases such as user databases (*userxxx.db*) and message databases (*msgnnn.db*) with the most current information stored in other post offices, run Analyze/Fix Databases with *Contents* selected, as described in [Section 27.1, “Analyzing and Fixing User and Message Databases,” on page 409](#).
- 6 Restart the POA for the post office.

32.3 Restoring a Library

Typically, damage to library databases (*dmsb.db* and others) can be repaired using the database maintenance tools provided in ConsoleOne or using GroupWise Check (GWCheck). See [Chapter 28, “Maintaining Library Databases and Documents,” on page 415](#) and [Section 34.1, “GroupWise Check,” on page 447](#).

If damage to the library is so severe that rebuilding databases is not possible:

- 1 Stop the POA that services the library.
- 2 Use the backup software for your platform, as listed in [Section 31.3, “Backing Up a Library and Its Documents,” on page 432](#), to restore the library.
- 3 Restart the POA.
- 4 To update the restored library databases with the most current information stored in other post offices:
 - 4a In ConsoleOne, run Analyze/Fix Databases with *Contents* selected.
 - 4b Run Analyze/Fix Library.
For more information, see [Section 28.2, “Analyzing and Fixing Library and Document Information,” on page 416](#).

32.4 Restoring an Individual Database

Typically, damage to user and resource databases (*userxxx.db*) and message databases (*msgnnn.db*) can be repaired using the database maintenance tools provided in ConsoleOne or using GroupWise Check (GWCheck). See [Chapter 27, “Maintaining User/Resource and Message Databases,” on page 409](#) and [Section 34.1, “GroupWise Check,” on page 447](#).

If damage to an individual database is so severe that repair is not possible:

- 1 Make sure the user to whom the affected database belongs is not running the GroupWise client.
- 2 Use your backup software of choice to restore the database into the proper location in the post office directory.

User databases are stored in the `ofuser` subdirectory in the post office. Message databases are stored in the `ofmsg` subdirectory.

- 3 To update the restored database with the most current information available, run *Analyze/Fix Databases* with *Contents* selected, as described in [Section 27.1, “Analyzing and Fixing User and Message Databases,”](#) on page 409.

32.5 Restoring Deleted Mailbox Items

With proper planning, you can assist users in retrieving accidentally deleted items and items that became unavailable because of database damage.

- [Section 32.5.1, “Setting Up a Restore Area,”](#) on page 435
- [Section 32.5.2, “Restoring a User’s Mailbox Items,”](#) on page 437
- [Section 32.5.3, “Letting Client Users Restore Their Own Mailbox Items,”](#) on page 437

NOTE: Setting up a restore area enables users to restore deleted mailbox items (messages, appointments, tasks, and so on), but not deleted contacts (entries in Contacts folders and personal address books).

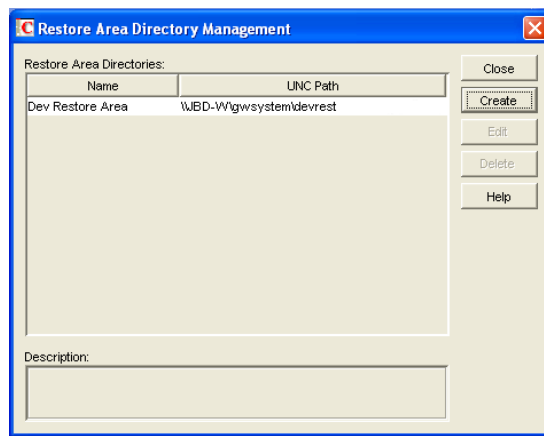
32.5.1 Setting Up a Restore Area

A restore area is only as useful as the post office data that is backed up regularly. Make sure you are backing up every GroupWise post office regularly, as described in [Section 31.2, “Backing Up a Post Office,”](#) on page 431.

A restore area is a location you designate to hold a backup copy of a post office so that you or GroupWise Windows client users can access it to retrieve mailbox items that are unavailable in your live GroupWise system.

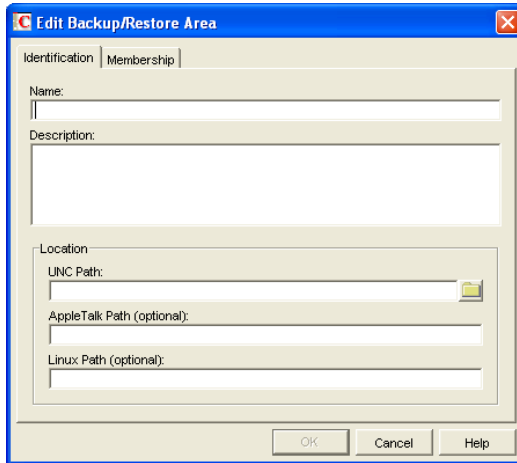
To set up a restore area:

- 1 Create a backup copy of the post office directory for users to access as a restore area.
The name of the restore area directory must follow the same conventions as a post office directory, as described in [Section 11.2.5, “Deciding Where to Create the Post Office Directory,”](#) on page 177.
- 2 In ConsoleOne, click *Tools > GroupWise System Operations > Restore Area Management*.



The Restore Area Directory Management dialog box lists any restore areas that currently exist in your GroupWise system.

- 3 Click *Create* to set up a new restore area.



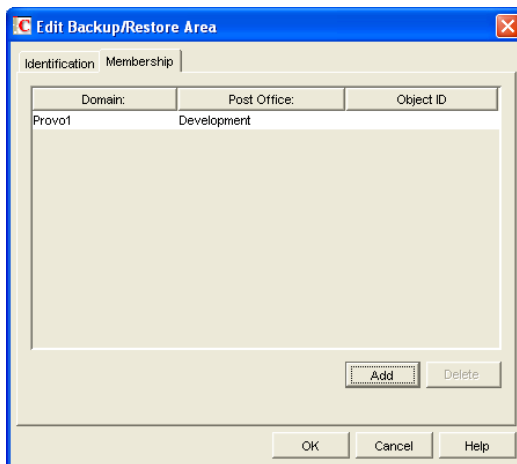
- 4 On the *Identification* tab, specify a unique name for the new restore area. If desired, provide a lengthier description to further identify the restore area.

You can set up one restore area per post office.

- 5 In the *UNC Path* field, browse to and select the directory that you created in [Step 1](#).
- 6 (Conditional) For a restore area on Linux, specify the full path to the directory that you created in [Step 1](#) in the *Linux Path* field in Linux path format, so that the Linux POA can locate the restore area.

ConsoleOne needs the UNC path in order to locate the restore area from its viewpoint on the network, and the Linux POA needs the Linux path in order to locate the restore area from its viewpoint on the Linux server.

- 7 Click *Membership*.



- 8 Click *Add*, select the post office, or one or more individual users in the post office, that need access to the new restore area, then click *OK* to add them to the membership list.

- 9 When the membership list is complete, click *OK* to create the new restore area.

If you display the Post Office Settings page for a post office that has a restore area assigned to it, you see that the *Restore Area* field has been filled in.

- 10 Use the backup software for your platform, as listed in [Section 31.2, “Backing Up a Post Office,” on page 431](#), to restore a backup copy of the post office into the restore area.
- 11 Grant the POA the following rights to the restore area:

Linux: 755

Windows: Change

- 12 (Conditional) For a restore area on Windows, if the restore area is located on a different server from where the post office directory is located, provide the POA with a user name and password for logging in to the remote server.

You can provide that information using the *Remote User Name* and *Password* fields on the Post Office object’s Post Office Settings page, or using the `/user` and `/password` startup switches.

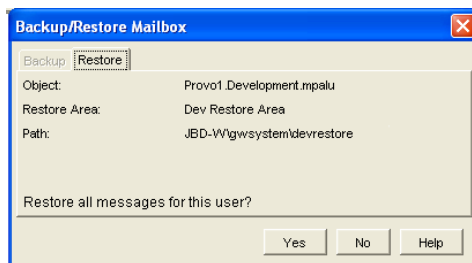
- 13 Continue with [Section 32.5.2, “Restoring a User’s Mailbox Items,” on page 437](#) or [Section 32.5.3, “Letting Client Users Restore Their Own Mailbox Items,” on page 437](#) as needed.

32.5.2 Restoring a User’s Mailbox Items

After you have set up a restore area and placed a backup copy of a post office into it, you can restore a user’s mailbox items for the user.

- 1 In ConsoleOne, browse to and select a User object for which you need to restore mailbox items.
- 2 Click *Tools > GroupWise Utilities > Backup/Restore Mailbox*.

The *Restore* tab is automatically selected for you, with the restore area and directory location displayed for verification.



- 3 Click *Yes* to restore the selected user’s mailbox items into his or her mailbox.
- 4 Notify the user and explain the following about the restored items:
 - ♦ The user might want to manually delete unwanted restored items.
 - ♦ The user should file or archive the items that he or she wants within seven days. After seven days, unaccessed items are deleted after the amount of time allowed by existing auto-delete settings, as described in [“Environment Options: Cleanup” on page 1039](#). If auto-deletion is not enabled, the restored items remain in the mailbox indefinitely.

32.5.3 Letting Client Users Restore Their Own Mailbox Items

After you have set up a restore area and given client users access to it, users can selectively restore individual items into their mailboxes. This saves you the work of restoring mailbox items for users and it also saves users the work of deleting unwanted restored items.

In the backup copy of a mailbox, only items that are different from the live mailbox are displayed. If the backup mailbox looks empty, it means that it matches the contents of the live mailbox.

After a restore area has been set up:

- 1 In the GroupWise client, click *File > Open Backup*.
- 2 (Conditional) If you are prompted:
 - 2a In the *Restore From* field, browse to and select the restore area directory.
 - 2b In the *Password* field, type your GroupWise password.
 - 2c Click *OK* to access the backup copy of your mailbox.
- 3 Retrieve individual items as needed.

The backup copy of your mailbox offers basic features such as Read, Search, and Undelete so that you can locate and retrieve the items you need.
- 4 When you are finished restoring items to your live mailbox, click *File > Open Backup* again to remove the check mark from the *Open Backup* option and return to your live mailbox.

32.6 Recovering Deleted GroupWise Accounts

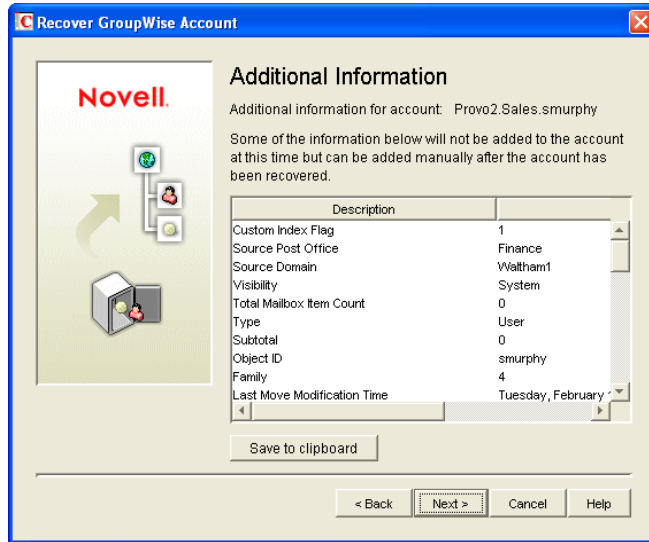
If you have a reliable backup procedure in place, as described in [Chapter 31, “Backing Up GroupWise Databases,”](#) on page 431, you can restore recently deleted GroupWise user and resource accounts.

- 1 Make available a backup copy of a domain database (`wpdomain.db`) where the deleted GroupWise account still exists.
- 2 In ConsoleOne, click *Tools > GroupWise Utilities > Recover Deleted Account*.



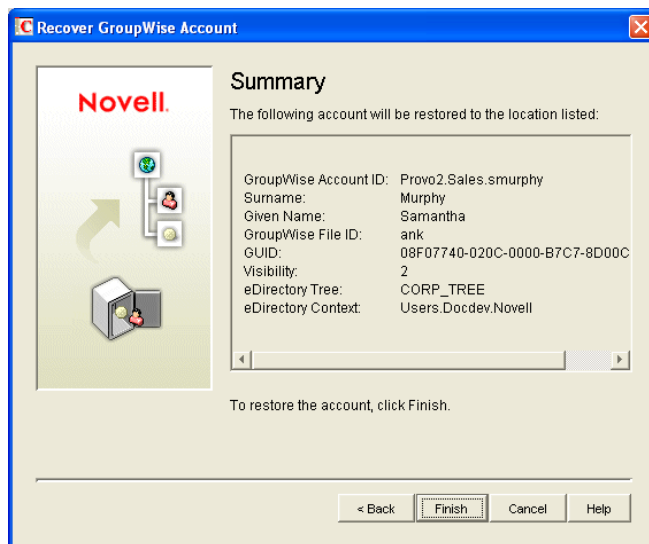
- 3 Browse to and select the backup copy of the domain database.
- 4 Select the user or resource that you need to recover the account for.

5 Click *Next*.



6 If desired, click *Save to Clipboard*, paste the information into a file, then save or print it.

7 Click *Next*.



8 Click *Finish*.

At this point, you have restored the user's or resource's GroupWise account into the GroupWise system. However, this does not restore ownership of resources, nor does the account's mailbox contain any item at this point.

- 9 If the restored user owned resources, manually restore the ownership, as described in [Section 16.2, "Changing a Resource's Owner,"](#) on page 271
- 10 To restore the contents of the account's mailbox, follow the instructions in [Section 32.5, "Restoring Deleted Mailbox Items,"](#) on page 435.

33 Retaining User Messages

GroupWise enables you to retain user messages until they have been copied from message databases to another storage location. This means that a user cannot perform any action, such as emptying the mailbox Trash, that results in a message being removed from the message database before it has been copied.

Message retention primarily consists of three activities: 1) not allowing users to remove messages until they have been retained, 2) retaining the messages by copying them from message databases to another location, and 3) time-stamping the retained messages so that they can be subsequently deleted.

GroupWise supplies the ability to not allow users to remove messages until they have been retained. It also provides methods for message retention applications to securely access user mailboxes and copy messages. However, it does not provide the message retention application. You must develop or purchase a third-party (non-GroupWise) application that performs this service.

- ♦ [Section 33.1, “How Message Retention Works,” on page 441](#)
- ♦ [Section 33.2, “Acquiring a Message Retention Application,” on page 443](#)
- ♦ [Section 33.3, “Enabling Message Retention,” on page 444](#)

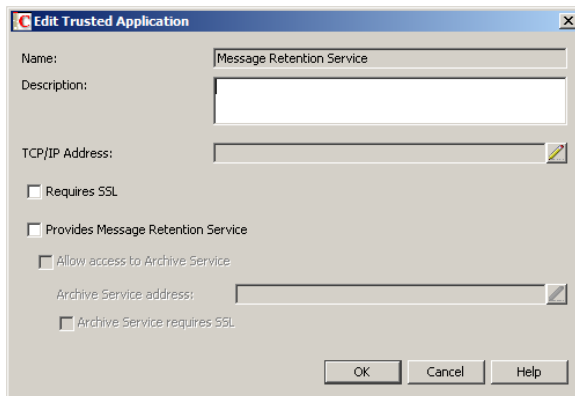
33.1 How Message Retention Works

To understand how message retention works, you need to understand what GroupWise does and what the message retention application does, as explained in the following sections:

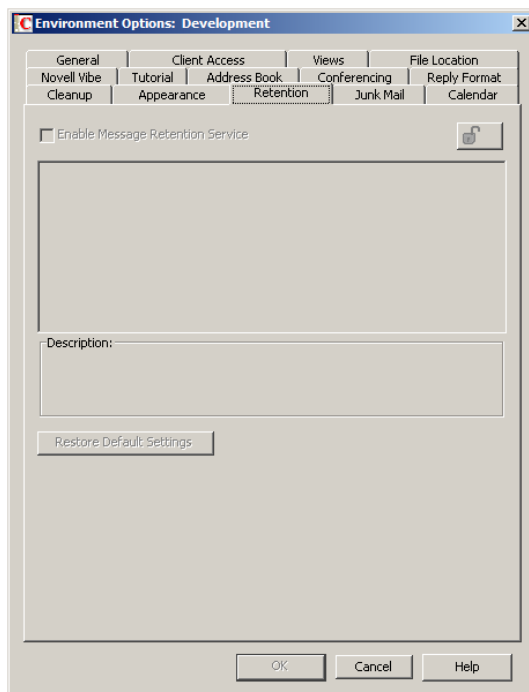
- ♦ [Section 33.1.1, “What GroupWise Does,” on page 442](#)
- ♦ [Section 33.1.2, “What the Message Retention Application Does,” on page 443](#)

33.1.1 What GroupWise Does

During installation of the message retention application, the application uses the GroupWise Trusted Application API to create a trusted application record in the GroupWise system. The trusted application record includes a flag that designates it as a message retention application. This flag is accessed through the trusted application's *Provides Message Retention Service* setting in ConsoleOne (*Tools > GroupWise System Operations > Trusted Applications > Edit*).



When ConsoleOne reads a trusted application record that has the *Provides Message Retention Service* setting turned on, it adds a *Retention* tab to the GroupWise Client Environment Options (*Tools > GroupWise Utilities > Client Options > Environment*).



You use this *Retention* tab to enable message retention at the domain, post office, or user level, meaning that you can enable it for all users in a domain, all users in a post office, or individual users.

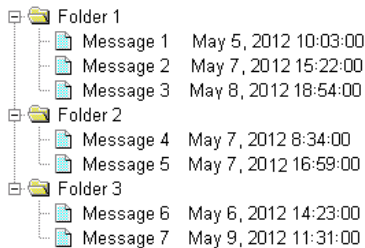
Turning on message retention alters the GroupWise client purge behavior by preventing a user from purging any messages from his or her mailbox that have not yet been retained.

33.1.2 What the Message Retention Application Does

Different message retention applications might vary slightly in their approach to retaining messages. This section provides a general approach to message retention.

To determine whether or not mailbox messages have been retained, the message retention application adds a time stamp to the mailbox. The message retention application can use the GroupWise Object API or GroupWise IMAP support to write (and read) the time stamp. In addition, you can use the [GroupWise Time Stamp Utility \(page 457\)](#) to manually set the time stamp.

The time stamp represents the most recent date and time that message retention was completed for the mailbox. Messages delivered after the time stamp cannot be purged until they have been retained. This requires that the message retention application retain items chronologically, oldest to newest. For example, assume a mailbox has a message retention time stamp of May 7, 2012 12:00:00. The mailbox has three folders with a total of seven messages:



The message retention application reads the existing time stamp (May 7, 2012 12:00:00) and selects a time between that time and the current time. For example, suppose the current time is May 9, 2012 14:00:00. The message retention application could choose May 8, 2012 12:00:00 as the new time stamp. It would then retain any messages delivered between the existing time stamp (May 7, 2012 12:00:00) and the new time stamp (May 8, 2012, 12:00:00).

In the above example, messages 1, 4, and 6 are older than the existing time stamp (May 7, 2012 12:00:00). The message retention application would not retain these messages again, assuming that they had already been safely retained. Messages 2 and 5 have dates that fall between the existing time stamp (May 7, 2012 12:00:00) and the new time stamp (May 8, 2012, 12:00:00) so they would be retained. Messages 3 and 7 have dates that fall after the new time stamp (May 8, 2012, 12:00:00) so they would not be retained until the next time the message retention application ran against the mailbox.

Optionally, the message retention service can be associated with an archive service. For more information, see [Section 4.2.7, "Archive Service Settings," on page 77](#).

33.2 Acquiring a Message Retention Application

If you do not already have a message retention application to use with GroupWise, you have two options: 1) you can purchase an application from a GroupWise partner or 2) you can develop your own application.

For information about GroupWise partners that provide message (email) retention applications, see the [Partner Product Guide \(http://www.novell.com/partnerguid\)](http://www.novell.com/partnerguid).

For information about developing a message retention application, see the *GroupWise Object API* and *GroupWise Trusted Application API* documentation at the [Novell Developer Kit Web site \(http://developer.novell.com/wiki/index.php/Category:Novell_Developer_Kit\)](http://developer.novell.com/wiki/index.php/Category:Novell_Developer_Kit).

33.3 Enabling Message Retention

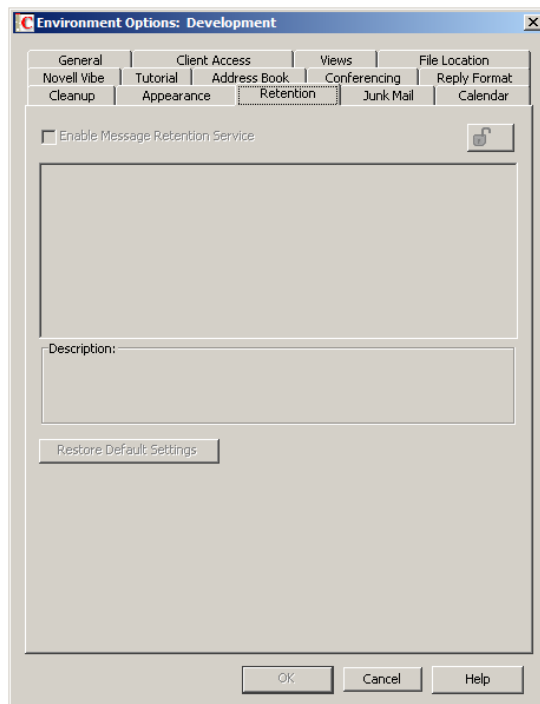
This section assumes that you have installed a message retention application as a GroupWise trusted application and that it is configured to provide a message retention service. If not, see [Section 4.12, “Trusted Applications,”](#) on page 90.

Message retention is not enabled until you designate the users whose messages you want retained by the application. You can designate users at the domain level, post office level, or individual user level.

- 1 In ConsoleOne, right-click the domain, post office, or user for which you want to enable message retention, click *GroupWise Utilities > Client Options* to display the GroupWise Client Options dialog box.



- 2 Click *Environment* to display the Environment Options dialog box, then click the *Retention* tab.



- 3 Turn on the *Enable Message Retention Service* setting.
- 4 If you want to lock the setting at this level, click the *Lock* button.

For example, if you lock the setting at the domain level, the setting cannot be changed for any post offices or users within the domain. If you lock the setting at the post office level, it cannot be changed individually for the post office's users.

This setting does not display in the GroupWise client. Therefore, there is no lock available when editing this setting for individual users.

- 5 Click *OK* to save the changes.

34 Stand-Alone Database Maintenance Programs

Some aspects of GroupWise database maintenance are performed by stand-alone maintenance programs that can be incorporated into batch files along with other system maintenance programs.

- ◆ [Section 34.1, “GroupWise Check,” on page 447](#)
- ◆ [Section 34.2, “GroupWise Time Stamp Utility,” on page 457](#)
- ◆ [Section 34.3, “GroupWise Database Copy Utility,” on page 463](#)

34.1 GroupWise Check

GroupWise Check (GWCheck) is a tool provided for GroupWise to check and repair GroupWise user, message, library, and resource databases without using ConsoleOne. In addition to checking post office, user, and library databases, it also checks users’ remote, caching, and archive databases.

The GWCheck utility runs on Linux and Windows. You should match the platform of GWCheck to the platform where the databases are located. Linux GWCheck processes databases on Linux. Windows GWCheck processes databases on Windows.

IMPORTANT: GWCheck should not be used to process databases that are located across a network connection between different machines.

- ◆ [Section 34.1.1, “GWCheck Functionality,” on page 447](#)
- ◆ [Section 34.1.2, “Using GWCheck on Windows,” on page 449](#)
- ◆ [Section 34.1.3, “Using GWCheck on Linux,” on page 450](#)
- ◆ [Section 34.1.4, “Performing Mailbox/Library Maintenance Using GWCheck,” on page 452](#)
- ◆ [Section 34.1.5, “Executing GWCheck from a Windows Batch File,” on page 454](#)
- ◆ [Section 34.1.6, “Executing GWCheck from a Linux Script,” on page 455](#)
- ◆ [Section 34.1.7, “GWCheck Startup Switches,” on page 455](#)

34.1.1 GWCheck Functionality

The GWCheck utility begins by comparing three databases.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
The post office database (wphost.db) is checked for the file ID (FID) of the selected user.	The guardian database (ngwguard.db) is checked to find out if this user database has been created.	The file system for this post office is checked to see if the user database (userxxx.db) for this user exists.

After GWCheck makes the database comparisons, it begins processing according to the databases selected and any inconsistencies found.

Case 1 - Missing Entry in the Post Office Database (wphost.db)

In this example, a contents check is run either against all users on the post office or against one user, "ABC." GWCheck does not find the FID of one or more users.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
?	userabc.db	userabc.db
No entry for this user is found in the post office database (wphost.db).	An entry is found in the guardian database (ngwguard.db), indicating that the user has been deleted.	Also, a user database (userxxx.db) for this user is found in the ofuser directory.

GWCheck removes the entry from `ngwguard.db`, deletes `userabc.db`, and systematically deletes all of the user's messages from the message databases that are not still being referenced by other users. If the user has been deleted, GWCheck cleans up after that user.

WARNING: If a post office database becomes damaged so some users are unable to log in, GWCheck should not be run until the post office has been rebuilt. For more information, see [Section 26.3, "Rebuilding Domain or Post Office Databases,"](#) on page 405.

Case 2 - Missing Entry in the Guardian Database (ngwguard.db)

In this example, a GWCheck is run either against all users on the post office or against one user, "ABC." A user's FID is found and the user's database is found in the post office, but the user is missing in `ngwguard.db`.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
FID abc	?	userabc.db
The user appears in the post office database (wphost.db).	The guardian database (ngwguard.db) shows no user database for this user.	A user database (userxxx.db) for the user does exist in the ofuser directory.

GWCheck creates the user in `ngwguard.db`, using database `userabc.db`. Even if `ngwguard.db` is damaged, it is unlikely that data is lost.

Case 3 - Missing User Database (userxxx.db)

In this example, a GWCheck is run either against all users on the post office or against one user, "ABC." The user's FID is found, as well as the user's record in `ngwguard.db`. However, the user's database is not found.

WPHOST.DB	NGWGUARD.DB	FILE SYSTEM
FID abc	userabc.db	?
The user is found in the post office database (wphost.db).	The user is found in the guardian database (ngwguard.db).	No user database (userxxx.db) is found in the ofuser directory.

GWCheck takes action depending on what options are selected.

Contents Check: GWCheck deletes all of this user's messages from the message databases if they are not referenced by other users.

Structural Rebuild: GWCheck creates a blank user database for this user. Existing messages for this user are ignored.

Re-create User Database: GWCheck creates a blank user database for this user and populates it with messages in the message databases that have been sent to or from this user.

WARNING: If a user database has been deleted, do not run a Contents Check until after a Structural Rebuild or Re-create User Database has been run for that user. For more information, see [Section 27.2, "Performing a Structural Rebuild of a User Database,"](#) on page 411 and [Section 27.3, "Re-creating a User Database,"](#) on page 412.

34.1.2 Using GWCheck on Windows

You can use GWCheck on any Windows XP/Vista/7 workstation or Windows 2003/2008 server.

As an administrator, you can run GWCheck for databases in any post office accessible from the workstation where GWCheck is installed. The GWCheck program performs all database maintenance itself, rather than handing off a task to the POA as ConsoleOne would do to perform database maintenance.

Depending on how GWCheck is installed, users can have a Repair Mailbox item on the GroupWise Windows client Tools menu that enables them to run GWCheck from the client. If the GWCheck program is available to users, users can perform database maintenance on their Remote, Caching, and archive mailboxes, which are not accessible from ConsoleOne.

For the Repair Mailbox item to display on the GroupWise Windows client *Tools* menu, the following files must be installed in the GroupWise software directory; by default, this is `c:\Program Files\Novell\GroupWise`.

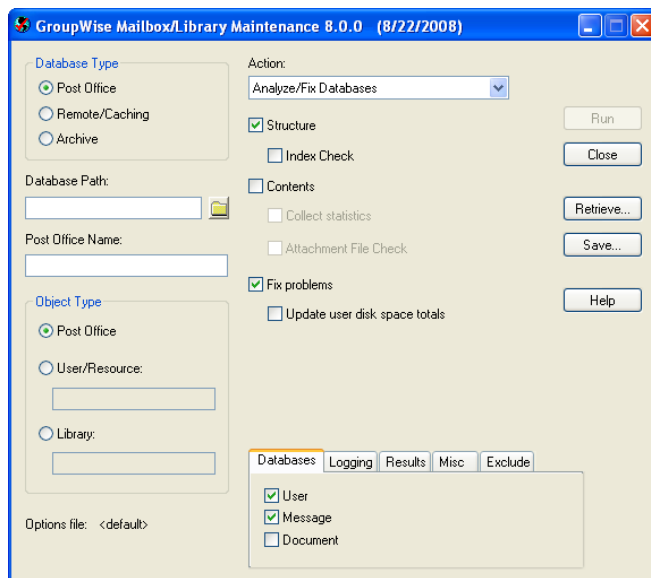
- ◆ `gwcheck.exe`
- ◆ `gwchkxx.dll` (Replace *xx* with your language code)
- ◆ `gwchkxx.chm` (Replace *xx* with your language code)

The GroupWise administrator can install these files by using SetupIP to install the GroupWise Windows client, and selecting to install and enable GWCheck. The default for SetupIP is to install GWCheck, but not enable GWCheck. The files are then copied to the `\novell\groupwise\gwcheck` directory. For additional information about SetupIP and GWCheck, see ["\[GWCheck\]"](#) on page 1078.

If the client was installed using the GroupWise Windows client Setup program or the defaults are chosen for SetupIP, the client user needs to copy the files from the GWCheck directory (`\novell\groupwise\gwcheck`) to the main GroupWise directory (`\novell\groupwise`).

To run GWCheck:

- 1 From the *Start* menu, click *Run*, then browse to and double-click `gwcheck.exe`.



- 2 To view online help in GWCheck, click *Help*.
- 3 Continue with [Section 34.1.4, “Performing Mailbox/Library Maintenance Using GWCheck,”](#) on page 452.

34.1.3 Using GWCheck on Linux

Two versions of GWCheck are available on Linux, one for a graphical user interface (GUI) environment and one for a text-only environment.

- ♦ “Using GUI GWCheck (`gwcheck`)” on page 450
- ♦ “Using Text-Based GWCheck (`gwcheckt`)” on page 451

Using GUI GWCheck (`gwcheck`)

- 1 Change to the directory where the GWCheck RPM is located or copy it to a convenient location on your server.

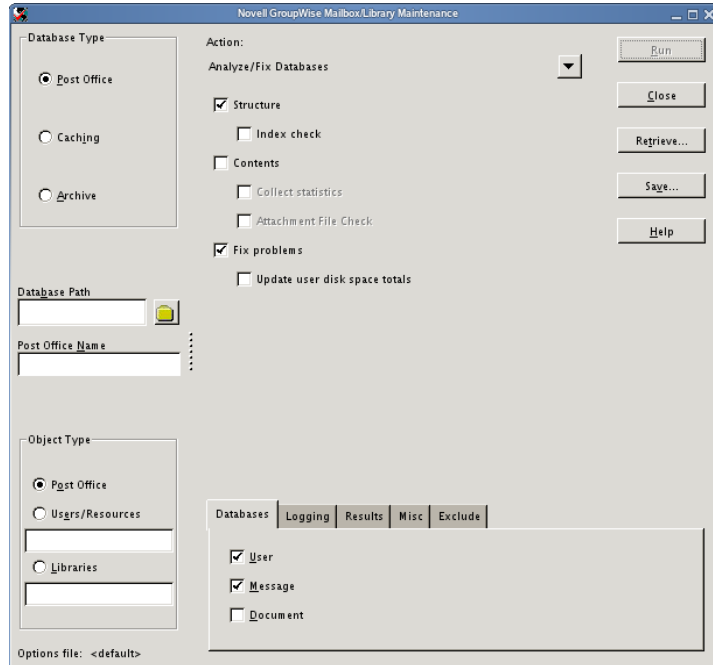
The GWCheck RPM (`groupwise-gwcheck-groupwise_version-build_number.i586.rpm`) is located in the `/admin` directory in your GroupWise software distribution directory if it is has been updated, or in the downloaded *GroupWise 2012* software image.

- 2 Install GWCheck.

```
rpm -i groupwise-gwcheck-groupwise_version-build_number.i386.rpm
```

- 3 Change to the `/opt/novell/groupwise/gwcheck/bin` directory.

- 4 Enter `./gwcheck` to start GWCheck.



- 5 To view online help in GWCheck, click *Help*.
- 6 Continue with [Performing Mailbox/Library Maintenance Using GWCheck](#).

Using Text-Based GWCheck (gwcheckt)

You can use text-based GWCheck in any environment where the X Window System is not available, such as on a text-only server where a post office and its POA are located. However, you must use GUI GWCheck to create an options file before you can run text-based GWCheck.

- 1 Install and run GUI GWCheck in a convenient location, as described in [“Using GUI GWCheck \(gwcheck\)” on page 450](#).
- 2 Select the maintenance activities that you want GWCheck to perform, as described in [Section 34.1.4, “Performing Mailbox/Library Maintenance Using GWCheck,” on page 452](#).
- 3 Save the settings you selected in an options file, as described in [“Saving Mailbox/Library Maintenance Options” on page 454](#).

The default options file name is `gwcheck.opt`.

- 4 Copy the GWCheck RPM to a convenient location on the text-only server.
- 5 Install GWCheck on the text-only server.

```
rpm -i groupwise-gwcheck-version-mmdd.i386.rpm
```

- 6 Copy the GWCheck options file you created in [Step 3](#) to the `/opt/novell/groupwise/gwcheck/bin` directory.
- 7 Change to the `/opt/novell/groupwise/gwcheck/bin` directory.
- 8 Enter `./gwcheckt options_file_name` to run text-based GWCheck.

If you did not copy the options file to your home directory on the text-only server, specify the full path to the options file.

Over time, a collection of options files might accumulate. To see what maintenance activities an options file performs, use `./gwcheckt options_file_name --dump`.

To remind yourself of these options when you are at your Linux server, view the [gwcheckt](#) man page.

34.1.4 Performing Mailbox/Library Maintenance Using GWCheck

With only a few differences in interface functionality, as described in the online help, you can perform the same maintenance activities in GWCheck as you can in Mailbox/Library Maintenance in ConsoleOne:

- ♦ [“Using Mailbox/Library Maintenance Tab Options”](#) on page 452
- ♦ [“Reusing Mailbox/Library Maintenance Settings”](#) on page 454

Using Mailbox/Library Maintenance Tab Options

Both GWCheck and Mailbox/Library Maintenance in ConsoleOne use tab options to control the checking process.

- ♦ [“Databases”](#) on page 452
- ♦ [“Logging”](#) on page 453
- ♦ [“Results”](#) on page 453
- ♦ [“Misc”](#) on page 453
- ♦ [“Exclude”](#) on page 454

Databases

To select the types of database to perform the Mailbox/Library Maintenance check on, click *Databases*.



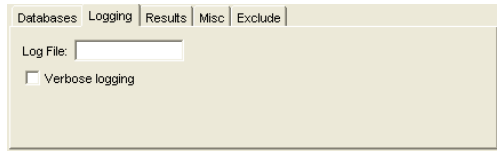
Depending on the object type and action already selected in the main window, some database types might be unavailable. If all the database types are unavailable, then one or more database types have been preselected for you.

You can perform an action on the following databases when the type is not unavailable:

- ♦ **User:** Checks the [user databases](#).
- ♦ **Message Databases:** Checks the [message databases](#).
- ♦ **Document:** Checks the [library and document properties databases](#).

Logging

To specify the name of the file where you want the results of the MailBox/Library Maintenance check to be stored, click *Logging*.



The screenshot shows a window with tabs: Databases, Logging, Results, Misc, and Exclude. The Logging tab is active. It contains a text input field labeled "Log File:" and a checkbox labeled "Verbose logging".

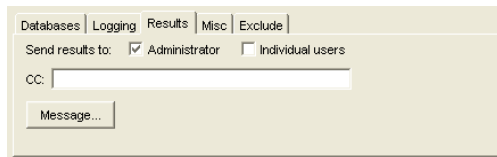
Specify a file name. By default, the file is created in the *post_office_directory*\wpcout\ofs directory.

Click *Verbose Logging* to log detailed information. Verbose logging might produce large log files and slow execution.

This file is sent to the users selected on the *Results* tab.

Results

To select users to receive the results of the Mailbox/Library Maintenance check, click *Results*.

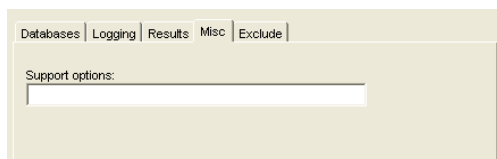


The screenshot shows a window with tabs: Databases, Logging, Results, Misc, and Exclude. The Results tab is active. It contains a section "Send results to:" with two radio buttons: "Administrator" (checked) and "Individual users". Below this is a text input field labeled "CC:" and a button labeled "Message...".

Select *Administrator* to send the results to the user defined as the GroupWise domain administrator. Select *Individual Users* to send each user the results that pertain to him or her. Specify each user's GroupWise user ID (mailbox ID) or email address in a comma-delimited list. Click *Message* to include a message with the results file.

Misc

If you need to run a Mailbox/Library Maintenance check with special options provided by Novell Support, click *Misc*.

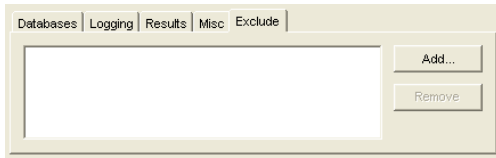


The screenshot shows a window with tabs: Databases, Logging, Results, Misc, and Exclude. The Misc tab is active. It contains a text input field labeled "Support options:".

Use the *Support Options* field to specify command line parameters. Support options are typically obtained from Novell Support representatives when you need assistance resolving specific database problems. Search the [Novell Support Knowledgebase \(http://www.novell.com/support\)](http://www.novell.com/support) for TIDs and Support Pack Readmes that list support options. Make sure that you clearly understand what the Support options do before you use them.

Exclude

If you want to exclude certain users in the selected post office from having the Mailbox/Library Maintenance check performed on their databases, click *Exclude*.



Click *Add*, select one or more users to exclude, then click *OK*.

Reusing Mailbox/Library Maintenance Settings

For convenience, you can store the options you select in Mailbox/Library Maintenance and GWCheck so that you can retrieve them for later use.

- ♦ [“Saving Mailbox/Library Maintenance Options” on page 454](#)
- ♦ [“Retrieving Mailbox/Library Maintenance Options” on page 454](#)

Saving Mailbox/Library Maintenance Options

- 1 After you have selected all of the options in the Mailbox/Library Maintenance dialog box, click *Save*.
- 2 Browse to the directory where you want to save the options file.
You might want to save it in the [domain directory](#) to which you are currently connected.
- 3 Specify a file name if you do not want to use the default of `gwcheck.opt`.
- 4 Click *Save*.

The GWCheck options file is created in XML format on all platforms. Therefore, you can create the GWCheck options file on any platform and use it on any platform interchangeably.

Retrieving Mailbox/Library Maintenance Options

- 1 In the Mailbox/Library Maintenance dialog box, click *Retrieve*.
- 2 Browse to and select your saved option file.
- 3 Click *Open*.

34.1.5 Executing GWCheck from a Windows Batch File

The GWCheck program is located in the `\admin\utility\tools` directory in your GroupWise software distribution directory if it has been updated, or in the downloaded *GroupWise 2012* software image if an updated software distribution directory is not available. It might also be installed along with the GroupWise client software in the `gwcheck` subdirectory of the client installation directory.

- 1 Use the following syntax to create a batch file to execute GWCheck:

```
gwcheck /opt=options_file /batch
```

If you want to include the path to an archive database, use the `/pa` switch.

- 2 To create an options file, see [“Saving Mailbox/Library Maintenance Options” on page 454](#).

34.1.6 Executing GWCheck from a Linux Script

The GWCheck program is located in the `/admin` directory in your GroupWise software distribution directory if it has been updated, or in the downloaded *GroupWise 2012* software image if an updated software distribution directory is not available.

- 1 Make sure that GWCheck has been installed, as described in [Section 34.1.3, “Using GWCheck on Linux,”](#) on page 450
- 2 Create a script to execute GWCheck using the following syntax:

```
/opt/novell/groupwise/gwcheck/bin/gwcheck --opt=options_file --batch
```

If you did not create the options file in your home directory, specify the full path to the options file.

If you want to include the path to an archive database, use the `--pa` switch.

- 3 To create an options file, see [“Saving Mailbox/Library Maintenance Options”](#) on page 454.

34.1.7 GWCheck Startup Switches

The following startup switches can be used with GWCheck:

Linux GWCheck	Windows GWCheck
<code>--batch</code>	<code>/batch</code>
<code>--lang</code>	<code>/lang</code>
<code>--opt</code>	<code>/opt</code>
<code>--pa</code>	<code>/pa</code>
<code>--po</code>	<code>/po</code>
<code>--pr</code>	<code>/pr</code>

/batch

Indicates that you want to run GWCheck without a user interface. Because you do not provide the desired options from the interface, you must provide an options file.

	Linux GWCheck	Windows GWCheck
Syntax:	<code>--batch</code>	<code>/batch</code>

For example, to specify that you want GWCheck to run it batch mode, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --batch`

Windows: `gwcheck /opt=gwcheck.opt /batch`

/lang

Specifies the language to run GWCheck in, using a two-letter language code. You must install GWCheck in the selected language in order for it to display in the selected language.

	Linux GWCheck	Windows GWCheck
Syntax:	<code>--lang=<i>language_code</i></code>	<code>/lang=<i>language_code</i></code>

For a list of current language codes, see [Chapter 7, “Multilingual GroupWise Systems,”](#) on page 123.

For example, to specify that you want GWCheck to run in Spanish, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --lang=es`

Windows: `gwcheck /opt=gwcheck.opt /lang=es`

/opt

Specifies a database maintenance options file created in a GWCheck session. This starts GWCheck with the same options settings as the session in which the options file was created. The default location of the options file varies by platform:

Linux: User’s home directory

Windows: Directory where `gwcheck.exe` is installed.

If the options file is not in the default directory, you must specify the full path name.

	Linux GWCheck	Windows GWCheck
Syntax:	<code>--opt=<i>file_name</i></code>	<code>/opt=<i>file_name</i></code>

For example, to start GWCheck with saved settings, you would use:

Linux: `./gwcheck --opt=gwcheck.opt`
`./gwcheck --opt=/gwsystem/post1/gwcheck.opt`

Windows: `gwcheck /opt=gwcheck.opt`
`gwcheck /opt=\gwsystem\post1\gwcheck.opt`

/pa

Specifies the path to an archive database.

	Linux GWCheck	Windows GWCheck
Syntax:	<code>--pa=<i>path_to_archive</i></code>	<code>/pa=<i>path_to_archive</i></code>

For example, to specify the archive database that a user keeps in his or her home directory, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --batch --pa=/home/gsmith/of7bharc`

Windows: `gwcheck /opt=gwcheck.opt /batch /pa=\home\gsmith\of7bharc`

/po

Specifies the path to a post office.

	Linux GWCheck	Windows GWCheck
Syntax:	<code>--po=path_to_post_office</code>	<code>/po=path_to_post_office</code>

For example, to specify a post office directory, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --batch --po=/mail/sales`

Windows: `gwcheck /opt=gwcheck.opt /batch /po=\mail\sales`

/pr

Specifies the path to a Remote mailbox.

	Linux GWCheck	Windows GWCheck
Syntax:	<code>--pr=path_to_mailbox</code>	<code>/pr=path_to_mailbox</code>

For example, to specify the Remote mailbox that a user keeps on a computer at home, you would use:

Linux: `./gwcheck --opt=gwcheck.opt --pr=/novell/groupwise\of7bharc`

Windows: `gwcheck /opt=gwcheck.opt /pr=\novell\groupwise\of7bharc`

34.2 GroupWise Time Stamp Utility

You can use the GroupWise Time Stamp (GWTMSTMP) utility to ensure that GroupWise user databases include the dates when they were last backed up, restored, and retained.

The following sections provide information about the utility:

- [Section 34.2.1, “GWTMSTMP Functionality,” on page 457](#)
- [Section 34.2.2, “Running GWTMSTMP on Linux,” on page 458](#)
- [Section 34.2.3, “Running GWTMSTMP on Windows,” on page 459](#)
- [Section 34.2.4, “GWTMSTMP Startup Switches,” on page 459](#)

34.2.1 GWTMSTMP Functionality

GWTMSTMP places date and time information on user databases (`userxxx.db`) in order to support message backup, restore, and retention. No other databases are affected. You can run GWTMSTMP on all user databases in a post office or on a single user database.

Backup

To ensure thorough user database backups, you can make sure that deleted items are not purged from users' databases until they have been backed up. Two conditions must be met in order to provide this level of protection against loss of deleted items:

- ♦ The *Do Not Purge Items Until They Are Backed Up* option must be selected in ConsoleOne, as described in [“Environment Options: Cleanup” on page 1039](#).
- ♦ User databases (`userxxx.db`) must be time-stamped every time a backup is performed so that items can be purged only after being backed up.

Restore

The restore time stamp is not required for any GroupWise feature to work properly. Its primary purpose is informational.

Retention

If you use a message retention application, as described in [Chapter 33, “Retaining User Messages,” on page 441](#), the application should automatically add the retention time stamp after retaining the database's messages. Any messages with dates that are newer than the retention time stamp cannot be purged from the database.

You can also use GWTMSTMP to manually add a retention time stamp.

Modified Retention

If you use a message retention application, you might need to retain items more than once if you want to capture changes to personal subjects and personal attachments on items. You can use GWTMSTMP to manually update the retention time stamp on modified items, so that they are retained again.

34.2.2 Running GWTMSTMP on Linux

The GWTMSTMP executable (`gwtmstmp`) is installed into the `bin` and `lib` subdirectories of `/opt/novell/groupwise/agents` along with the GroupWise agents (POA and MTA). You can copy it to additional locations if needed.

To check the existing time stamp on all GroupWise user databases in a post office, use the following command:

Syntax:

```
./gwtmstmp -p /post_office_directory
```

Example:

```
./gwtmstmp -p /gwsystem/acct
```

The results are displayed on the screen.

To set a current time stamp on all user databases in a post office, use the following command:

Syntax:

```
./gwtmstmp -p /post_office_directory --set
```

Example:

```
./gwtmstmp -p /gwsystem/acct --set
```

A basic backup time stamp can also be set in ConsoleOne. Select a Post Office object, then click *Tools > GroupWise Utilities > Backup/Restore Mailbox*. On the *Backup* tab, select *Backup*, then click *Yes*.

More specialized functionality is provided through additional GWTMSTMP startup switches. See [Section 34.2.4, “GWTMSTMP Startup Switches,” on page 459](#).

To remind yourself of these options when you are at your Linux server, view the [gwtmstmp](#) man page.

34.2.3 Running GWTMSTMP on Windows

The GWTMSTMP program file (`gwtmstmp.exe`) is installed into the same directory where you installed the GroupWise agents (POA and MTA). You can copy it to additional locations if needed.

To check the existing time stamp on all GroupWise user databases in a post office, use the following command:

Syntax:

```
gwtmstmp.exe /p-drive:\post_office_directory
```

Example:

```
gwtmstmp.exe /p-m:\gwsystem\acct
```

The results are displayed on the screen

To set a current time stamp on all user databases in a post office, use the following command:

Syntax:

```
gwtmstmp.exe /p-drive:\post_office_directory /set
```

Example:

```
gwtmstmp.exe /p-m:\gwsystem\acct /set
```

A basic backup time stamp can also be set in ConsoleOne. Select a Post Office object, then click *Tools > GroupWise Utilities > Backup/Restore Mailbox*. On the *Backup* tab, select *Backup*, then click *Yes*.

More specialized functionality is provided through additional GWTMSTMP startup switches.

34.2.4 GWTMSTMP Startup Switches

The following startup switches can be used with GWTMSTMP:

Linux GWTMSTMP	Windows GWTMSTMP
-p	/p
--backup or -b	/backup
--restore or -r	/restore
--retention or -n	/retention
--modifiedretention or -mn	/modifiedretention

Linux GWTMSTMP	Windows GWTMSTMP
--get or -g	/get
--set or -s	/set
--clear or -c	/clear
--date or -d	/date
--time or -t	/time
--gmttime or -m	/gmttime
--userid or -u	/u
--userdb or -e	/userdb

-p

Specifies the post office directory where the user databases to time-stamp are located. This switch is required.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>-p /post_office_dir</code>	<code>/p-drive:\post_office_dir</code>
Example:	<code>-p /gwsystem/dev</code>	<code>/p-j:\dev</code>

--backup, --restore, --retention, and --modifiedretention

Specifies the time stamp on which to perform the get or set operation. If no time stamp is specified, the operation is performed on the backup time stamp.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--backup -b</code>	<code>/backup</code>
	<code>--restore -r</code>	<code>/restore</code>
	<code>--retention -n</code>	<code>/retention</code>
	<code>--modifiedretention -mn</code>	<code>/modifiedretention</code>

For example, to set the restore time stamp, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --restore --set`

Windows: `gwtmstmp /p-j:\dev /restore /set`

--get

Lists existing backup, restore, and retention time stamp information for user databases. If no time stamps are set, no times are displayed.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--get -g</code>	<code>/get</code>

For example:

Linux: `./gwtmstmp -p /gwsystem/dev --get`

Windows: `gwtmstmp /p-j:\dev /get`

If no other operational switch is used, `/get` is assumed. The following example returns the same results as the above example:

Linux: `./gwtmstmp -p /gwsystem/dev`

Windows: `gwtmstmp /p-j:\dev`

--set

Sets the current date and time on user databases.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--set -s</code>	<code>/set</code>

For example, to set the backup time stamp, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --backup --set`

Windows: `gwtmstmp /p-j:\dev /backup /set`

or

Linux: `./gwtmstmp -p /gwsystem/dev --set`

Windows: `gwtmstmp /p-j:\dev /set`

--clear

Clears existing time stamps.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--clear -c</code>	<code>/clear</code>

For example, to clear all time stamps on databases in a post office, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --clear`

Windows: `gwtmstmp /p-j:\dev /clear`

--date

Specifies the date that you want placed on user databases.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--date mm/dd/yyyy -d mm/dd/yyyy</code>	<code>/date-mm/dd/yyyy</code>
Example:	<code>--date 05/18/2012 -d 05/18/2012</code>	<code>/date-04/12/2012</code>

For example, to set the restore date to June 15, 2012, you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --restore --date 06/15/2012`

Windows: `gwtmstmp /p-j:\dev /restore /date-06/14/2012`

--time

Specifies the time that you want placed on user databases.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--time hh:mm am pm -t hh:mm am pm</code>	<code>/time-hh:mm am pm</code>
Example:	<code>--time 2:00am -t 2:00am</code>	<code>/time-6:15pm</code>

For example, to set the restore time to 4:45 p.m., you would use:

Linux: `./gwtmstmp -p /gwsystem/dev --restore --time 4:45pm`

Windows: `gwtmstmp /p-j:\dev /restore /time-4:45pm`

--gmttime

Specifies the time in seconds since January 1, 1970, Greenwich Mean Time (GMT), that you want placed on user databases.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--gmttime seconds -m seconds</code>	<code>/gmttime-seconds</code>

--userid

Provides a specific GroupWise user ID so that an individual user database can be time-stamped.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--userid userID -u userID</code>	<code>/u-userID</code>
Example:	<code>---userid gsmith -u gsmith</code>	<code>/u-mbarnard</code>

For example, to set the retention time stamp for a user whose GroupWise user ID is mpalu, you would use:

```
Linux:      ./gwtmstamp -p /gwsystem/dev --userid mpalu --retention --set
```

```
Windows:   gwtmstamp /p-j:\dev /u-mpalu /retention /set
```

--userdb

Provides a specific GroupWise user database (`userxxx.db`) so that an individual user database can be time-stamped.

	Linux GWTMSTMP	Windows GWTMSTMP
Syntax:	<code>--userdb user_database -e user_database</code>	<code>/userdb user_database</code>
Example:	<code>--userdb user3gh.db</code>	<code>/userdb user3gh.db</code>

For example, to set the retention time stamp for a user whose user database is named user3gh, you would use:

```
Linux:      ./gwtmstamp -p /gwsystem/dev --userdb user3gh.db --retention --set
```

```
Windows:   gwtmstamp /p-j:\dev /userdb user3gh.db /retention /set
```

34.3 GroupWise Database Copy Utility

You can use the GroupWise Database Copy Utility to back up your GroupWise system if you would prefer not to purchase a third-party backup solution, as recommended in [Chapter 31, “Backing Up GroupWise Databases,”](#) on page 431.

- ♦ [Section 34.3.1, “DBCOPY Functionality,”](#) on page 463
- ♦ [Section 34.3.2, “Using DBCOPY on Linux,”](#) on page 464
- ♦ [Section 34.3.3, “Using DBCOPY on Windows,”](#) on page 465
- ♦ [Section 34.3.4, “DBCOPY Startup Switches,”](#) on page 465

IMPORTANT: If you want to move domains and post offices from NetWare or Windows to Linux, see the *GroupWise Server Migration Guide*. The migration process includes DBCopy startup switches that are not described in this *GroupWise 2012 Administration Guide* because they are used only for migration.

34.3.1 DBCopy Functionality

The GroupWise Database Copy utility (DBCOPY) copies files from a live GroupWise post office or domain to a static location for backup. During the copy process, DBCOPY prevents the files from being modified, using the same locking mechanism used by other GroupWise programs that access

databases. This ensures that the backed-up versions are consistent with the originals even when large databases take a substantial amount of time to copy. DBCopy is a multi-threaded application that provides highly efficient copying of large quantities of data.

DBCopY copies only GroupWise-recognized directories and files, as illustrated in “Post Office Directory” and “Domain Directory” in “Directory Structure Diagrams” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*. DBCopY does not copy some directories:

- ♦ Post office queue directories (`wpcsin` and `wpcout`): Only post office data files and directories are copied. Queue directories are not copied.
- ♦ All domain **subdirectories**: Only domain files are copied. Queue directories are not copied.
- ♦ All subdirectories under each gateway directory in `wpgate`: Only gateway files are copied from each gateway directory. Queue directories of gateway directories are not copied. For example, under `gwia`, gateway files are copied, but no gateway subdirectories are copied.

When planning disk space for your backups, you should plan to have at least three times the size of a post office. This accommodates the post office itself, the backup of the post office, and extra space for subsequent growth of the post office.

Typically, domains grow less than post offices, so domain backups should occupy somewhat less disk space.

34.3.2 Using DBCopY on Linux

- 1 Change to the directory where the DBCopY RPM is located or copy it to a convenient location on your workstation.

The DBCopY RPM (`groupwise-dbcopy-version-mmdd.i386.rpm`) is located in the `/admin` directory in your GroupWise software distribution directory if you have created one or in the downloaded *GroupWise 2012* software image.

- 2 Install DBCopY.

```
rpm -i groupwise-dbcopy-version-mmdd.i386.rpm
```

- 3 Change to the `/opt/novell/groupwise/agents/bin` directory.

- 4 Use the following command to back up a post office:

```
./dbcopY /post_office_directory /destination_directory
```

or

Use the following command to back up a domain:

```
./dbcopY /domain_directory /destination_directory
```

or

Use the following command to back up a remote document storage area:

```
./dbcopY -b /storage_area_directory /destination_directory
```

You can include the `-i` switch in any of these commands to provide the date (`mm-dd-yyyy`) of the previous copy. This causes DBCopY to copy only files that have been modified since the previous copy, like an incremental backup.

To remind yourself of these options when you are at your Linux server, view the `dbcopY` man page.

DBCopY creates a log file named *mmdgwbk.nnn*. The first four characters represent the date. A three-digit extension allows for multiple log files created on the same day. The log file is created at the root of the destination directory. Include the *-v* switch in the *dbcopY* command to enable verbose logging for the backup.

- 5 After DBCopY has finished copying the post office, domain, or remote document storage area, use your backup software of choice to back up the static copy of the data.
- 6 After the backup has finished, delete the static copy of the data to conserve disk space.

You might find it helpful to set up a cron job to run DBCopY regularly at a time of day when your system is not busy.

34.3.3 Using DBCopY on Windows

- 1 At a command prompt, change to the directory where you installed the GroupWise agents (typically *c:\Program Files\Novell\GroupWise Server\Agents*).
- 2 Use the following command to back up a post office:

```
dbcopY.exe \post_office_directory \destination_directory
```

or

Use the following command to back up a domain:

```
dbcopY.exe \domain_directory \destination_directory
```

or

Use the following command to back up a remote document storage area:

```
dbcopY.exe /b \storage_area_directory \destination_directory
```

You can include the */i* switch in any of these commands to provide the date (*mm-dd-yyyy*) of the previous copy. This causes DBCopY to copy only files that have been modified since the previous copy, like an incremental backup.

DBCopY creates a log file named *mmdgwbk.nnn*. The first four characters represent the date. A three-digit extension allows for multiple log files created on the same day. The log file is created at the root of the destination directory. Include the */v* switch in the *dbcopY* command to enable verbose logging for the backup.

- 3 After DBCopY has finished copying the post office, domain, or remote document storage area, use your backup software of choice to back up the static copy of the data.
- 4 After the backup has finished, delete the static copy of the data to conserve disk space.

34.3.4 DBCopY Startup Switches

The following startup switches can be used with DBCopY when you are preparing to back up GroupWise data:

Linux DBCopY	Windows DBCopY	Explanation
<i>--b</i>	<i>/b</i>	Backup of BLOB files in a document storage area
<i>-i</i>	<i>/i</i>	Incremental backup
<i>-j</i>	<i>/j</i>	DBCopY priority control

Linux DBCopy	Windows DBCopy	Explanation
-t	/t	Number of threads
-v	/v	Verbose logging
-w	/w	Continuous logging to the screen

-b

Indicates that DBCopy is copying a document storage area, which includes BLOB (binary large object) files. Use this switch only when you need to copy BLOB files.

-i

Specifies the date of the previous copy of the data. This causes DBCopy to copy only files that have been modified since the previous copy, like an incremental backup. There is no default date; you must specify a date.

	Linux DBCopy	Windows DBCopy
Syntax:	-i <i>mm-dd-yyyy</i>	/i <i>mm-dd-yyyy</i>
Example:	-i 5-18-2012	/i 10-30-2012

-j

Raises the priority of DBCopy processing. By default, if DBCopy detects that a POA is running, it lowers its own priority so that it does not interfere with POA processing. If DBCopy runs at night, when GroupWise users are not active, use the -j switch so that DBCopy does not lower its own priority. This speeds up DBCopy processing.

-t

Specifies the number of threads that you want DBCopy to start for copying data. The default number of threads is 5. Valid values range from 1 to 10.

	Linux DBCopy	Windows DBCopy
Syntax:	-t <i>number</i>	/t <i>number</i>
Example:	-t 10	/t 10

-v

Specifies verbose logging, which provides more detail than the default of normal logging. DBCopy creates a log file named *mmddgwbk.nnn*. The first four characters represent the date. A three-digit extension allows for multiple log files created on the same day. The log file is created at the root of the destination directory. By default, DBCopy provides a normal level of logging.

-W

Turns on continuous logging to the screen.

IX Post Office Agent

- ♦ Chapter 35, “Understanding Message Delivery and Storage in the Post Office,” on page 471
- ♦ Chapter 36, “Configuring the POA,” on page 481
- ♦ Chapter 37, “Monitoring the POA,” on page 525
- ♦ Chapter 38, “Optimizing the POA,” on page 559
- ♦ Chapter 39, “Managing Indexing of Attachment Content,” on page 573
- ♦ Chapter 40, “Using POA Startup Switches,” on page 581

For a complete list of port numbers used by the POA, see [Section A.3, “Post Office Agent Port Numbers,”](#) on page 1167.

For detailed Linux-specific POA information, see [Appendix C, “Linux Commands, Directories, and Files for GroupWise Administration,”](#) on page 1179.

For additional assistance in managing the POA, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

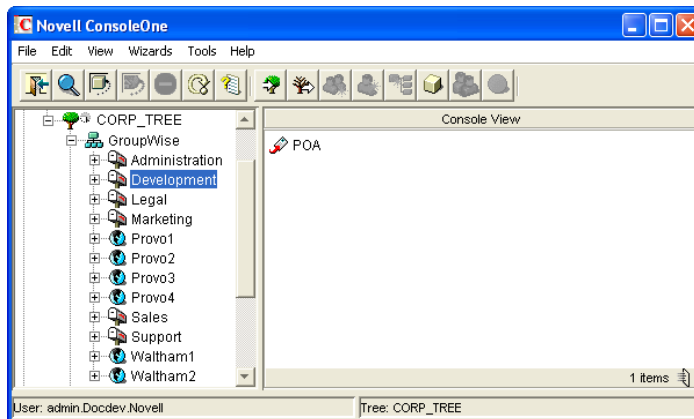
35 Understanding Message Delivery and Storage in the Post Office

A post office is a collection of user mailboxes and GroupWise objects. Messages are delivered into mailboxes by the Post Office Agent (POA). The following topics help you understand the post office and the functions of the POA:

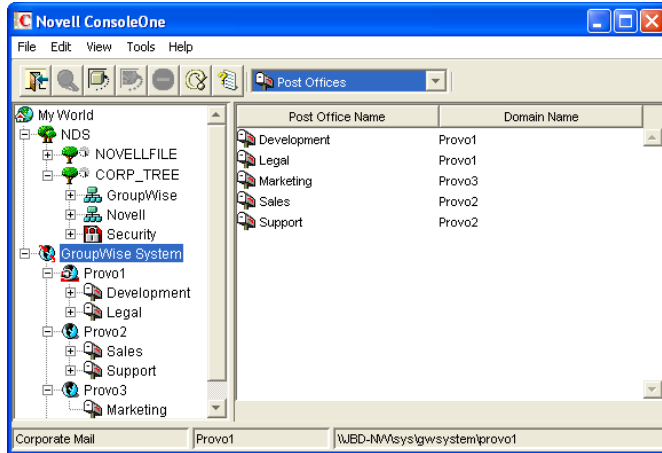
- ◆ [Section 35.1, “Post Office Representation in ConsoleOne,” on page 471](#)
- ◆ [Section 35.2, “Post Office Directory Structure,” on page 472](#)
- ◆ [Section 35.3, “Information Stored in the Post Office,” on page 472](#)
- ◆ [Section 35.4, “Post Office Access Mode,” on page 476](#)
- ◆ [Section 35.5, “Role of the Post Office Agent,” on page 477](#)
- ◆ [Section 35.6, “Message Flow in the Post Office,” on page 479](#)

35.1 Post Office Representation in ConsoleOne

In ConsoleOne, post offices are container objects that contain at least one POA object, as shown below:



Although each post office is linked to a domain, it does not display as subordinate to the domain in the Console View. However, using the GroupWise View, you can display post offices as subordinate to the domains to which they are linked in your GroupWise system.



35.2 Post Office Directory Structure

Physically, a post office consists of a set of directories that house all the information stored in the post office. See “[Post Office Directory](#)” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

35.3 Information Stored in the Post Office

The following types of information are stored in the post office:

- ◆ [Section 35.3.1, “Post Office Database,”](#) on page 472
- ◆ [Section 35.3.2, “Message Store,”](#) on page 473
- ◆ [Section 35.3.3, “Guardian Database,”](#) on page 474
- ◆ [Section 35.3.4, “Agent Input/Output Queues in the Post Office,”](#) on page 475
- ◆ [Section 35.3.5, “Libraries \(optional\),”](#) on page 476

All databases in the post office should be backed up regularly. How often you back up GroupWise databases depends on the reliability of your network and hardware. See [Section 31.2, “Backing Up a Post Office,”](#) on page 431.

35.3.1 Post Office Database

The post office database (`wphost.db`) contains all administrative information for the post office, including a copy of the GroupWise Address Book. This information is necessary for users to send messages to others in the GroupWise system.

35.3.2 Message Store

GroupWise messages are made up of three parts:

- ♦ **Message Header:** The message header contains addressing information including the sender's address, recipient's address, message priority, status level, and a pointer that links the header to the message body.
- ♦ **Message Body:** The message body contains the message text in an encrypted format and a distribution list containing user IDs of the sender and recipients.
- ♦ **File Attachments (optional):** File attachments can be any type of file that is attached to the message.

The message store consists of directories and databases that hold messages. The message store is shared by all members of the post office so only one copy of a message and its attachments is stored in the post office, no matter how many members of the post office receive the message. This makes the system more efficient in terms of message processing, speed, and storage space.

All information in the message store is encrypted to prevent unauthorized access.

The message store contains the following components:

- ♦ ["User Databases" on page 473](#)
- ♦ ["Message Databases" on page 474](#)
- ♦ ["Attachments Directory" on page 474](#)

User Databases

Each member of the post office has a personal database ([userxxx.db](#)) which represents the user's mailbox. The user database contains the following:

- ♦ Message header information
- ♦ Pointers to messages
- ♦ Folder assignments
- ♦ Personal groups
- ♦ Personal address books
- ♦ Rules
- ♦ Contacts
- ♦ Checklists
- ♦ Categories
- ♦ Junk Mail lists

When a member of another post office shares a folder with one or more members of the local post office, a "prime user" database ([puxxxxx.db](#)) is created to store the shared information. The "prime user" is the owner of the shared information.

Local user databases and prime user databases are stored in the [ofuser](#) directory in the post office.

Message Databases

Each member of the post office is arbitrarily assigned to a message database (`msgnnn.db`) where the body portions of messages are stored. Many users in a post office share a single message database. There can be as many as 255 message databases (numbered 0 through 254) in a post office. Message databases are stored in the `ofmsg` directory in the post office.

Historical Note: Prior to GroupWise 7, the POA created a maximum of 25 message databases per post office. The current maximum of 255 message databases speeds up message delivery and minimizes user impact if a database is damaged.

Outgoing messages from local senders are stored in the message database assigned to each sender. Incoming messages from users in other post offices are stored in the message database that corresponds to the message database assigned to the sender in his or her own post office. In each case, only one copy of the message is stored in the post office, no matter how many members of the post office it is addressed to.

Attachments Directory

The attachments directory (`offiles`) contains subdirectories that store file attachments, message text, and distribution lists that exceed 2 KB. Items of this size are stored more efficiently as files than as database records. The message database contains a pointer to where each item is found.

35.3.3 Guardian Database

The guardian database (`ngwguard.db`) serves as the master copy of the data dictionary information for the following subordinate databases in the post office:

- ♦ User databases (`userxxx.db`)
- ♦ Message databases (`msgnnn.db`)
- ♦ Prime user databases (`puxxxxx.db`)
- ♦ Library databases (`dmsh.db` and `dmxxnn01-FF.db`)

The guardian database is vital to GroupWise functioning. Therefore, the POA has an automated fall-back and roll-forward process to protect it. The POA keeps a known good copy of the guardian database called `ngwguard.fbk`. Whenever it modifies the `ngwguard.db` file, the POA also records the transaction in the roll-forward transaction log called `ngwguard.rfl`. If the POA detects damage to the `ngwguard.db` file on startup or during a write transaction, it goes back to the `ngwguard.fbk` file (the “fall back” copy) and applies the transactions recorded in the `ngwguard.rfl` file to create a new, valid and up-to-date `ngwguard.db`.

In addition to the POA fall-back and roll-forward process, you should still back up the `ngwguard.db`, `ngwguard.fbk`, and `ngwguard.rfl` files regularly to protect against media failure. Without a valid `ngwguard.db` file, you cannot access your email. With current `ngwguard.fbk` and `ngwguard.rfl` files, a valid `ngwguard.db` file can be rebuilt should the need arise.

The `ngwguard.dc` file is the structural template for building the guardian database and its subordinate databases. Also called a dictionary file, the `ngwguard.dc` file contains schema information, such as data types and record indexes. If this dictionary file is missing, no additional databases can be created in the post office.

35.3.4 Agent Input/Output Queues in the Post Office

Each post office contains agent input/output queues where messages are deposited and picked up for processing by the POA and the MTA. The MTA transfers messages into and out of the post office, while the POA handles message delivery.

For illustrations of the processes presented below, see [“Message Delivery to a Different Post Office”](#) and [“Message Delivery to a Different Domain”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

MTA Output Queue in the Post Office

The MTA output queue in each post office is the `post_office\wpcout` directory.

If the MTA has a mapped or UNC link to the post office, the MTA writes user messages directly into its output queue, which requires write access to the post office. If the MTA has a TCP/IP link to the post office, the MTA transfers user messages to the POA by way of TCP/IP. The POA then stores the messages in the MTA output queue on behalf of the MTA, so the MTA does not need write access to the post office.

The `post_office\wpcout\ofs` subdirectory is where the MTA transfers user messages for delivery by the POA to users' mailboxes in the local post office.

The MTA `post_office\wpcout\ads` subdirectory is where the MTA transfers administrative messages instructing the POA admin thread to update the post office database (`wphost.db`).

POA Input Queue in the Post Office

The POA input queue in each post office is the `post_office\wpcout` directory, which is the same as the MTA output queue.

The `post_office\wpcout\ofs` subdirectory is where the POA picks up user messages deposited there by the MTA and updates the local message store, so users receive their messages.

The `post_office\wpcout\ads` subdirectory is where the POA admin thread picks up administrative messages deposited there by the MTA and updates the post office database (`wphost.db`).

POA Output Queue in the Post Office

The POA output queue (`post_office\wpcsin`) is where the POA deposits user messages for the MTA to transfer to other domains and post offices.

Historical Note: In earlier versions of GroupWise, the GroupWise client wrote user messages to the POA output queue when using direct access to the post office. In GroupWise 6.x and later, client/server access to the post office is the preferred method.

MTA Input Queue in the Post Office

The MTA input queue in each post office (`post_office\wpcsin`) is the same as the POA output queue. The MTA picks up user messages deposited there by the POA and transfers them to other domains and post offices.

For a mapped or UNC link between the domain and post office, the MTA requires read/write access rights to its input/output queues in the post office. For a TCP/IP link, no access rights are required because messages are communicated to the MTA by way of TCP/IP.

35.3.5 Libraries (optional)

A library is a collection of documents and document properties stored in a database system that can be managed and searched. You do not need to set up libraries unless you are using GroupWise Document Management Services (DMS). See [Part VII, “Libraries and Documents,” on page 313](#).

Library Databases

The databases for managing libraries are stored in the `gwdms` directory and its subdirectories in the post office.

The `dmsh.db` file is a database shared by all libraries in the post office. It contains information about where each library in the post office is located.

Each library has its own subdirectory in the `gwdms` directory. In each library directory, the `dmxxnn01-FF.db` files contain information specific to that library, such as document properties and what users have rights to access the library.

Document Storage Areas

The actual documents in a library are not kept in the library databases. They are kept in a document storage area, which consists of a series of directories for storing document files. Documents are encrypted and stored in BLOBs (binary large objects) to make document management easier. A document, its versions, and related objects are stored together in the same BLOB.

A document storage area might be located in the post office directory structure, or in some other location where more storage space is available. If it is located in the post office, the document storage area can never be moved. Therefore, storing documents in the post office directory structure is not usually recommended. If it is stored outside the post office, a document storage area can be moved when additional disk space is required.

35.4 Post Office Access Mode

The GroupWise 6.x and later Windows client uses client/server access mode to the post office. This requires a TCP/IP connection between the GroupWise clients and the POA in order for users to access their mailboxes. Benefits of client/server access include:

- ♦ **Load Balancing:** The workload is split between the client workstation and the POA on another server. The POA can perform a processor-intensive request while the client is doing something else.
- ♦ **Database Integrity:** The GroupWise client does not need write access to databases in the post office. Therefore, client failures cannot damage databases.
- ♦ **Reduced Network Traffic:** Requests are processed on the POA server and only the results are sent back across the network to the client workstation.
- ♦ **Tighter Security:** Client users do not need to log in to the server where the post office is located. This eliminates the need for users to have write access to the post office directory.
- ♦ **Scalability:** More concurrent users can be supported in a single post office.
- ♦ **Platform Independence:** The GroupWise client on any platform can access the post office by way of TCP/IP communication with the POA.
- ♦ **Simplified Client Connections:** The GroupWise client can communicate with any POA in the GroupWise system. Any POA can then redirect the client to connect to the correct POA for the users' post office.

Historical Note: In GroupWise 5.x, the GroupWise client allowed the user to enter a path to the post office directory to facilitate direct access mode. The GroupWise 6.x and later clients no longer offer that option. However, you can force the GroupWise 6.x and later client to use direct access by starting it with the --ph switch and providing the path to the post office directory.

35.5 Role of the Post Office Agent

The GroupWise Post Office Agent (POA) delivers messages to users' mailboxes, connects users to their post offices in client/server access mode, updates post office databases, indexes messages and documents, and performs other post office-related tasks. You must run at least one POA for each post office.

The following sections help you understand the various functions of the POA:

- ♦ [Section 35.5.1, "Client/Server Processing," on page 477](#)
- ♦ [Section 35.5.2, "Message File Processing," on page 478](#)
- ♦ [Section 35.5.3, "Other POA Functions," on page 478](#)

35.5.1 Client/Server Processing

Using client/server access mode, the GroupWise client maintains one or more TCP/IP connections with the POA and does not access the post office directly. Consequently, the performance of the POA in responding to requests from the GroupWise client directly affects the GroupWise client's responsiveness to users. To provide the highest responsiveness to client users, you can configure a POA just to handle client/server processing. See [Section 38.1.3, "Configuring a Dedicated Client/Server POA \(Windows Only\)," on page 562](#).

When using client/server access mode, the GroupWise client can be configured to control how much time it spends actually connected to the POA.

- ♦ In Online mode, the client is continuously connected.
- ♦ In Caching mode, the client connects at regular intervals to check for incoming messages and also whenever the client user sends a message. Address lookup is performed locally. Caching mode allows the POA to service a much higher number of users than Online Mode.
- ♦ In Remote mode, the client connects whenever the client user chooses, such as when using a brief modem connection to download and upload messages.

For more information about the client modes available with client/server access mode, see ["Using Caching Mode"](#) and ["Using Remote Mode"](#) in the *GroupWise 2012 Windows Client User Guide*

Client/server access mode also allows users to access their GroupWise mailboxes from POP and IMAP clients, in addition to the GroupWise client. See [Section 36.2.3, "Supporting IMAP Clients," on page 498](#).

In client/server mode, the POA is enabled for secure SSL connections by default. If necessary, you can configure the POA to force SSL connections with all clients. See [Section 36.3.3, "Securing the Post Office with SSL Connections to the POA," on page 508](#).

35.5.2 Message File Processing

Messages from users in other post offices arrive in the local post office in the form of message files deposited in the POA input queue. See [Section 35.3.4, “Agent Input/Output Queues in the Post Office,”](#) on page 475.

The POA picks up the message files and updates all user and message databases to deliver incoming messages in the local post office. To provide timely delivery for a large volume of incoming messages, you can configure a POA just to handle message file processing. See [Section 38.2.2, “Configuring a Dedicated Message File Processing POA \(Windows Only\),”](#) on page 565.

35.5.3 Other POA Functions

In addition to client/server processing (interacting with client users) and message file processing (delivering messages), the POA:

- ♦ Performs indexing tasks for document management.
See [Section 39.1, “Regulating Indexing,”](#) on page 573.
- ♦ Performs scheduled maintenance on databases in the post office.
See [Section 36.4.1, “Scheduling Database Maintenance,”](#) on page 517.
- ♦ Monitors and manages disk space usage in the post office.
See [Section 36.4.2, “Scheduling Disk Space Management,”](#) on page 520.
- ♦ Restricts the size of messages that users can send outside the post office.
See [Section 36.2.7, “Restricting Message Size between Post Offices,”](#) on page 504.
- ♦ Primes users’ mailboxes for Caching mode.
See [Section 36.2.6, “Supporting Forced Mailbox Caching,”](#) on page 503.
- ♦ Performs nightly user upkeep so users do not need to wait while the GroupWise client performs it; also creates a downloadable version of the GroupWise Address Book for Remote and Caching users.
See [Section 36.4.3, “Performing Nightly User Upkeep,”](#) on page 523.
- ♦ Provides LDAP authentication and LDAP server pooling.
See [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,”](#) on page 510.
- ♦ Prevents unauthorized access to the post office.
See [Section 36.3.5, “Enabling Intruder Detection,”](#) on page 516.
- ♦ Tracks the GroupWise client software in use in the post office.
See [Section 36.2.5, “Checking What GroupWise Clients Are in Use,”](#) on page 502.
- ♦ Automatically detects and repairs invalid information in user databases (`userxxx.db`) and message databases (`msgnnn.db`) for the local post office by using an efficient multi-threaded process.
See [Section 38.4.1, “Adjusting the Number of POA Threads for Database Maintenance,”](#) on page 567.
- ♦ Automatically detects and repairs invalid information in the post office database (`wphost.db`).
- ♦ Automatically detects and repairs damage to the guardian database (`ngwguard.db`) in the post office.
- ♦ Updates the post office database whenever GroupWise users, resources, post offices, or other GroupWise objects are added, modified, or deleted.

- ♦ Replicates shared folders between post offices.
- ♦ Executes GroupWise client rules.
- ♦ Processes requests from GroupWise Remote users.

35.6 Message Flow in the Post Office

To see how messages are delivered using client/server access mode, see [“Message Delivery in the Local Post Office”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

36 Configuring the POA

For POA system requirements, see “[Agent System Requirements](#)” in the *GroupWise 2012 Installation Guide*. For detailed instructions about installing and starting the POA for the first time, see “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.

As your GroupWise system grows and evolves, you might need to modify POA configuration to meet the changing needs of the post office it services. The following topics help you configure the POA:

- ◆ [Section 36.1, “Performing Basic POA Configuration,” on page 482](#)
 - [Creating a POA Object in eDirectory](#)
 - [Configuring the POA in ConsoleOne](#)
 - [Changing the Link Protocol between the Post Office and the Domain](#)
 - [Binding the POA to a Specific IP Address](#)
 - [Moving the POA to a Different Server](#)
 - [Adjusting the POA for a New Post Office Location](#)
 - [Configuring the POA for Remote Server Login \(Windows Only\)](#)
 - [Adjusting the POA Logging Level and Other Log Settings](#)
- ◆ [Section 36.2, “Configuring User Access to the Post Office,” on page 494](#)
 - [Using Client/Server Access to the Post Office](#)
 - [Simplifying Client/Server Access with a GroupWise Name Server](#)
 - [Supporting IMAP Clients](#)
 - [Supporting SOAP Clients](#)
 - [Checking What GroupWise Clients Are in Use](#)
 - [Supporting Forced Mailbox Caching](#)
 - [Restricting Message Size between Post Offices](#)
- ◆ [Section 36.3, “Configuring Post Office Security,” on page 505](#)
 - [Securing Client/Server Access through an External Proxy Server](#)
 - [Controlling Client Redirection Inside and Outside Your Firewall](#)
 - [Securing the Post Office with SSL Connections to the POA](#)
 - [Providing LDAP Authentication for GroupWise Users](#)
 - [Enabling Intruder Detection](#)
 - [Configuring Trusted Application Support](#)
- ◆ [Section 36.4, “Configuring Post Office Maintenance,” on page 517](#)
 - [Scheduling Database Maintenance](#)
 - [Scheduling Disk Space Management](#)
 - [Performing Nightly User Upkeep](#)

36.1 Performing Basic POA Configuration

POA configuration information is stored as properties of its POA object in eDirectory. The following topics help you modify the POA object in ConsoleOne and change POA configuration to meet changing system configurations:

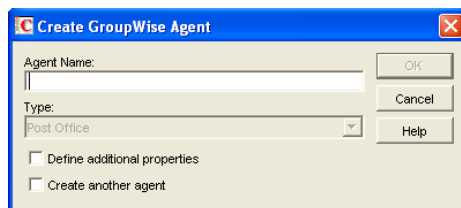
- ♦ [Section 36.1.1, “Creating a POA Object in eDirectory,” on page 482](#)
- ♦ [Section 36.1.2, “Configuring the POA in ConsoleOne,” on page 484](#)
- ♦ [Section 36.1.3, “Changing the Link Protocol between the Post Office and the Domain,” on page 487](#)
- ♦ [Section 36.1.4, “Binding the POA to a Specific IP Address,” on page 490](#)
- ♦ [Section 36.1.5, “Moving the POA to a Different Server,” on page 490](#)
- ♦ [Section 36.1.6, “Adjusting the POA for a New Post Office Location,” on page 491](#)
- ♦ [Section 36.1.7, “Configuring the POA for Remote Server Login \(Windows Only\),” on page 492](#)
- ♦ [Section 36.1.8, “Adjusting the POA Logging Level and Other Log Settings,” on page 493](#)

36.1.1 Creating a POA Object in eDirectory

When you create a new post office, one POA object is automatically created for it. You can set up additional POAs for an existing post office if message traffic in the post office is heavy. To accomplish this, you must also create additional POA objects.

To create a new POA object in Novell eDirectory:

- 1 In ConsoleOne, browse to and right-click the Post Office object for which you want to create a new POA object, then click *New > Object*.
- 2 Double-click *GroupWise Agent* to display the Create GroupWise Agent dialog box.



- 3 Type a unique name for the new POA. The name can include as many as 8 characters. Do not use any of the following invalid characters in the name:

ASCII characters 0-31	Comma ,
Asterisk *	Double quote "
At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

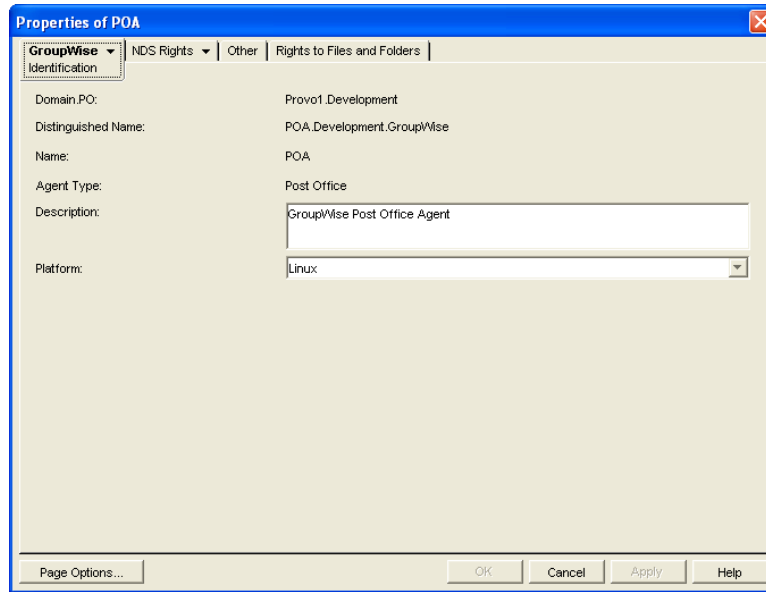
You use this name with the `--name` startup switch when you start the new POA.

The *Type* field is automatically set to Post Office.

- 4 Select *Define Additional Properties*.
- 5 Click *OK*.

The POA object is automatically placed within the Post Office object.

- 6 Review the information displayed for the first four fields on the Identification page to ensure that you are creating the correct type of Agent object in the correct location.



- 7 In the *Description* field, type one or more lines of text describing the POA.

This description displays on the POA server console as the POA runs. When you run multiple POAs on the same server, the description should uniquely identify each one. If multiple administrators work at the server where the POA runs, the description could include a note about who to contact before stopping the POA.

- 8 In the *Platform* field, select the platform (Linux or Windows) where the POA will run.
- 9 Click *OK* to save the updated properties.
- 10 (Conditional) If you plan to set up the additional POA on the same server with the original POA:
 - 10a Assign it a unique port number on the Network Address properties page of the new POA object.
 - 10b Create a copy of the POA startup file associated with the original POA for use with the additional POA.
 - 10c Set up whatever mechanism you use for starting the original POA for use with the additional POA.

For example, if you want to use the `rcgrpwise` script on Linux to start the additional POA, you must add a section in the `gwha.conf` file for it. For more information, see [“Configuring the GroupWise High Availability Service in the gwha.conf File”](#) in *“Installing GroupWise Agents”* in the *GroupWise 2012 Installation Guide*.

If you plan to install the additional POA on a different server, the installation process takes care of these issues for you.

- 11 Continue with [Section 36.1.2, “Configuring the POA in ConsoleOne,”](#) on page 484.

36.1.2 Configuring the POA in ConsoleOne

The advantage to configuring the POA in ConsoleOne, as opposed to using startup switches in a POA startup file, is that the POA configuration settings are stored in eDirectory.

- 1 In ConsoleOne, expand the eDirectory container where the Post Office object is located.
- 2 Expand the Post Office object.
- 3 Right-click the POA object, then click *Properties*.

The table below summarizes the POA configuration settings in the POA object properties pages and how they correspond to POA startup switches (as described in [Chapter 40, "Using POA Startup Switches," on page 581](#)). The table also includes settings on the Post Office object that correspond to POA startup switches.

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
POA Identification Page	
Domain.PO	See Section 36.1.1, "Creating a POA Object in eDirectory," on page 482 .
Distinguished Name	
Name	
Agent Type	
Description	
Platform	
POA Agent Settings Page	
Message File Processing	See Section 38.2.2, "Configuring a Dedicated Message File Processing POA (Windows Only)," on page 565 . See also <code>--nomf</code> , <code>--nomfhigh</code> , and <code>--nomflow</code> .
Message Handler Threads	See Section 38.2.1, "Adjusting the Number of POA Threads for Message File Processing," on page 564 . See also <code>--threads</code> .
Enable Client/Server	See Section 36.2.1, "Using Client/Server Access to the Post Office," on page 494 and Section 38.1.3, "Configuring a Dedicated Client/Server POA (Windows Only)," on page 562 . See also <code>--notcpip</code> .
Client/Server Handler Threads	See Section 38.1.2, "Adjusting the Number of Connections for Client/Server Processing," on page 561 . See also <code>--tcpthreads</code> .
Max Physical Connections Max Application Connections	See Section 38.1.2, "Adjusting the Number of Connections for Client/Server Processing," on page 561 . See also <code>--maxphysconns</code> and <code>--maxappconns</code> .
Enable Caching	See <code>--nocache</code> .
Max Thread Usage for Priming and Moves	See Section 36.2.6, "Supporting Forced Mailbox Caching," on page 503 . See also <code>--primingmax</code> .

ConsoleOne Properties Pages and Settings **Corresponding Tasks and Startup Switches**

Enable IMAP	See Section 36.2.3, "Supporting IMAP Clients," on page 498.
Max IMAP Threads	See also <code>--imap</code> , <code>--imapmaxthreads</code> , <code>--imapport</code> , <code>--imapreadlimit</code> , <code>--imapreadnew</code> , <code>--imapssl</code> , and <code>--imapsslport</code> .
Enable SOAP	See Section 36.2.4, "Supporting SOAP Clients," on page 499.
Max SOAP Threads	See also <code>--soap</code> and <code>--soapmaxthreads</code> .
Enable SNMP	See Section 37.6, "Using an SNMP Management Console," on page 553.
SNMP Community "Get" String	See also <code>--nosnmp</code> .
Disable Administration Task Processing	See <code>--noada</code> .
HTTP User Name	See Section 37.2.1, "Setting Up the POA Web Console," on page 540.
HTTP Password	See also <code>--httpuser</code> and <code>--httppassword</code> .

Network Address Page

TCP/IP Address	See Section 36.2.1, "Using Client/Server Access to the Post Office," on page 494 and "Using TCP/IP Links between the Post Office and the Domain" on page 487. See also <code>--ip</code> .
External IP Address	See Section 36.3.1, "Securing Client/Server Access through an External Proxy Server," on page 506.
Bind Exclusively to TCP/IP Address	See Section 36.1.4, "Binding the POA to a Specific IP Address," on page 490 See also <code>--ip</code> .
Message Transfer	See "Using TCP/IP Links between the Post Office and the Domain" on page 487. See also <code>--mtpinipaddr</code> , <code>--mtpinport</code> , <code>--mtpoutipaddr</code> , <code>--mtpoutport</code> , <code>--mtpsendmax</code> , and <code>--mtpssl</code> .
HTTP	See Section 37.2.1, "Setting Up the POA Web Console," on page 540. See also <code>--httpport</code> and <code>--https</code> .
Internal Client/Server External Client/Server	See Section 36.2.1, "Using Client/Server Access to the Post Office," on page 494 and "Using TCP/IP Links between the Post Office and the Domain" on page 487. See also <code>--port</code> , <code>--internalclientssl</code> , and <code>--externalclientssl</code> .

IMPORTANT: Until you configure the POA external client/server connections for SSL, you receive the following message whenever you modify any POA property settings:

```
SSL will not be used for Internet Client/Server connections until a proxy server has been specified. Would you like to enter one now?
```

To eliminate the message, follow the instructions in:

- ◆ [Section 36.3.1, "Securing Client/Server Access through an External Proxy Server,"](#) on page 506
 - ◆ [Section 36.3.3, "Securing the Post Office with SSL Connections to the POA,"](#) on page 508
-

ConsoleOne Properties Pages and Settings	Corresponding Tasks and Startup Switches
IMAP	See Section 36.2.3, “Supporting IMAP Clients,” on page 498. See also <code>--imapport</code> , <code>--imapssl</code> , and <code>--imapsslport</code> .
SOAP	See Section 36.2.4, “Supporting SOAP Clients,” on page 499. See also <code>--soapport</code> and <code>--soapssl</code> .
QuickFinder Page	
Enable QuickFinder Indexing	See Section 39.1, “Regulating Indexing,” on page 573 and Section 39.5, “Configuring a Dedicated Indexing POA (Windows Only),” on page 577.
Start QuickFinder Indexing	
QuickFinder Interval	See also <code>--qfbaseoffset</code> , <code>--qfbaseoffsetinminute</code> , <code>--qfinterval</code> ,
Quarantine Files That Fail during Conversion	<code>--qfintervalinminute</code> , and <code>--noqf</code> .
Maintenance Page	
Enable Auto DB Recovery	See <code>--norecover</code> .
Maintenance Handler Threads	See Section 38.4.1, “Adjusting the Number of POA Threads for Database Maintenance,” on page 567. See also <code>--gwchkthreads</code> and <code>--nogwchk</code> .
Perform User Upkeep	See Section 36.4.3, “Performing Nightly User Upkeep,” on page 523.
Start User Upkeep	See also <code>--nuuoffset</code> , <code>--nonuu</code> , <code>--rdaboffset</code> , and <code>--nordab</code> .
Generate Address Book for Remote	
Start Address Book Generation	
Disk Check Interval	See Section 36.4.2, “Scheduling Disk Space Management,” on page 520.
Disk Check Delay	
POA Log Settings Page	
Log File Path	See Section 37.3, “Using POA Log Files,” on page 551.
Logging Level	See also <code>--log</code> , <code>--logdays</code> , <code>--logdiskoff</code> , <code>--loglevel</code> , and <code>--logmax</code> .
Max Log File Age	
Max Log Disk Space	
POA Scheduled Events Page	
Disk Check Event	See Section 36.4.2, “Scheduling Disk Space Management,” on page 520.
Mailbox/Library Maintenance Event	See Section 36.4.1, “Scheduling Database Maintenance,” on page 517.
POA SSL Settings Page	
Certificate File	See Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,” on page 508.
SSL Key File	
Password	See also <code>--certfile</code> , <code>--keyfile</code> , <code>--keypassword</code> .
Post Office Settings Page	
Remote User Name	See <code>--user</code> and <code>--password</code> .
Remote Password	

ConsoleOne Properties Pages and Settings **Corresponding Tasks and Startup Switches**

Post Office Client Access Settings Page

Lock Out Older GroupWise Clients	See Section 36.2.5, “Checking What GroupWise Clients Are in Use,” on page 502.
Minimum Client Release Version Minimum Client Release Date	See also <code>--gwclientreleasedate</code> , <code>--gwclientreleaseversion</code> , and <code>--enforcedclientversion</code> .
Enable Intruder Detection	See Section 36.3.5, “Enabling Intruder Detection,” on page 516.
Incorrect Logins Allowed Incorrect Login Reset Time Lockout Reset Time	See also <code>--intruderlockout</code> , <code>--incorrectloginattempts</code> , <code>--attemptsresetinterval</code> , and <code>--lockoutresetinterval</code> .

Post Office Security Page

LDAP Authentication	See Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510. See also <code>--ldapipaddr</code> , <code>--ldapport</code> , <code>--ldapuser</code> , <code>--ldappwd</code> , <code>--ldapuserauthmethod</code> , <code>--ldapdisablepwdchg</code> , <code>--ldapssl</code> , <code>--ldapsslkey</code> , and <code>--ldapstimeout</code> . See also <code>--ldapippooln</code> , <code>--ldappoolresettime</code> , <code>--ldapportpooln</code> , <code>--ldapsslpooln</code> , and <code>--ldapsslkeypooln</code> .
---------------------	---

After you install the POA software, you can further configure the POA using a startup file. See [Chapter 40, “Using POA Startup Switches,”](#) on page 581 to survey the many ways the POA can be configured.

36.1.3 Changing the Link Protocol between the Post Office and the Domain

How messages are transferred between the POA and the MTA is determined by the link protocol in use between the post office and the domain. For a review of link protocols, see [Section 10.1.3, “Link Protocols for Direct Links,”](#) on page 159.

If you need to change from one link protocol to another, some reconfiguration of the POA and its link to the domain is necessary.

- ♦ [“Using TCP/IP Links between the Post Office and the Domain”](#) on page 487
- ♦ [“Using Mapped or UNC Links between the Post Office and the Domain”](#) on page 489

NOTE: The Linux POA requires TCP/IP links between the post office and the domain.

Using TCP/IP Links between the Post Office and the Domain

To change from a mapped or UNC link to a TCP/IP link between a post office and its domain, you must perform the following two tasks:

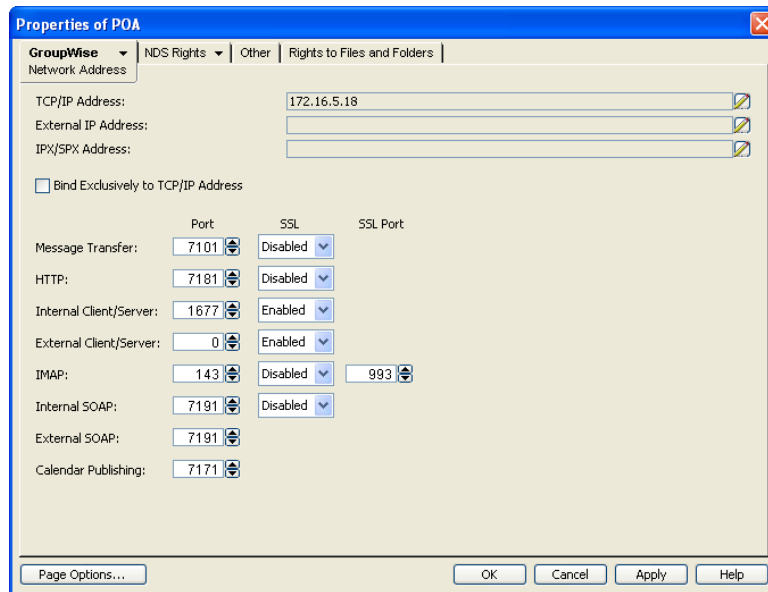
- ♦ [“Configuring the Agents for TCP/IP”](#) on page 488
- ♦ [“Changing the Link between the Post Office and the Domain to TCP/IP”](#) on page 488

Configuring the Agents for TCP/IP

- 1 If the MTA in the domain is not yet set up for TCP/IP communication, follow the instructions in [“Configuring the MTA for TCP/IP”](#) on page 632.
- 2 To make sure the POA is properly set up for TCP/IP communication, follow the instructions in [Section 36.2.1, “Using Client/Server Access to the Post Office,”](#) on page 494.

Only one POA per post office needs to communicate with the MTA. If the post office has multiple POAs, have a POA that performs message file processing communicate with the MTA for best performance. For information about message file processing, see [Section 35.5, “Role of the Post Office Agent,”](#) on page 477.

- 3 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 4 Click *GroupWise > Network Address* to display the Network Address page.



- 5 In the *Message Transfer* field, specify the TCP port on which the POA will listen for incoming messages from the MTA.

The default message transfer port for the POA to listen on is 7101.

- 6 Click *OK* to save the TCP/IP information and return to the main ConsoleOne window.

Corresponding Startup Switches: You can also use the `--mtpinipaddr` and `--mtpinport` startup switches in the POA startup file to set the incoming IP address and port.

Changing the Link between the Post Office and the Domain to TCP/IP

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration*.
- 2 In the drop-down list, select the domain where the post office resides.
- 3 Click *Post Office Links*, then double-click the post office for which you want to change the link protocol.

- 4 In the *Protocol* field, select *TCP/IP*.



- 5 Make sure the information displayed in the Edit Post Office Link dialog box matches the information on the Network Address page for the POA.

When you use a TCP/IP link, the *Maximum Send Message Size* field enables you to restrict the size of messages that users can send between post offices, as described in [Section 36.2.7, “Restricting Message Size between Post Offices,”](#) on page 504.

- 6 Click *OK*.
- 7 To exit the Link Configuration tool and save your changes, click *File > Exit > Yes*.

ConsoleOne then notifies the POA and MTA to restart using the new link protocol.

For a sample message flow for this configuration, see “[TCP/IP Link Open: Transfer between Post Offices Successful](#)” in “[Message Delivery to a Different Post Office](#)” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

Corresponding Startup Switches: You can also use the `--mtpoutipaddr` and `--mtpoutport` startup switches in the POA startup file to set the outgoing IP address and port.

Using Mapped or UNC Links between the Post Office and the Domain

To change from a TCP/IP link to a mapped or UNC link between a post office and its domain:

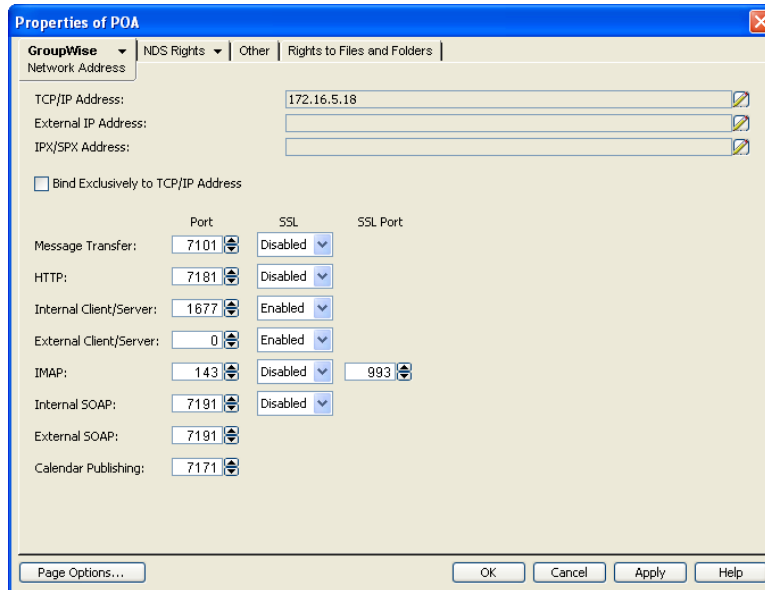
- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration*.
- 2 In the drop-down list, select the domain where the post office resides.
- 3 Click *Post Office Links*, then double-click the post office for which you want to change the link protocol.
- 4 In the *Protocol* field, select *Mapped* or *UNC*.
- 5 Provide the location of the post office in the format appropriate to the selected protocol.
- 6 Click *OK*.
- 7 To exit the Link Configuration tool and save your changes, click *File > Exit > Yes*.

ConsoleOne then notifies the POA and MTA to restart using the new link protocol.

36.1.4 Binding the POA to a Specific IP Address

You can now cause the POA to bind to a specified IP address when the server where it runs uses multiple IP addresses. The specified IP address is associated with all ports used by the agent. Without an exclusive bind, the POA binds to all IP addresses available on the server.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.



- 3 Select *Bind Exclusively to TCP/IP Address*, then click *OK* to save your change.

Corresponding Startup Switches: You can also use the `--ip` and `--mtpoutport` startup switch in the POA startup file to establish an exclusive bind to the specified IP address.

36.1.5 Moving the POA to a Different Server

As your GroupWise system grows and evolves, you might need to move a POA from one server to another. For example, you might decide to run the POA on a different platform, or perhaps you want to move it to a server that has more memory or disk space.

- 1 Reconfigure the POA object with the new IP address and port number for the POA to use on the new server, as described in [Section 36.2.1, "Using Client/Server Access to the Post Office,"](#) on page 494.
- 2 Install the POA on the new server, as described in ["Installing GroupWise Agents"](#) in the [GroupWise 2012 Installation Guide](#).
- 3 Start the new POA, as described in the following sections in the [GroupWise 2012 Installation Guide](#):
 - ◆ ["Starting the Linux Agents with a User Interface"](#)
 - ◆ ["Starting the Windows GroupWise Agents"](#)
- 4 Observe the new POA to see that it is running smoothly, as described in [Chapter 37, "Monitoring the POA,"](#) on page 525.
- 5 Stop the old POA.

- 6 If you are no longer using the old server for any GroupWise agents, you can remove them to reclaim the disk space, as described in the following sections in the [GroupWise 2012 Installation Guide](#):
 - ♦ “Uninstalling the Linux GroupWise Agents”
 - ♦ “Uninstalling the Windows GroupWise Agents”

36.1.6 Adjusting the POA for a New Post Office Location

If you move a post office from one server to another, you also need to edit the POA startup file to provide the new location of the post office directory.

- 1 Stop the POA for the old post office location if it is still running.
- 2 Use an ASCII text editor to edit the POA startup file.

The POA startup file is named after the post office name, plus a `.poa` extension.

Windows: Only the first 8 characters of the post office name are used in the file name. The startup file is typically located in the directory where the POA software is installed.

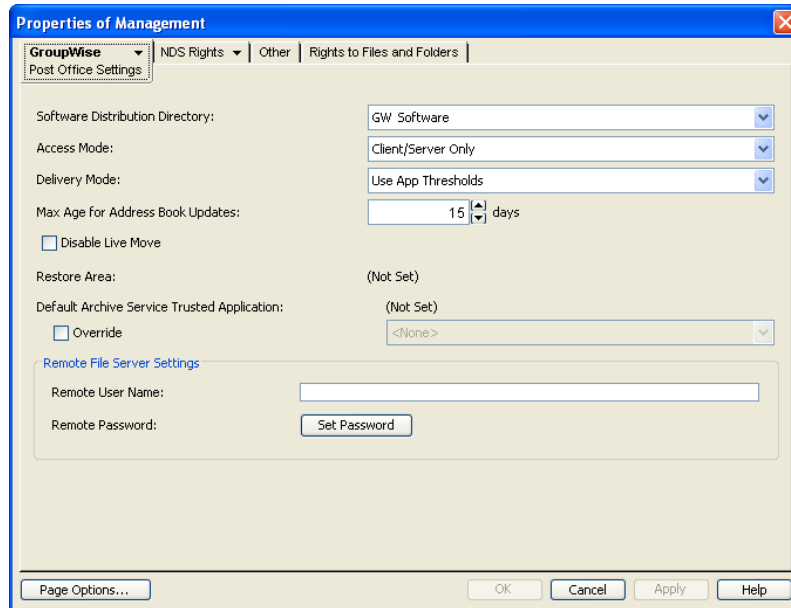
Linux: The full post office name is used in the file name. However, all letters are lowercase and any spaces in the post office name are removed. The startup file is located in the `/opt/novell/groupwise/agents/share` directory.

- 3 Adjust the setting of the `--home` switch to point to the new location of the post office directory.
- 4 Save the POA startup file.
- 5 Start the POA for the new post office location, as described in the following sections in the [GroupWise 2012 Installation Guide](#):
 - ♦ “Starting the Linux Agents with a User Interface”
 - ♦ “Starting the Windows GroupWise Agents”
- 6 Adjust the link between the post office and the domain. See [Section 42.1.7, “Adjusting the MTA for a New Location of a Domain or Post Office,”](#) on page 640.

36.1.7 Configuring the POA for Remote Server Login (Windows Only)

On Windows, you can organize a post office so that some components, such as a library, remote document storage area, restore area, or software distribution directory, are located on a remote Windows server. In order for the POA access the remote Windows server, you must provide a user name and password that provide sufficient access to the remote server for the POA to perform the required task on the remote server.

- 1 In ConsoleOne, browse to and right-click the Post Office object that includes remote components, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Post Office Settings page.

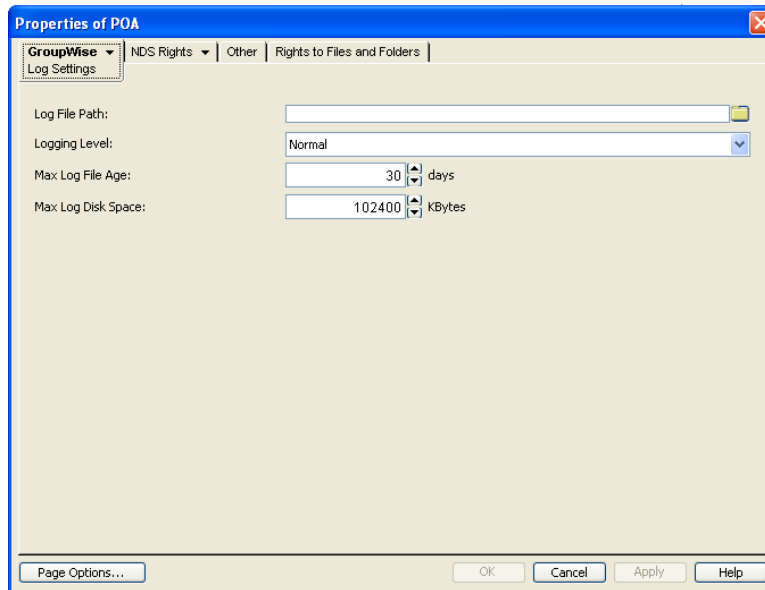


- 3 In the *Remote File Server Settings* box, provide the user name and password that the POA can use to log in to the remote server where post office components are located, then click *OK*.

36.1.8 Adjusting the POA Logging Level and Other Log Settings

When installing or troubleshooting the POA, a logging level of Verbose can be useful. However, when the POA is running smoothly, you can set the logging level down to Normal to conserve disk space occupied by log files.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Log Settings* to display the Log Settings page.



- 3 Set the desired settings for logging.

Log File Path: Browse to and select the directory where you want this POA to store its log files. The default location varies by platform:

Linux: `/var/log/novell/groupwise/post_office.poa`

Windows: `post_office\wpcsout\ofs`

For more information about log settings and log files, see [Section 37.3, “Using POA Log Files,” on page 551](#).

Logging Level: Select the amount of data displayed on the POA agent console and written to the POA log file.

- ◆ **Off:** Turns off disk logging and sets the logging level for the POA to its default. Logging information is still displayed on the POA agent console.
- ◆ **Normal:** Displays only the essential information suitable for a smoothly running POA.
- ◆ **Verbose:** Displays the essential information, plus additional information that can be helpful for troubleshooting.
- ◆ **Diagnostic:** Turns on *Extensive Logging Options* and *SOAP Logging Options* on the POA Web console Log Settings page.

Maximum Log File Age: Specifies how many days to keep POA log files on disk. The default is 30 days.

Maximum Log Disk Space: Sets the maximum amount of disk space for all POA log files. When the specified disk space is consumed, the POA deletes existing log files, starting with the oldest. The default is 102400 KB (100 MB). The maximum allowable setting is 102400000 (1 GB).

Corresponding Startup Switches: You can also use the `--log`, `--loglevel`, `--logdays`, `--logmax`, and `--logdiskoff` switches in the POA startup file to configure logging.

POA Web Console: You can view and search POA log files on the [Log Files](#) page.

36.2 Configuring User Access to the Post Office

As described in [Section 35.4, "Post Office Access Mode,"](#) on page 476, the GroupWise client defaults to client/server access mode. The following topics help you configure the POA to customize the types of client/server access provided to the post office:

- ◆ [Section 36.2.1, "Using Client/Server Access to the Post Office,"](#) on page 494
- ◆ [Section 36.2.2, "Simplifying Client/Server Access with a GroupWise Name Server,"](#) on page 496
- ◆ [Section 36.2.3, "Supporting IMAP Clients,"](#) on page 498
- ◆ [Section 36.2.4, "Supporting SOAP Clients,"](#) on page 499
- ◆ [Section 36.2.5, "Checking What GroupWise Clients Are in Use,"](#) on page 502
- ◆ [Section 36.2.6, "Supporting Forced Mailbox Caching,"](#) on page 503
- ◆ [Section 36.2.7, "Restricting Message Size between Post Offices,"](#) on page 504
- ◆ [Section 36.2.8, "Supporting Calendar Publishing,"](#) on page 505

36.2.1 Using Client/Server Access to the Post Office

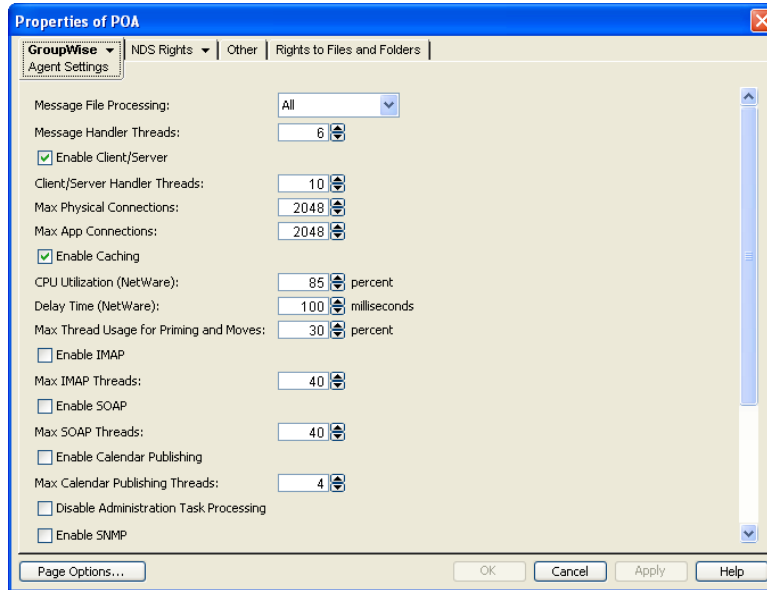
The POA defaults to Client/Server mode, which enables you to:

- ◆ Set up TCP/IP for client/server communication between this POA and the GroupWise client
- ◆ Set up TCP/IP communication between this POA and the MTA for the domain
- ◆ Configure the POA so network management and monitoring programs can use TCP/IP to send SNMP requests to this POA
- ◆ Set up an external server with Internet access for the POA
- ◆ Configure the POA to provide a Web console for use with GroupWise Monitor
- ◆ Configure the POA to communicate with IMAP (Internet Message Application Protocol) clients
- ◆ Configure the POA to communicate with SOAP (Simple Object Access Protocol) clients
- ◆ Configure the POA for calendar publishing so that users' calendars can be viewed on the Internet

To make sure the GroupWise client has proper client/server access to the post office:

- 1 Make sure TCP/IP is properly set up on the server where the POA is running.
- 2 In ConsoleOne, browse to and right-click the POA object, then click Properties.

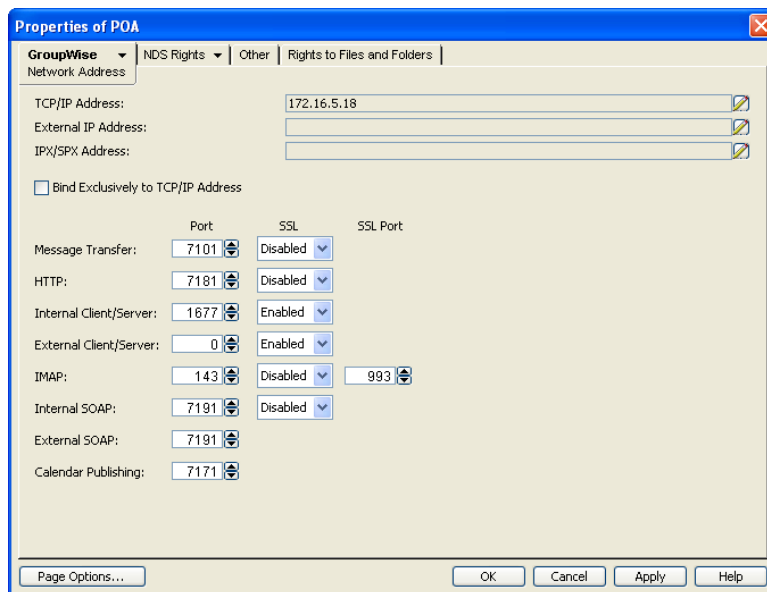
- 3 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 4 Make sure that *Enable Client/Server* is selected.

The default numbers of physical connections and application connections are appropriate for a post office with as many as 500 users. If you are configuring the POA to service more than 500 users, see [Section 38.1.2, "Adjusting the Number of Connections for Client/Server Processing," on page 561](#) for more detailed recommendations. Configuring the POA with insufficient connections can result in error conditions.

- 5 Click *GroupWise > Network Address*.



- 6 On the Network Address page, click the pencil icon for the *TCP/IP Address* field to display the Edit Network Address dialog box.



- 7 Select *IP Address*, then specify the IP address, in dotted decimal format, of the server where the POA is running.

or

Select *DNS Host Name*, then provide the DNS hostname of the server where the POA is running.

IMPORTANT: The POA must run on a server that has a static IP address. DHCP cannot be used to dynamically assign an IP address for it.

Specifying the DNS hostname rather than the IP address makes it easier to move the POA from one server to another, if the need arises at a later time. You can assign a new IP address to the hostname in DNS, without needing to change the POA configuration information in ConsoleOne.

- 8 Click *OK*.
- 9 To use a TCP port number other than the default port of 1677, type the port number in the *Internal Client/Server Port* field.
If multiple POAs will run on the same server, each POA must have a unique TCP port number.
- 10 For optimum security, select *Required* in the *SSL* drop-down list for local intranet client/server connections, Internet client/server connections, or both. For more information, see [Section 36.3.3, "Securing the Post Office with SSL Connections to the POA,"](#) on page 508.
- 11 Click *OK* to save the network address and port information and return to the main ConsoleOne window.

ConsoleOne then notifies the POA to restart with client/server processing enabled.

For a sample message flow for this configuration, see "[Message Delivery in the Local Post Office](#)" in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

Corresponding Startup Switches: You can also use the `--port` switch in the POA startup file to provide the client/server port number. On a server with multiple IP addresses, you can use the `--ip` switch to bind the POA to a specific address.

POA Web Console: You can view the TCP/IP address and port information for the POA on the [Configuration](#) page under the *Client/Server Settings* heading.

36.2.2 Simplifying Client/Server Access with a GroupWise Name Server

If GroupWise users are set up correctly in eDirectory, the GroupWise client can determine which post office to access for each user based on the information stored in eDirectory. This lets the GroupWise client start automatically in client/server mode without users needing to know and provide any IP

address information. However, some GroupWise users might be on platforms where eDirectory is not in use. To fill the same function for non-eDirectory users, you can set up a GroupWise name server.

A GroupWise name server redirects each GroupWise client user to the IP address and port number of the POA that services the user's post office. By setting up a GroupWise name server, non-eDirectory GroupWise client users do not need to know and provide any IP address information when they start the GroupWise client in client/server mode. The GroupWise name server takes care of this for them.

- ♦ [“Required Hostnames” on page 497](#)
- ♦ [“Required Port Number” on page 497](#)
- ♦ [“How a GroupWise Name Server Helps the GroupWise Client Start” on page 497](#)
- ♦ [“Setting Up a GroupWise Name Server” on page 497](#)

Required Hostnames

The primary GroupWise name server must be designated using the hostname `ngwnameserver`. You can also designate a backup GroupWise name server using the hostname `ngwnameserver2`.

Required Port Number

Each server designated as a GroupWise name server must have a POA running on it that uses the default port number of 1677. Other agents can run on the same server, but one POA must use the default port number of 1677 in order for the GroupWise name server to function. For setup instructions, see [Section 36.2.1, “Using Client/Server Access to the Post Office,” on page 494](#).

How a GroupWise Name Server Helps the GroupWise Client Start

After a server has been designated as `ngwnameserver`, and a POA using the default port number of 1677 is running on that server, the GroupWise client can connect to the POA of the appropriate post office by contacting the POA located on `ngwnameserver`. If `ngwnameserver` is not available, the client next attempts to contact the backup name server, `ngwnameserver2`. If no GroupWise name server is available, the user must provide the IP address and port number of the appropriate POA in order to start the GroupWise client in client/server mode.

Setting Up a GroupWise Name Server

- 1 Make sure that TCP/IP is set up and functioning on your network.
- 2 Know the IP address of the server you want to set up as a GroupWise name server.
- 3 Make sure the POA on that server uses the default TCP port of 1677.
- 4 If you want a backup GroupWise name server, identify the IP address of a second server where the POA uses the default TCP port of 1677.
- 5 Use your tool of choice for modifying DNS.

Linux: You can use the YaST Control Center.

Windows: You can use DNS Manager.

- 6 Create an entry for the IP address of the first POA and give it the hostname `ngwnameserver`.
- 7 If you want a backup name server, create an entry for the IP address of the second POA and give it the hostname `ngwnameserver2`.

You must use the hostnames `ngwnameserver` and `ngwnameserver2`. Any other hostnames are not recognized as GroupWise name servers.

- 8 Save your changes.

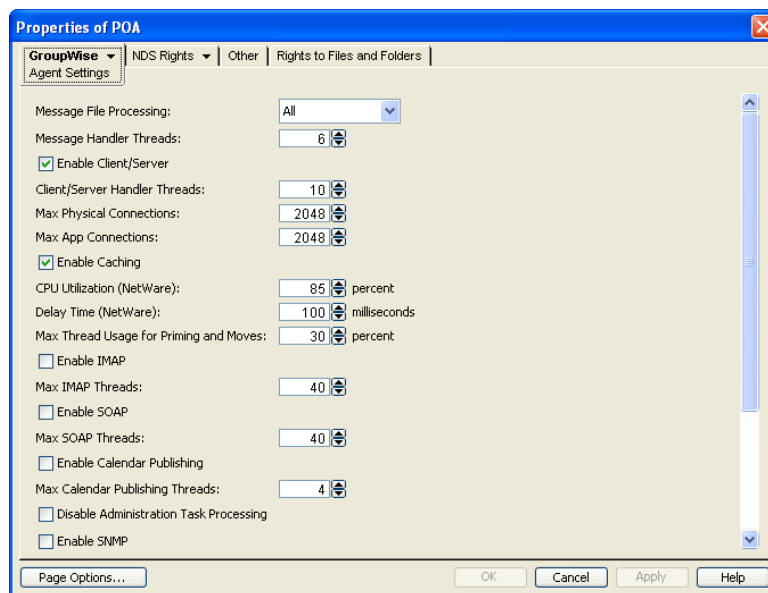
As soon as the hostname information replicates throughout your system, GroupWise client users can start the GroupWise client in client/server mode without specifying a TCP/IP address and port number.

36.2.3 Supporting IMAP Clients

Internet Messaging Application Protocol (IMAP) is used by email clients such as Microsoft Outlook and Evolution. You can configure the POA to communicate with IMAP-enabled email clients much like the GroupWise client does.

NOTE: IMAP clients connecting to your GroupWise system from outside your firewall must connect through the Internet Agent (GWIA), as described in [Section 53.2, “Configuring POP3/IMAP4 Services,” on page 777](#), rather than through the POA. Connecting directly through the POA provides faster access for internal IMAP clients.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 3 Fill in the following fields:

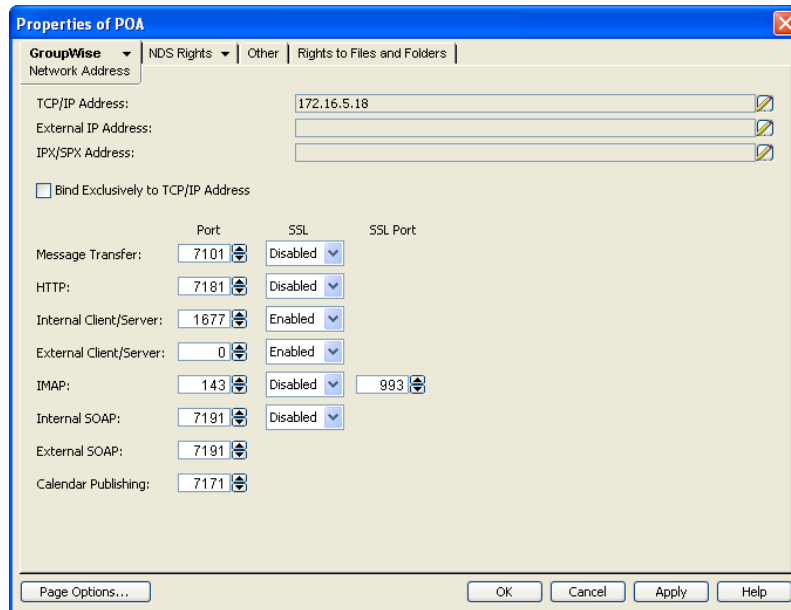
Enable IMAP: Select *Enable IMAP* to turn on IMAP processing.

Max IMAP Threads: Specify the maximum number of IMAP threads you want the POA to start.

The default maximum number of IMAP threads is 40. This is adequate for most post offices, because each IMAP thread can service multiple IMAP clients. By default, the POA creates 2 IMAP threads and automatically creates additional threads as needed to service clients until the maximum number is reached. You cannot set the maximum higher than 40.

You might want to lower the maximum number of IMAP threads if IMAP processing is monopolizing system resources that you prefer to have available for other processes. However, insufficient IMAP threads can cause slow response for IMAP client users.

- 4 Click *Apply* to save the IMAP thread settings.
- 5 To secure IMAP connections to the post office or to change the IMAP port:
 - 5a Click *GroupWise > Network Address*.



- 5b Select *Required* in the *IMAP SSL* drop-down list.
For additional instructions about using SSL connections, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107.
- 5c Change the IMAP port as needed.
- 6 Click *OK* to save the IMAP settings and return to the main ConsoleOne window.
ConsoleOne then notifies the POA to restart with IMAP enabled.

Corresponding Startup Switches: You can also use the `--imap`, `--imapmaxthreads`, `--imapport`, `--imapssl`, and `--imapsslport` startup switches in the POA startup file to configure the POA to support IMAP clients. In addition, you can use the `--imapreadlimit` and `--imapreadnew` startup switches to configure how the POA downloads messages to IMAP clients.

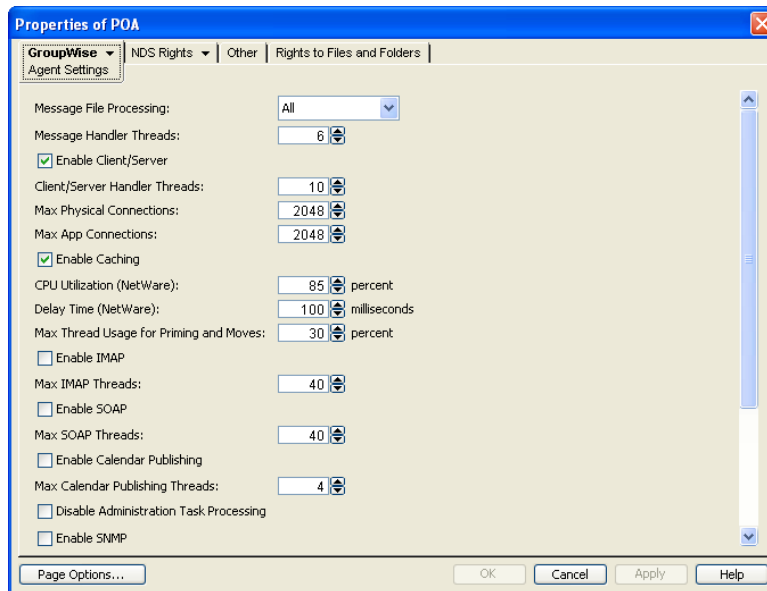
POA Web Console: You can see whether IMAP is enabled on the [Configuration](#) page under the General Settings heading.

36.2.4 Supporting SOAP Clients

Simple Object Access Protocol (SOAP) is used by email clients such as Evolution and other clients such as the Novell Data Synchronizer Connector for GroupWise to access mailboxes. You can configure the POA to communicate with SOAP-enabled email clients much like the GroupWise Windows client does.

IMPORTANT: Starting in GroupWise 2012, GroupWise WebAccess is also a SOAP client.

- 1 In ConsoleOne, browse to and select the POA object to configure, then click *Properties*.
- 2 Click *GroupWise > Agent Settings*.



- 3 Fill in the following fields:

Enable SOAP: Select *Enable SOAP* to turn on SOAP processing.

Max SOAP Threads: Specify the maximum number of SOAP threads you want the POA to start.

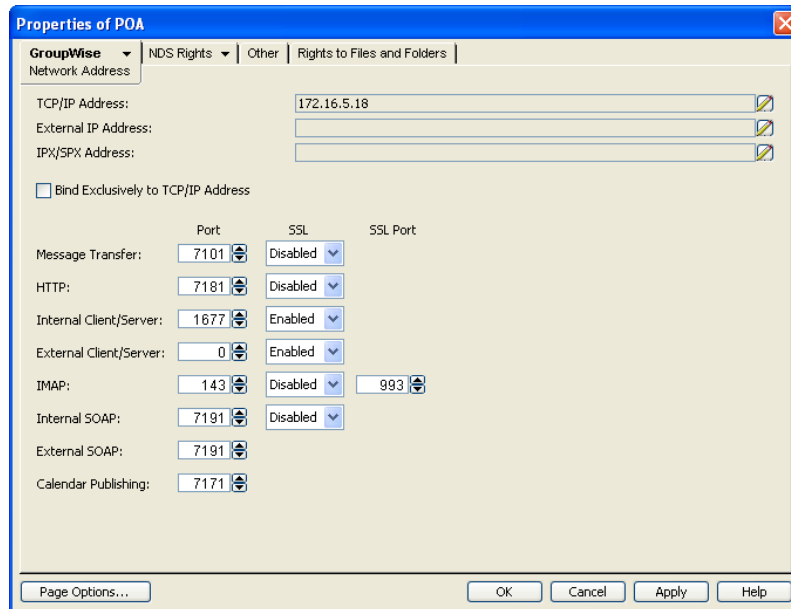
The default maximum number of SOAP threads is 40. This is adequate for most post offices, because each SOAP thread can service multiple SOAP clients. By default, the POA creates 4 SOAP threads and automatically creates additional threads as needed to service clients until the maximum number is reached. You cannot set the maximum higher than 40.

You might want to lower the maximum number of SOAP threads if SOAP processing is monopolizing system resources that you prefer to have available for other processes. However, insufficient SOAP threads can cause slow response for SOAP client users.

- 4 Click *Apply* to save the SOAP thread settings.

5 To secure SOAP connections to the post office or to change the SOAP port:

5a Click *GroupWise > Network Address*.



5b Select *Required* in the *Internal SOAP SSL* drop-down list.

The same SSL setting applies to both the internal SOAP port and the external SOAP port.

For additional instructions about using SSL connections, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107.

5c Change the SOAP port as needed.

6 Click OK.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Users of Evolution 2.0 and later can find instructions for connecting to a GroupWise system in the Evolution online help. For more information about using Evolution to access a GroupWise mailbox, see “[Evolution](#)” in “[Non-GroupWise Email Clients](#)” in the *GroupWise 2012 Interoperability Guide*.

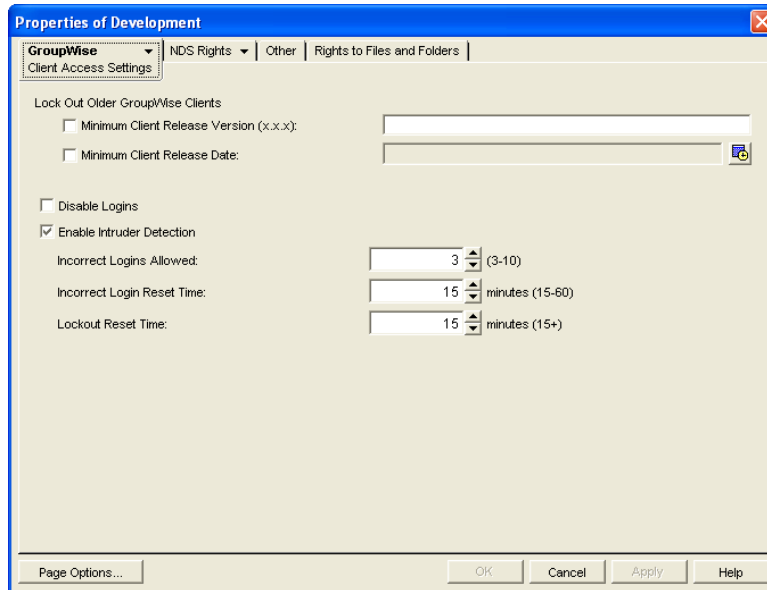
Corresponding Startup Switches: You can also use the `--soap`, `--soapmaxthreads`, `--soapport`, `--soapssl`, and `--soapthreads` startup switches in the POA startup file to configure the POA to support SOAP clients. In addition, you can use the `--evocontrol` startup switch to configure the POA to allow only specified versions of Evolution to connect to the post office.

POA Web Console: You can see whether SOAP is enabled on the [Configuration](#) page under the *General Settings* heading.

36.2.5 Checking What GroupWise Clients Are in Use

You can configure the POA to identify GroupWise client users who are running GroupWise clients that do not correspond to a specified release version and/or date. You can also force them to update to the specified version.

- 1 In ConsoleOne, browse to and right-click the Post Office object, then click *Properties*.
- 2 Click *GroupWise > Client Access Settings* to display the Client Access Settings page.



- 3 Specify the approved GroupWise release version, if any.
Only 6.x and later versions of the client are supported for lockout.
- 4 Specify the approved GroupWise release date, if any
You can specify the minimum version, the minimum date, or both. If you specify both minimums, any user for which both minimums are not true is identified as running an older GroupWise client.
- 5 Select *Lock Out Older GroupWise Clients* for the version and/or date if you want to force users to update in order to access their GroupWise mailboxes.
If you lock out older clients, client users receive an error message and are unable to access their mailboxes until they upgrade their GroupWise client software to the minimum required version and/or date.
- 6 Click *OK* to save the GroupWise version and/or date settings.
ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches: You can also use the `--gwclientreleaseversion`, `--gwclientreleasedate`, and `--enforceclientversion` startup switches in the POA startup file to configure the POA to check client version and/or date information.

POA Web Console: On the [Status](#) page of the POA Web console, click *C/S Users* to display the Current Users page, which lists all GroupWise users who are currently accessing the post office. Users who are running GroupWise clients older than the approved version and/or date are highlighted in red in the list. Users who are running newer versions are shown in blue.

If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540, you can change the expected release dates for the current POA session. Under *Client/Server Settings*, click *Enforce Lockout on Older GroupWise Clients*.

Historical Note: The capability of identifying client version and date information was first introduced in GroupWise 5.5 Enhancement Pack Support Pack 1. Any clients with versions and dates earlier than GroupWise 5.5 Enhancement Pack Support Pack 1 do not appear at all on the Current Users page of the POA Web console.

36.2.6 Supporting Forced Mailbox Caching

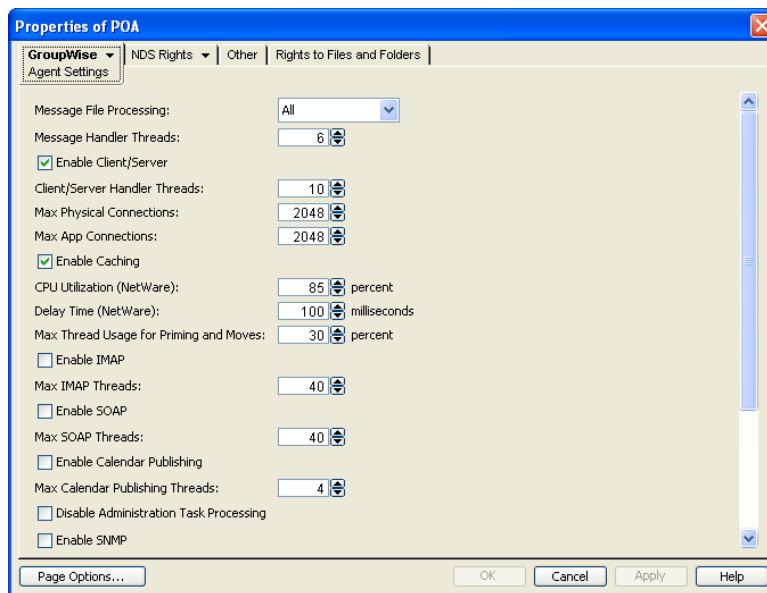
GroupWise client users have the option to download their GroupWise mailboxes to their workstations so they can work without being continuously connected to the network. This is called Caching mode. For more information, see [Section 75.1.2, “Caching Mode,”](#) on page 1017.

When client users change to Caching mode, the contents of their mailboxes must be copied to their hard drives. This process is called “priming” the mailbox. If users individually decide to use Caching mode, the POA easily handles the process.

If you force all users in the post office to start using Caching mode, as described in [“Allowing or Forcing Use of Caching Mode”](#) on page 1018, multiple users might attempt to prime their mailboxes at the same time. This creates a load on the POA that can cause unacceptable response time for other users.

To configure the POA to handle multiple requests to prime mailboxes:

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 3 Set *Max Thread Usage for Priming and Moves* as needed.

By default, the POA allocates 30% of its client/server handler threads for priming mailboxes for users who are using Caching mode for the first time. By default, the POA starts 10 client/server handler threads, so in a default configuration, three threads are available for priming. You might want to specify 60 or 80 so that 60% to 80% of POA threads are used for priming mailboxes. You might also want to increase the number of client/server handler threads the POA can start in

order to handle the temporarily heavy load while users are priming their mailboxes. See [Section 38.1.2, “Adjusting the Number of Connections for Client/Server Processing,”](#) on page 561.

- 4 Click *OK* to save the new setting.

ConsoleOne then notifies the POA to restart so the new setting can be put into effect.

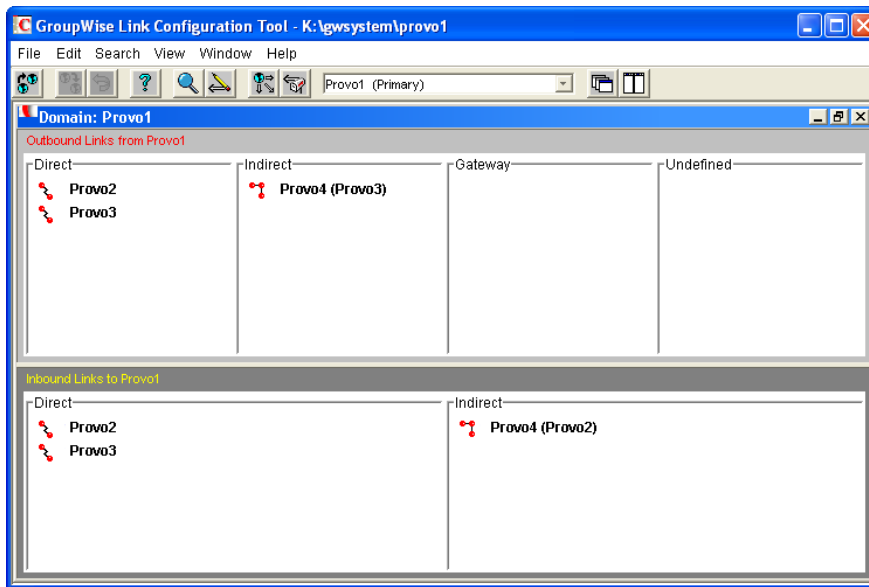
Corresponding Startup Switches: You can also use the `--primingmax` switch in the POA startup file to configure the POA to handle multiple requests to prime mailboxes.

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540, you can change the POA’s ability to respond to caching requests for the current POA session on the [Configuration](#) page. Under the *Client/Server Settings* heading, click *Max Thread Usage for Priming and Live Moves*. To increase the number of client/server threads, click *Client/Server Processing Threads* under the *Performance Settings* heading.

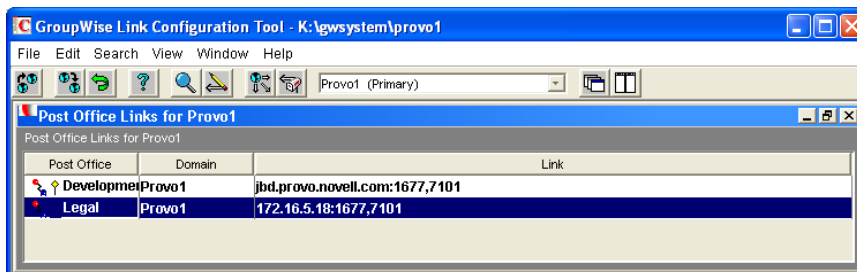
36.2.7 Restricting Message Size between Post Offices

You can configure the POA to restrict the size of messages that users are permitted to send outside the post office.

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration*.



- 2 In the drop-down list, select the domain where the post office resides, then click *Post Office Links*.



- 3 Double-click the post office where you want to restrict message size.



- 4 In the *Maximum Send Message Size* field, specify in megabytes the size of the largest message you want users to be able to send outside the post office, then click *OK*.

A setting of 0 (zero) indicates that no size limitations have been set.

- 5 To exit the Link Configuration tool and save your changes, click *File > Exit > Yes*.

ConsoleOne then notifies the POA to restart using the new maximum message size limit.

If a user's message is not sent out of the post office because of this restriction, the user receives an email notification message with a subject line of:

```
Delivery disallowed
```

The notification message also includes the subject of the original message. This message provides information to the user about why and where the message was disallowed. However, the message is still delivered to recipients in the sender's own post office.

There are additional ways to restrict the size of messages that users can send, as described in [Section 12.3.5, "Restricting the Size of Messages That Users Can Send," on page 201](#).

Corresponding Startup Switches: You can also use the `--mtpsendmax` startup switch in the POA startup file to restrict message size.

POA Web Console: You can view the maximum message size on the [Configuration](#) page. If the POA Web console is password protected as described in [Section 37.2.1, "Setting Up the POA Web Console," on page 540](#), you can change the maximum message size for the current POA session using the *Message Transfer Protocol* link on the Configuration page.

36.2.8 Supporting Calendar Publishing

See ["Configuring a POA for Calendar Publishing"](#) in ["Installing the GroupWise Calendar Publishing Host"](#) in the *GroupWise 2012 Installation Guide*.

36.3 Configuring Post Office Security

You can configure the POA in various ways to meet the security needs of the post office.

- ♦ [Section 36.3.1, "Securing Client/Server Access through an External Proxy Server," on page 506](#)
- ♦ [Section 36.3.2, "Controlling Client Redirection Inside and Outside Your Firewall," on page 507](#)
- ♦ [Section 36.3.3, "Securing the Post Office with SSL Connections to the POA," on page 508](#)
- ♦ [Section 36.3.4, "Providing LDAP Authentication for GroupWise Users," on page 510](#)

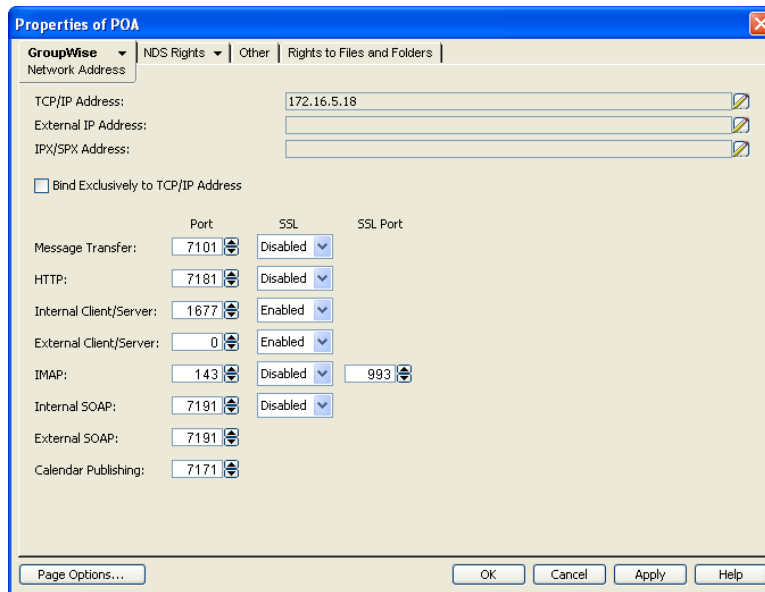
- ♦ [Section 36.3.5, “Enabling Intruder Detection,”](#) on page 516
- ♦ [Section 36.3.6, “Configuring Trusted Application Support,”](#) on page 517

36.3.1 Securing Client/Server Access through an External Proxy Server

If the server where the POA runs is behind your firewall, you can link it to an external proxy server in order to provide client/server access to the post office for GroupWise client users who are outside the firewall. You could also use generic proxy, network address translation (NAT), and port address translation (PAT) to achieve the same results.

If the POA is configured with both an internal IP address and an external proxy IP address, the POA returns both IP addresses to the GroupWise client when it attempts to log in. The client tries the internal address first, and if that does not succeed, it tries the external proxy address, then it records which address succeeded. If the user moves from inside the firewall to outside the firewall, the client might fail to log in on the first attempt, but succeeds on the second attempt.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the POA Network Address page.



- 3 Make sure the POA is already configured for client/server processing as explained in [Section 36.2.1, “Using Client/Server Access to the Post Office,”](#) on page 494.
- 4 Click the pencil icon for the *External IP Address* field to display the Edit Network Address dialog box.



- 5 Select *IP Address*, then specify the external IP address, in dotted decimal format, of the external server that GroupWise client users access from outside your firewall.

Typically, this is the public IP address presented by your external proxy server, generic proxy, NAT, or PAT.

or

Select *DNS Host Name*, then provide the DNS hostname of that server.

6 Click *OK*.

7 If you want to use a different port number for the external proxy server than you are using for client/server access to the POA itself, provide the port number in the *External Client/Server Port* field.

The network router is responsible for enabling the Network Address Translation (NAT) or Port Address Translation (PAT) between the external client requests and the internal network address of the POA. The external proxy server address and port should be listed as they are seen from the external GroupWise clients. The POA provides this address and port to clients that attempt to connect from outside the firewall.

If you are using NAT, provide an external server IP address for the POA, and in the *Port* field, use port 1677 (the default) for the external client/server port. If you are using PAT, provide an external server IP address for the POA, and in the *Port* field, use a unique external client/server port.

8 For optimum security, select *Required* in the *External Client Server SSL* drop-down list. For more information, see [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,” on page 508](#).

9 Click *OK* to save the external proxy server network address and port and return to the main ConsoleOne window.

ConsoleOne then notifies the POA to restart and begin communicating with the external proxy server.

POA Web Console You can list all POAs in your GroupWise system, along with their external IP addresses. On the [Configuration](#) page, click *IP Addresses Redirection Table* under the *General Settings* heading.

36.3.2 Controlling Client Redirection Inside and Outside Your Firewall

When a user tries to access his or her mailbox without providing the IP address of the POA for his or her post office, any POA or a GroupWise name server POA can redirect the request to the POA for the user’s post office.

A POA that is configured with both an internal IP address and a proxy IP address automatically redirects internal users to internal IP addresses and external users to proxy IP addresses. However, if you want to control which users are redirected to which IP addresses based on criteria other than user location, you can configure a post office with one POA to always redirect users to internal IP addresses and a second POA to always redirect users to proxy IP addresses. Users are then redirected based on which POA IP address they provide in the GroupWise Startup dialog box when they start the GroupWise client to access their mailboxes.

1 Configure the initial POA for the post office with the IP address that you want for internal users. For instructions, see [Section 36.2.1, “Using Client/Server Access to the Post Office,” on page 494](#).

Do not fill in the *Proxy External IP Address* field on the Network Address page of the POA object.

2 Create a second POA object in the post office and give it a unique name, such as POA_PRX. For instructions, see [Section 36.1.1, “Creating a POA Object in eDirectory,” on page 482](#).

3 Configure this second POA with an external IP address. For instructions, see [Section 36.3.1, “Securing Client/Server Access through an External Proxy Server,” on page 506](#).

Do not fill in the *TCP/IP Address* field on the Network Address page of the POA object.

- 4 Create a startup file for the new instance of the POA.
 - 4a Use the `--name` switch to specify the name of the POA object that you created in [Step 2](#).
 - 4b Use the `--ip` switch to specify the IP address of the server where this instance of the POA runs.
 - 4c Use the `--port` switch to specify the client/server port that this instance of the POA listens on.

This information needs to be specified in the POA startup file because this information is not specified in ConsoleOne for this instance of the POA.
- 5 Start the new instance of the POA.
- 6 Give users that you want to be redirected to internal IP addresses the IP address you used in [Step 1](#).
- 7 Give users that you want to be redirected to proxy IP addresses the IP address you used in [Step 3](#).

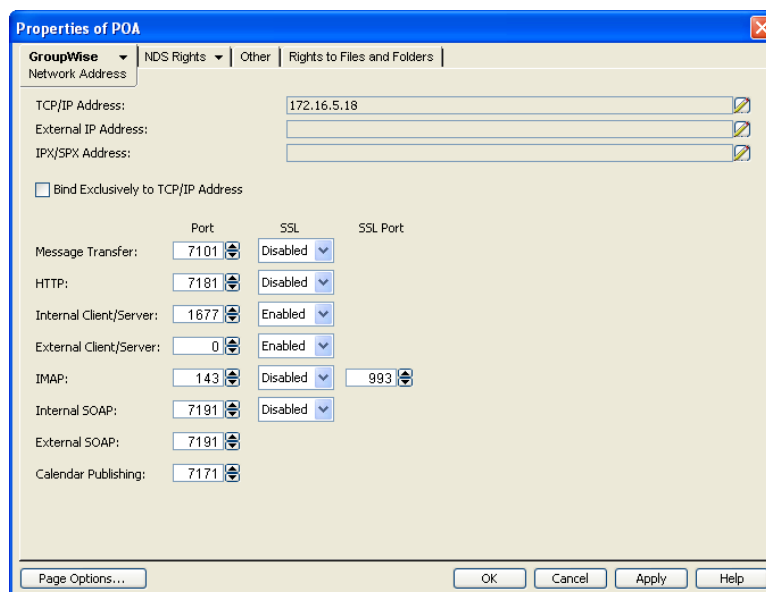
36.3.3 Securing the Post Office with SSL Connections to the POA

Secure Sockets Layer (SSL) ensures secure communication between the POA and other programs by encrypting the complete communication flow between the programs. By default, the POA is enabled to use SSL connections, but SSL connections are not required.

For background information about SSL and how to set it up on your system, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107.

To configure the POA to require SSL:

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.



- 3 To force SSL connections between the POA and its MTA, select *Required* in the *Message Transfer SSL* drop-down list.

The POA must use a TCP/IP link with the MTA in order to use SSL for the connection. See [“Using TCP/IP Links between the Post Office and the Domain”](#) on page 487.

The MTA must also use SSL for the connection to be secure. See [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,”](#) on page 643. If the MTA does not also use SSL, the connection is denied.

- 4 To force SSL connections between the POA and the POA Web console displayed in your Web browser, select *Required* in the *HTTP SSL* drop-down list.

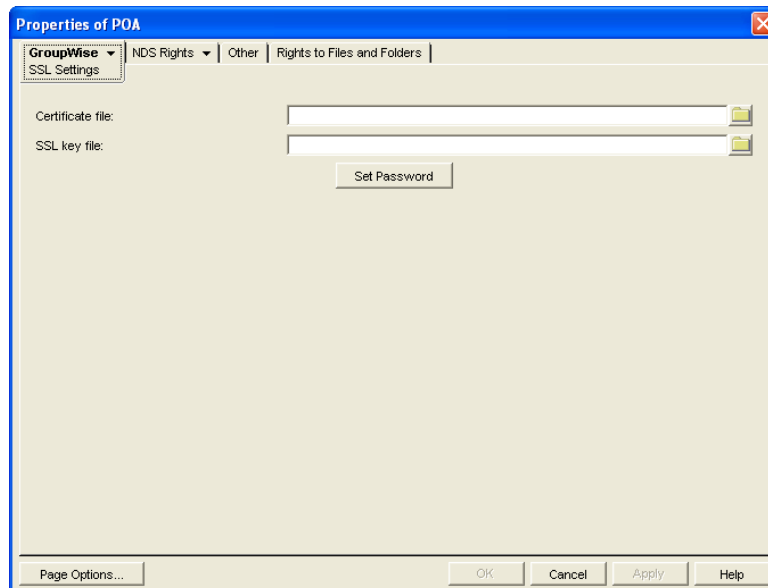
To set up the POA Web console, see [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540.

- 5 To force SSL connections between the POA and GroupWise internal clients located inside your firewall, select *Required* in the *Internal Client/Server SSL* drop-down list, so that non-SSL connections are denied.
- 6 To force SSL connections between the POA and GroupWise external clients located outside your firewall (for example, across the Internet), select *Required* in the *External Client/Server SSL* drop-down list, so that non-SSL connections are denied.
- 7 To use SSL connections between the POA and IMAP clients, select *Enabled* in the *IMAP SSL* drop-down list to let the IMAP client determine whether an SSL connection or non-SSL connection is used with an SSL-enabled POA.

or

For optimum security, select *Required* in the *IMAP SSL* drop-down list if you want the POA to force SSL connections, so that non-SSL connections from IMAP clients are denied.

- 8 To use SSL connections between the POA and SOAP clients, select *Required* in the *Internal SOAP SSL* drop-down list and/or the *External SOAP SSL* drop-down list so that internal and/or external SOAP clients must use SSL connections to the POA.
- 9 Click *Apply* to save the settings on the Network Address page.
You are prompted to supply the SSL certificate and key files. The key file must be password protected in order for SSL to function correctly.
- 10 Click *Yes* to display the SSL Settings page.



For background information about certificate files and SSL key files, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107.

By default, the POA looks for the certificate file and SSL key file in the same directory where the POA executable is located, unless you provide a full path name.

- 11 In the *Certificate File* field, browse to and select the public certificate file provided to you by your CA.
- 12 In the *SSL Key File* field:
 - 12a Browse to and select your private key file.
 - 12b Click *Set Password*.
 - 12c Provide the password that was used to encrypt the private key file when it was created.
 - 12d Click *Set Password*.
- 13 Click *OK* to save the SSL settings.

ConsoleOne then notifies the POA to restart and access the certificate and key files.

Corresponding Startup Switches: You can also use the `--certfile`, `--keyfile`, `--keypassword`, `--https`, `--mtps`, `--imap`, and `--imapsslport` switches in the POA startup file to configure the POA to use SSL.

POA Web Console: You can view SSL information for the POA on the [Status](#) and [Configuration](#) pages. In addition, when you list the client/server users that are accessing the post office, SSL information is displayed for each user.

36.3.4 Providing LDAP Authentication for GroupWise Users

By default, GroupWise client users' passwords are stored in GroupWise user databases, and the POA authenticates users to their GroupWise mailboxes by using those GroupWise passwords. For background information about passwords, see [Chapter 82, "GroupWise Passwords," on page 1099](#).

By enabling LDAP authentication for the POA, users' password information can be retrieved from any network directory that supports LDAP, including eDirectory. For background information about LDAP, see [Section 84.3, "Authenticating to GroupWise with Passwords Stored in an LDAP Directory," on page 1120](#).

When you enable LDAP authentication, it is important to provide fast, reliable access to the LDAP directory because GroupWise client users cannot access their mailboxes until they have been authenticated. The following sections provide instructions for configuring the POA to make the most efficient use of the LDAP servers available on your system:

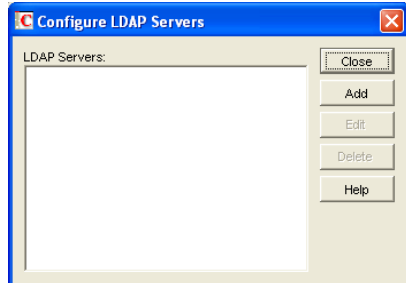
- ♦ ["Providing LDAP Server Configuration Information" on page 511](#)
- ♦ ["Enabling LDAP Authentication for a Post Office" on page 512](#)
- ♦ ["Configuring a Pool of LDAP Servers" on page 514](#)
- ♦ ["Specifying Failover LDAP Servers \(Non-SSL Only\)" on page 515](#)

NOTE: If multiple eDirectory trees are involved, refer to TID 10067272 in the [Novell Support Knowledgebase \(http://www.novell.com/support\)](#) for additional instructions.

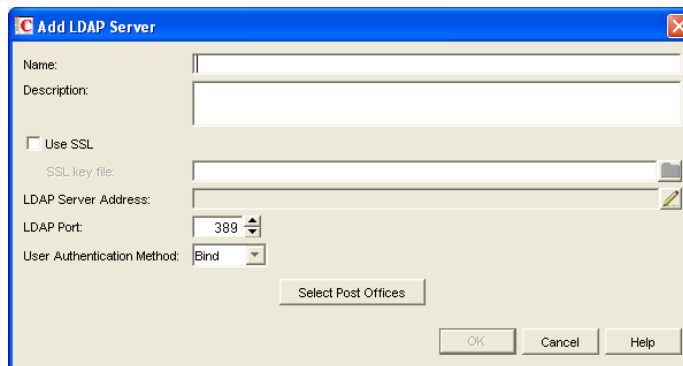
Providing LDAP Server Configuration Information

Information about your available LDAP servers must be provided in ConsoleOne before you can enable LDAP authentication for users.

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > LDAP Servers* to display the Configure LDAP Servers dialog box.



- 2 Click *Add* to add an LDAP server and provide configuration information about it.



- 3 In the *Name* field, type the name by which you want the LDAP server to be known in your GroupWise system.
- 4 In the *Description* field, provide additional information about the LDAP server as needed.
- 5 If the LDAP server requires an SSL connection, select *Use SSL*, then browse to and select the trusted root certificate of the LDAP server.

If you do not specify a full path, the POA looks in the following locations for the trusted root certificate:

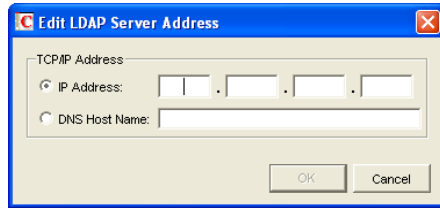
Linux: /opt/novell/groupwise/agents/bin

Windows: POA installation directory

By default, the POA looks for a file named `ngwkey.der`.

For more information about the trusted root certificate, see [Section 83.3, “Trusted Root Certificates and LDAP Authentication,”](#) on page 1115.

- 6 Click the pencil icon for the *LDAP Server Address* field.



- 7 Select *IP Address*, then specify the *IP address*, in dotted decimal format, of the LDAP server.
or

Select *DNS Host Name*, then provide the DNS hostname of the LDAP server.

The default LDAP port is 389 for non-SSL connections and 636 for SSL connections.

- 8 If the default port number is already in use, specify a unique LDAP port number.
- 9 Click *OK* to save the LDAP server address and port information.
- 10 In the *User Authentication Method* field, select *Bind* or *Compare*.
For a comparison of these methods, see [Section 84.3, "Authenticating to GroupWise with Passwords Stored in an LDAP Directory,"](#) on page 1120.
- 11 Click *OK* to save the configuration information for the LDAP server.
- 12 Repeat [Step 2](#) through [Step 11](#) for each LDAP server that you want to make available to GroupWise for LDAP authentication.
Providing configuration information for multiple LDAP servers creates a pool of LDAP servers, which provides fault tolerance and load balancing to ensure fast, reliable mailbox access for GroupWise users.
- 13 Continue with ["Enabling LDAP Authentication for a Post Office"](#) on page 512.

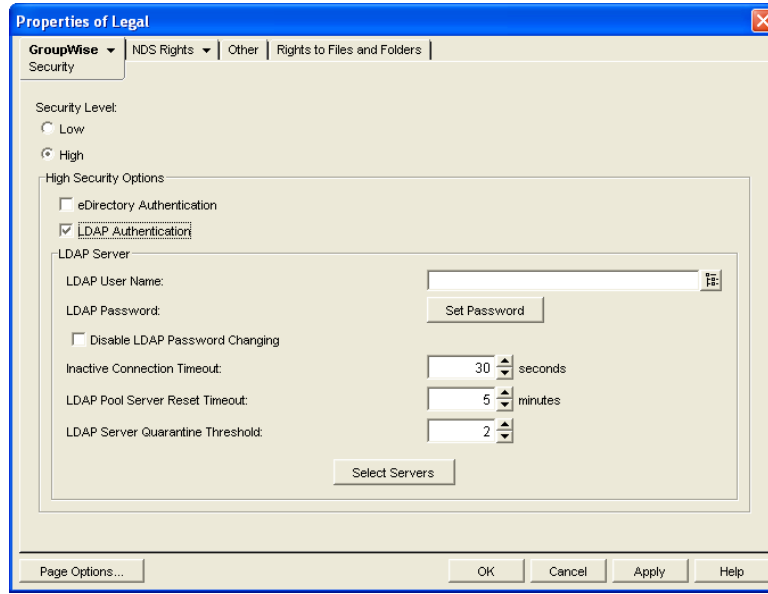
Corresponding Startup Switches: You can also use the `--ldapipaddr`, `--ldapport`, `--ldapuserauthmethod`, `--ldapssl`, and `--ldapsslkey` startup switches in the POA startup file to provide the LDAP server information.

Enabling LDAP Authentication for a Post Office

To configure the POA to perform LDAP authentication for the users in a post office:

- 1 In ConsoleOne, browse to and right-click the Post Office object, then click *Properties*.

- 2 Click *GroupWise > Security* to display the Security page.



- 3 For *Security Level*, select *High*.
- 4 In the *High Security Options* box, select *LDAP Authentication*.
- 5 If you want the POA to access the LDAP server with specific rights to the LDAP directory, specify a user name that has those rights.

If you are using a Novell LDAP server, you can browse for an eDirectory User object. The information returned from eDirectory uses the following format:

```
cn=user_name,ou=orgunit,o=organization
```

If you are using another LDAP server, you must type the information in the format used by that LDAP server.

If the LDAP user name for the POA requires a password, click *Set Password*, type the password twice for verification, then click *Set Password*.

For more information about LDAP user names, see [Section 84.3, "Authenticating to GroupWise with Passwords Stored in an LDAP Directory,"](#) on page 1120.

- 6 If you want to prevent GroupWise users from changing their LDAP passwords by using the Password dialog box in the GroupWise client, select *Disable LDAP Password Changing*.
This option is deselected by default, so that if users change their passwords in the GroupWise client through the Security Options dialog box (GroupWise Windows client > *Tools > Options > Security*) or on the Passwords page (GroupWise WebAccess > *Options > Password*), their LDAP passwords are changed to match the new passwords provided in the GroupWise client.
- 7 If the LDAP server is configured for bind connections, as described in ["Providing LDAP Server Configuration Information"](#) on page 511, specify the number of seconds the POA should maintain an inactive connection to the LDAP server.

The default is 30 seconds.

- 8 If you have only one LDAP server, click *OK* to save the security settings for the post office. You have provided all the necessary information to provide LDAP authentication for users in the post office.

or

If you have multiple LDAP servers and want to configure them into an LDAP server pool, click *Apply*, then continue with [“Configuring a Pool of LDAP Servers”](#) on page 514.

or

If you have multiple LDAP servers and want to configure them for failover, click *OK* to save the security settings for the post office, then continue with [“Specifying Failover LDAP Servers \(Non-SSL Only\)”](#) on page 515.

Corresponding Startup Switches: You can also use the `--ldapuser`, `--ldappwd`, `--ldapdisablepwdchg`, and `--ldaptimeout` startup switches in the POA startup file to configure POA access to the LDAP server.

POA Web Console: You can see if LDAP is enabled on the [Configuration](#) page. If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540, click *LDAP Authentication* to view LDAP settings and change some of them for the current POA session.

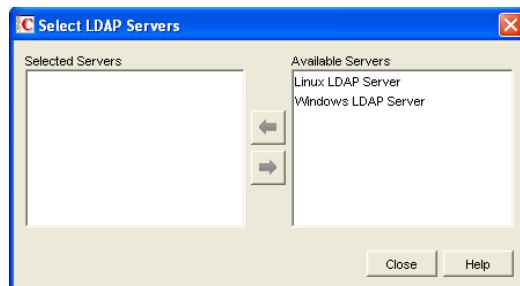
Configuring a Pool of LDAP Servers

You can configure the POA to contact a different LDAP server each time it needs to access the LDAP directory. This provides load balancing and fault tolerance because each LDAP server in the pool is contacted equally often by the POA. The LDAP server pool can include as many as five servers.

- 1 Make sure you have enabled LDAP Authentication as described in [“Enabling LDAP Authentication for a Post Office”](#) on page 512.
- 2 In the *LDAP Pool Server Reset Timeout* field, specify the number of minutes the POA should wait before trying to contact an LDAP server in the pool that failed to respond to the previous contact.

The default is 5 minutes.

- 3 Click *Select Servers* to define the specific pool of LDAP servers that you want to be available to users in this post office for LDAP authentication.



- 4 Select one or more LDAP servers in the *Available Servers* list, then click the arrow button to move them into the *Selected Servers* list.
- 5 Click *OK* to save the list of LDAP servers.
- 6 Click *OK* to save the security settings for the post office.

ConsoleOne then notifies the POA to restart so the new LDAP settings can be put into effect.

Corresponding Startup Switches: You can also use the `--ldappooln` and `--ldappoolresetime` startup switches in the POA startup file to configure the LDAP server pool and the timeout interval. If you choose to configure the LDAP server pool in the startup file rather than in ConsoleOne, additional switches must be provided to complete the configuration (`--ldappoolportn`, `--ldapsslpooln`, and `--ldapsslkeypooln`). Configuring the pool in ConsoleOne is the recommended approach.

If you previously set up LDAP authentication on the post office Security page in ConsoleOne and then you add the pooling startup switches to the POA startup file, the pooling switches override any LDAP information provided in ConsoleOne.

Specifying Failover LDAP Servers (Non-SSL Only)

If the POA does not need to use an SSL connection to your LDAP servers, you can use the `--ldapipaddr` switch to list multiple LDAP servers. Then, if the primary LDAP server fails to respond, the POA tries the next LDAP server in the list, and so on until it is able to access the LDAP directory. This provides failover LDAP servers for the primary LDAP server but does not provide load balancing, because the primary LDAP server is always contacted first.

- 1 Make sure you have provided the basic LDAP information on the post office Security page in ConsoleOne, as described in [“Enabling LDAP Authentication for a Post Office” on page 512](#).
- 2 Edit the POA startup file (`post_office.poa`) with an ASCII text editor.
For more information about the POA startup file, see [Chapter 40, “Using POA Startup Switches,” on page 581](#).
- 3 Use the `--ldapipaddr` startup switch to list addresses for multiple LDAP servers. Use a space between addresses.

For example:

```
/ldapipaddr-172.16.5.18 172.16.15.19 172.16.5.20
```

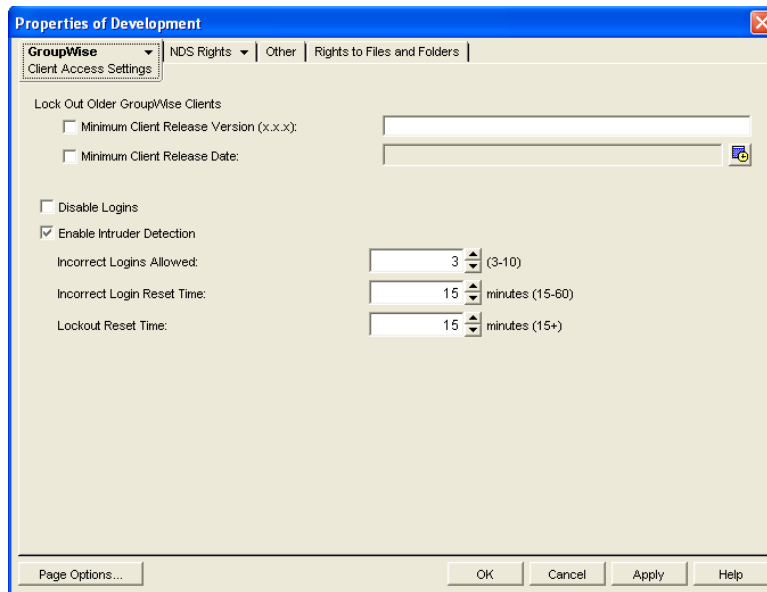
IMPORTANT: Do not include any LDAP servers that require an SSL connection. There is currently no way to specify multiple SSL key files unless you are using pooled LDAP servers, as described in [“Configuring a Pool of LDAP Servers” on page 514](#).

- 4 Save the POA startup file, then exit the text editor.
- 5 Stop the POA, then start the POA so that it reads the updated startup file.

36.3.5 Enabling Intruder Detection

You can configure the POA to detect system break-in attempts in the form of repeated unsuccessful logins.

- 1 In ConsoleOne, browse to and right-click the Post Office object, then click *Properties*.
- 2 Click *GroupWise > Client Access Settings* to display the Client Access Settings page.



- 3 Select *Enable Intruder Detection*.
- 4 Specify how many unsuccessful login attempts are allowed before the user is locked out. The default is 5; valid values range from 3 to 10.
- 5 Specify in minutes how long unsuccessful login attempts are counted. The default is 15; valid values range from 15 to 60.
- 6 Specify in minutes how long the user login is disabled. The default is 30; the minimum setting is 15.
- 7 Click *OK* to save the intruder detection settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

If a user is locked out by intruder detection, his or her GroupWise account is disabled. To restore access for the user in ConsoleOne, right-click the User object, click *GroupWise > Account*, then deselect *Disable Logins*. To restore access for the user at the POA Web console, click *Configuration > Intruder Detection*, then clear the lockout.

Corresponding Startup Switches: You can also use the `--intruderlockout`, `--incorrectloginattempts`, `--attemptsresetinterval`, and `--lockoutresetinterval` startup switches in the POA startup file to configure the POA for intruder detection.

POA Web Console: You can view current intruder detection settings on the [Configuration](#) page. If the POA Web console is password protected as described in [Section 37.2.1, "Setting Up the POA Web Console,"](#) on page 540, you can change the settings by clicking the *Intruder Detection* link. You cannot disable intruder detection from the POA Web console.

36.3.6 Configuring Trusted Application Support

For background information about setting up trusted applications in ConsoleOne, see [Section 4.12, “Trusted Applications,”](#) on page 90.

36.4 Configuring Post Office Maintenance

You can configure the POA to manage databases and disk space in the post office on a regular basis:

- ♦ [Section 36.4.1, “Scheduling Database Maintenance,”](#) on page 517
- ♦ [Section 36.4.2, “Scheduling Disk Space Management,”](#) on page 520
- ♦ [Section 36.4.3, “Performing Nightly User Upkeep,”](#) on page 523

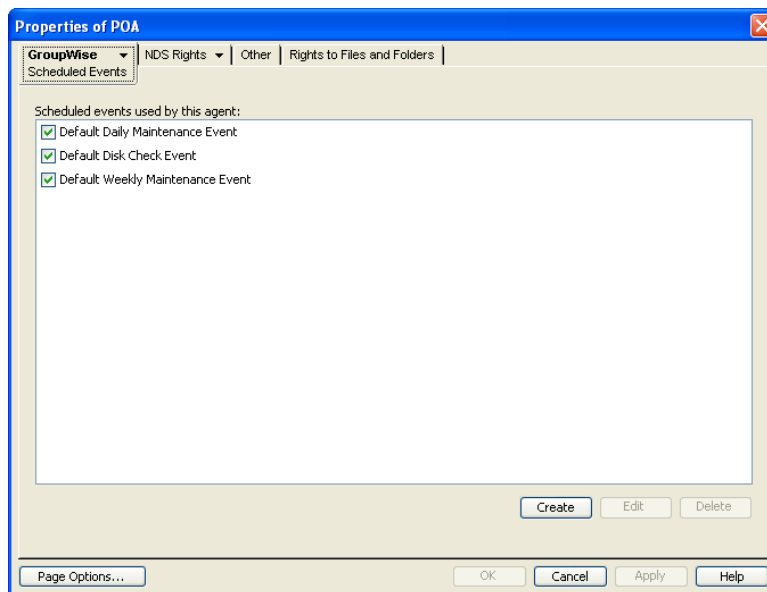
36.4.1 Scheduling Database Maintenance

By default, the POA performs the following database maintenance events:

- ♦ **Default Daily Maintenance Event:** The default daily maintenance event occurs at 2:00 a.m. The POA performs a Structure check on user, message, and document databases and fixes any problems it encounters.
- ♦ **Default Weekly Maintenance Event:** The default weekly maintenance event occurs on Saturday at 3:00 a.m. The POA runs an Audit Report and a Content check. The Audit report lists the type of license (full vs. limited) each mailbox requires and which mailboxes haven't been accessed for at least 60 days. The Content check verifies pointers from user databases to messages in message databases and pointers from message databases to attachments in the `offiles` directory structure, and fixes any problems it encounters.

You can modify the default database maintenance events, or create additional database maintenance events for the POA to perform on a regular basis.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Scheduled Events* to display the Scheduled Events page.



The Scheduled Events page lists a pool of POA events available to all POAs in your GroupWise system.

- 3 To modify the default daily database maintenance event, which affects all POAs that have this database maintenance event enabled, select *Default Daily Maintenance Event*, then click *Edit*.

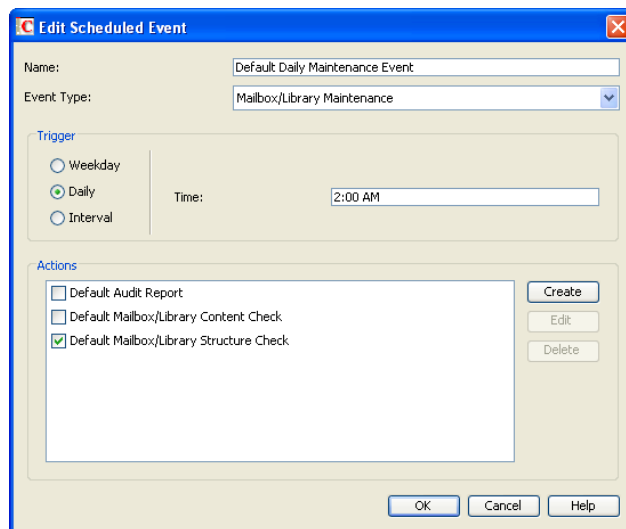
or

To modify the default weekly database maintenance event, which affects all POAs that have this database maintenance event enabled, select *Default Weekly Maintenance Event*, then click *Edit*.

or

To create a new database maintenance event, which is added to the pool of POA events that can be enabled for any POA in your GroupWise system, click *Create*, then type a name for the new database maintenance event. Select *Mailbox/Library Maintenance* in the *Type* field.

If the *Create* button is dimmed and you have a *View* button rather than an *Edit* button, you are connected to a secondary domain in a GroupWise system where *Restrict System Operations to Primary Domain* has been selected under *System Preferences*. For more information, see [Section 4.2, "System Preferences,"](#) on page 72.



- 4 In the *Trigger* box, specify when you want the database maintenance event to take place.

You can have the database maintenance event take place once a week, once a day, or at any other regular interval, at whatever time you choose.

The list below the *Trigger* box displays the pool of POA database maintenance actions that are available for inclusion in all POA database maintenance events in your GroupWise system.

- 5 To modify a default database maintenance action, select one of the existing actions, then click *Edit*.

or

To create a new database maintenance action, click *Create*, then type a name for the new database maintenance action.

The name can include as many as 128 characters.

Database maintenance actions and options you can schedule include:

Actions	Options on Actions
Analyze/Fix Databases	Databases
Structure	User
Index check	Message
Contents	Document
Collect statistics	
Attachment file check	Logging
Fix problems	Log file
Update user disk space totals	Verbose log level
Analyze/Fix Library	Results mailed to
Verify library	Administrator
Fix document/version/element	Individual users
Verify document files	
Validate all document security	Misc
Synchronize user name	Support options
Remove deleted storage areas	Exclude
Reassign orphaned documents	
Reset word lists	Selected users

For more detailed descriptions of the actions, click *Help* in the Scheduled Event Actions dialog box. See also:

- ♦ [Chapter 27, “Maintaining User/Resource and Message Databases,”](#) on page 409
- ♦ [Chapter 28, “Maintaining Library Databases and Documents,”](#) on page 415

- 6 Select and configure the database maintenance action to perform for the database maintenance event.
- 7 Click *OK* three times to close the various scheduled event dialog boxes and save the modified database maintenance event.

ConsoleOne then notifies the POA to restart so the new or modified database maintenance event can be put into effect.

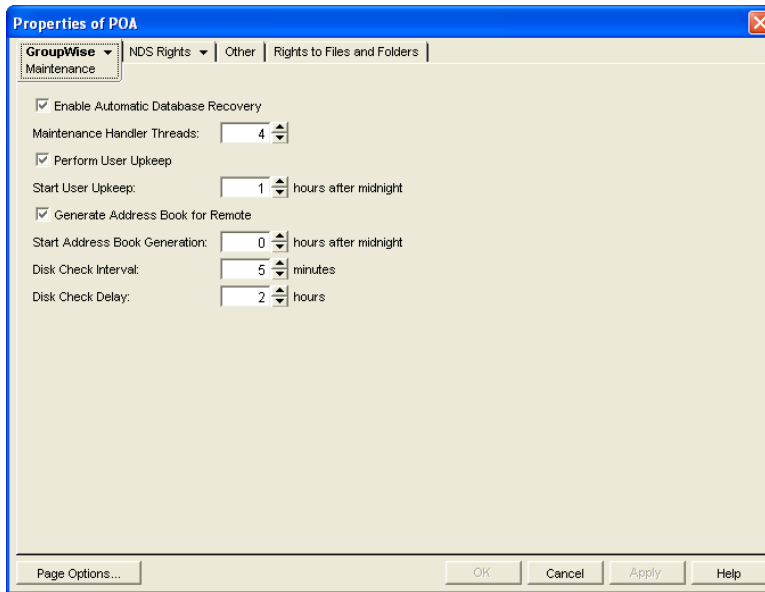
POA Web Console You can see what database maintenance events the POA is scheduled to perform at the bottom of the [Configuration](#) page.

36.4.2 Scheduling Disk Space Management

By default, the POA performs one recurring disk space management event. Every 5 minutes, the POA checks to make sure there is at least 2048 MB of free disk space in the post office directory. If there is less than 2048 MB of free disk space, the POA performs a Reduce operation on the user and message databases in the post office. If available disk space drops below 200 MB, the POA stops processing mail.

You can modify this default disk space management event, or create additional disk space management events for the POA to perform on a regular basis.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Maintenance* to display the POA Maintenance page.



- 3 To change the interval at which the selected POA checks for free disk space in its post office, adjust the number of minutes in the *Disk Check Interval* field as needed.

The default is 5 minutes, which could be much too frequent if ample disk space is readily available.

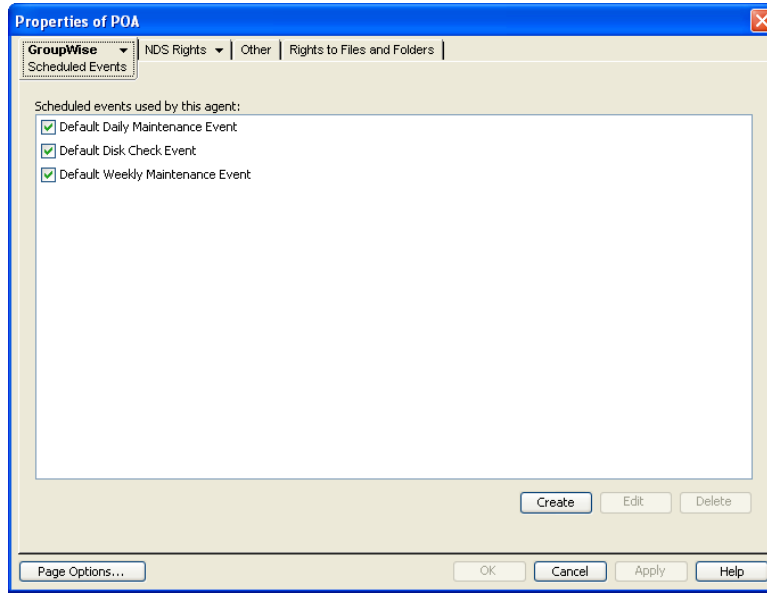
When a disk space problem is encountered, the time interval no longer applies until after the situation has been corrected. Instead, the POA continually checks available disk space to determine if it can restart message threads that have been suspended because of the low disk space condition.

- 4 To change the amount of time the POA allows to pass before notifying the administrator again about a problem condition that has already been reported, adjust the number of hours in the *Disk Check Delay* field as needed.

The default is 2 hours.

- 5 Client *Apply* to save the maintenance settings.

- 6 Click *GroupWise > Scheduled Events* to display the Scheduled Events page.



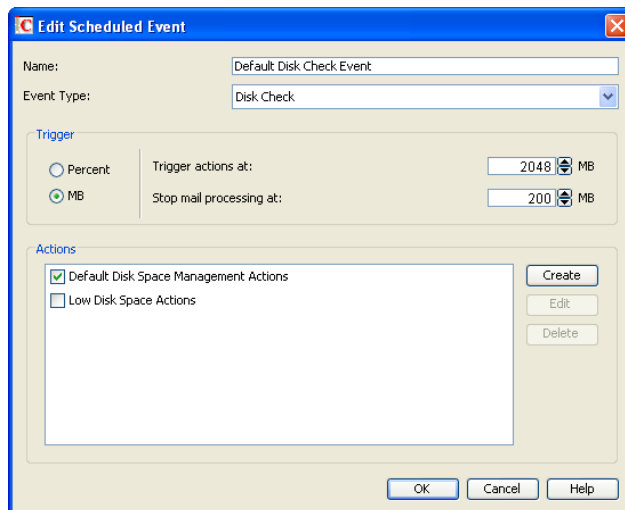
The Scheduled Events page lists a pool of POA events available to all POAs in your GroupWise system.

- 7 To modify the default disk space management event, which affects all POAs that have this disk space management event enabled, select *Default Disk Check Event*, then click *Edit*.

or

To create a new disk space management event, which is added to the pool of POA events that can be enabled for any POA in your GroupWise system, click *Create*, then type a name for the new disk space management event. The name can include as many as 128 characters. Select *Disk Check* in the *Type* field.

If the *Create* button is dimmed and you have a *View* button rather than an *Edit* button, you are connected to a secondary domain in a GroupWise system where *Restrict System Operations to Primary Domain* has been selected under *System Preferences*. For more information, see [Section 4.2, "System Preferences," on page 72](#).



- 8 In the *Trigger* box, select *Percent* or *MB* to determine whether you want the amount of available disk space measured by percentage or by megabytes.
- 9 In the *Trigger Actions At* field, specify the minimum amount of available disk space you want to have in the post office. When the minimum amount is reached, the Disk Check actions are triggered
- 10 In the *Stop Mail Processing At* field, specify the minimum amount of available disk space at which you want the POA to stop receiving and processing messages.

The list below the *Trigger* box displays the pool of disk space management actions that are available for inclusion in all POA disk space management events in your GroupWise system.

- 11 To modify the action that the default disk space management event includes, select *Default Disk Check Actions*, then click *Edit*.

or

To create a new disk space management action, click *Create*, then type a name for the new disk space management action.

The name can include as many as 128 characters.

Disk space management actions and options you can schedule include:

Actions	Options on Actions
Reduce/Expire Messages	Databases
Reduce only	User
Expire and reduce	Message
- Items older than	Logging
- Downloaded items older than	Log file
- Items larger than	Verbose log level
- Trash older than	Results mailed to
- Reduce mailbox to	Administrator
- Reduce mailbox to limited size	Individual users
Include	Misc
- Received items	Support options
- Sent items	Exclude
- Calendar items	Selected users
- Only backed-up items	Notification
- Only retained items	Notify administrator when action begins
Archive/Delete Documents	Notify administrator if action fails
Delete Activity Logs	Notify administrator when action completes

For more detailed descriptions of the actions, click *Help* in the Scheduled Event Actions dialog box. See also [Chapter 30, "Managing Database Disk Space," on page 423](#).

- 12 Select and configure the disk space management action to perform.

- 13 Click *OK* twice to close the scheduled event dialog boxes and save the modified disk space management event.

ConsoleOne then notifies the POA to restart so the new or modified disk space management event can be put into effect.

You might want to create several disk space management events with different triggers and actions. For some specific suggestions on implementing disk space management, see [Section 12.3, “Managing Disk Space Usage in the Post Office,”](#) on page 196.

POA Web Console You can view the currently scheduled disk check events on the [Scheduled Events](#) page.

36.4.3 Performing Nightly User Upkeep

To keep GroupWise users’ mailboxes and calendars up-to-date, the following activities must be performed each day:

- ♦ Advance uncompleted tasks to the next day
- ♦ Delete expired items from users’ mailboxes
- ♦ Empty expired items from the Trash
- ♦ Synchronize each user’s Frequent Contacts Address Book and personal address books with the GroupWise Address Book
- ♦ Synchronize user addresses in personal groups with the GroupWise Address Book, in case users have been moved, renamed, or deleted

The upkeep performed is determined by the settings located in each user’s Cleanup options (*Tools > Options > Environment Options > Cleanup*). Auto-Delete is run by the POA during user upkeep, but Auto-Archive is run by the client as soon as the user accesses his or her mailbox. In Caching mode, Auto-Delete is also run by the client.

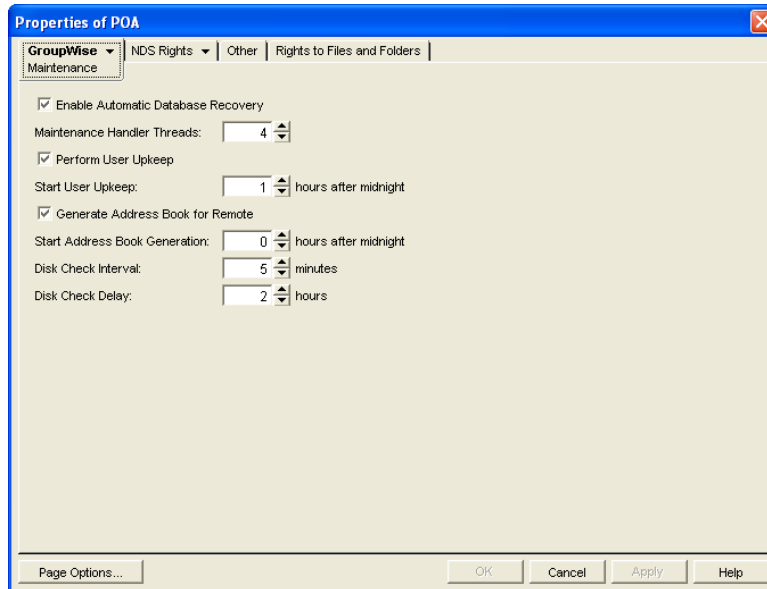
Unread items such as messages and upcoming appointments are not deleted. However, unread calendar items such as appointments, reminder notes, and tasks that are scheduled in the past are deleted.

Although user upkeep includes deletion activities, it does not necessarily reduce mailbox disk space usage. To reduce disk space usage, see [Section 12.3, “Managing Disk Space Usage in the Post Office,”](#) on page 196.

Synchronization of personal address books with the GroupWise Address Book enables the latest contact information to be synchronized to users’ mobile devices when a synchronization solution such as [Novell Data Synchronizer](http://www.novell.com/documentation/datasynchronizer1) (<http://www.novell.com/documentation/datasynchronizer1>) has been implemented. When users copy contacts from the GroupWise Address Book to personal address books, changes made in the GroupWise Address Book are mirrored in personal address books and, therefore, are available for synchronization to mobile devices. However, changes to copied contacts made on mobile devices are not retained in GroupWise because the contact information from the GroupWise Address Book always overrides the contact information of the copied contacts.

You can configure the POA to take care of these user upkeep activities once a day, at a convenient time.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Maintenance* to display the POA Maintenance page.



- 3 Select *Perform User Upkeep*.
- 4 In the *Start User Upkeep* field, specify the number of hours after midnight for the POA to start performing user upkeep.

The default is 1 hour.

- 5 If you have Remote or Caching users, select *Generate Address Book for Remote*.
- 6 Specify the number of hours after midnight for the POA to generate the daily copy of the GroupWise Address Book for Remote and Caching users.

The default is 0 hours (that is, at midnight).

If you want to generate the GroupWise Address Book for download more often than once a day, you can delete the existing `wprof50.db` file from the `\wpcout\ofs` subdirectory of the post office. A new downloadable GroupWise Address Book is automatically generated for users in the post office.

In addition to this feature, starting in GroupWise 7, the POA automatically tracks changes to the GroupWise Address Book and provides automatic synchronization, as described in [Section 6.5, "Controlling Address Book Synchronization for Caching and Remote Client Users,"](#) on [page 112](#).

- 7 Click *OK* to save the new nightly user maintenance settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches: You can also configure nightly user upkeep using startup switches in the POA startup file. By default, nightly user upkeep is enabled. Use the `--nuuoffset` and `--rdaboffset` switches to specify the start times.

POA Web Console: You can view the current user upkeep schedule on the [Scheduled Events](#) page.

37 Monitoring the POA

By monitoring the POA, you can determine whether or not its current configuration is meeting the needs of the post office it services. You have a variety of tools to help you monitor the operation of the POA:

- ♦ [Section 37.1, “Using the POA Server Console,” on page 525](#)
- ♦ [Section 37.2, “Using the POA Web Console,” on page 539](#)
- ♦ [Section 37.3, “Using POA Log Files,” on page 551](#)
- ♦ [Section 37.4, “Using GroupWise Monitor,” on page 553](#)
- ♦ [Section 37.5, “Using Novell Remote Manager,” on page 553](#)
- ♦ [Section 37.6, “Using an SNMP Management Console,” on page 553](#)
- ♦ [Section 37.7, “Notifying the GroupWise Administrator,” on page 557](#)
- ♦ [Section 37.8, “Using the POA Error Message Documentation,” on page 557](#)
- ♦ [Section 37.9, “Employing POA Troubleshooting Techniques,” on page 558](#)
- ♦ [Section 37.10, “Using Platform-Specific POA Monitoring Tools,” on page 558](#)

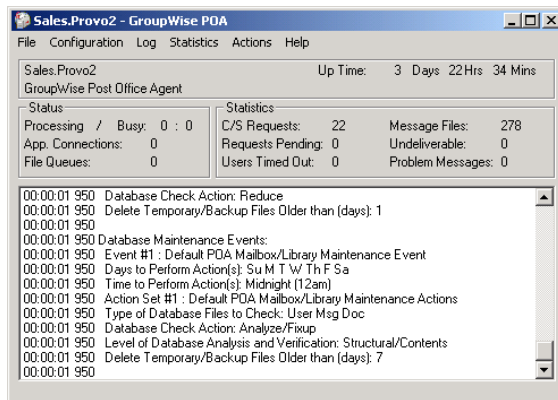
37.1 Using the POA Server Console

The following topics help you monitor and control the POA from the POA server console:

- ♦ [Section 37.1.1, “Monitoring the POA from the POA Server Console,” on page 525](#)
- ♦ [Section 37.1.2, “Controlling the POA from the POA Server Console,” on page 529](#)

37.1.1 Monitoring the POA from the POA Server Console

The POA server console provides information, status, and message statistics about the POA to help you assess its current functioning.



Linux: You must use the `--show` startup switch in order to display the Linux POA server console. See [“Starting the Linux Agents with a User Interface”](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.

Windows: You can suppress the Windows POA server console by running the POA as a service. See [“Starting the Windows GroupWise Agents”](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.

The POA server console consists of several components:

- ◆ [“POA Information Box”](#) on page 526
- ◆ [“POA Status Box”](#) on page 526
- ◆ [“POA Statistics Box”](#) on page 527
- ◆ [“POA Log Message Box”](#) on page 528
- ◆ [“POA Admin Thread Status Box”](#) on page 529

You can minimize the POA server console, but do not close it unless you want to stop the POA.

POA Information Box

The *POA Information* box identifies the POA whose POA server console you are viewing, which is especially helpful when multiple POAs are running on the same server.

PostOffice.Domain: Displays the name of the post office serviced by this POA, and what domain it is linked to.

Description: Displays the description provided in the *Description* field in the POA Identification page in ConsoleOne. When you run multiple POAs on the same server, the description should uniquely identify each one. If multiple administrators work at the server where the POA runs, the description could include a note about who to contact before stopping the POA.

Up Time: Displays the length of time the POA has been running.

POA Web Console The [Status](#) page also displays this information.

POA Status Box

The *POA Status* box displays the current status of the POA and its backlog. The information displayed varies depending on whether the POA is processing client/server connections, message files, both, or neither.

Processing: Displays a rotating bar when the POA is running. If the bar is not rotating, the POA has stopped. For assistance, see [“Post Office Agent Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

Busy: Displays the number of POA threads currently in use (busy) for client/server connections, message files, or both, depending on POA configuration. In a typical POA configuration, the number to the left of the colon is the number of busy client/server threads and the number to the right of the colon is the number of busy message handler threads. You can change the total number of threads available. See [Section 38.1.2, “Adjusting the Number of Connections for Client/Server Processing,”](#) on page 561 and [Section 38.2.1, “Adjusting the Number of POA Threads for Message File Processing,”](#) on page 564.

User Connections (for client/server processing): Displays the number of active application (“virtual”) TCP/IP connections between the POA and the GroupWise clients run by GroupWise users. You can change the maximum number of user connections. See [Section 38.1.2, “Adjusting the Number of Connections for Client/Server Processing,”](#) on page 561.

Physical Connections (for client/server processing): Displays the number of active physical TCP/IP connections between the post office and the GroupWise clients run by GroupWise users. You can change the maximum number of physical connections. See [Section 38.1.2, “Adjusting the Number of Connections for Client/Server Processing,”](#) on page 561.

Priority Queues (for message file processing): Displays the number of messages waiting in the high priority message queues. You can control the number of threads processing message files. See [Section 38.2.1, “Adjusting the Number of POA Threads for Message File Processing,”](#) on page 564.

Normal Queues (for message file processing): Displays the number of messages waiting in the normal priority message queues. You can control the number of threads processing message files. See [Section 38.2.1, “Adjusting the Number of POA Threads for Message File Processing,”](#) on page 564.

File Queues (for message file processing): Displays the total number of messages waiting in all message queues, when client/server information and message file information are displayed together.

The number of messages displayed as waiting in message queues is not an exact count. For example, if the POA detects numerous messages to process in the priority 4 queue (normal messages), it does not scan and count messages in lower priority queues. Therefore, actual counts of message files waiting in queues could be higher than the counts displayed in the Status box.

For information about the various message queues in the post office, see [“Post Office Directory”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

POA Web Console: The [Status](#) page also displays the status information listed above. In addition, you can display detailed information about specific queue contents.

POA Statistics Box

The *POA Statistics* box displays statistics showing the current workload of the POA. The information displayed varies depending on whether the POA is processing client/server connections, message files, both, or neither.

C/S Requests (for client/server processing): Displays the number of active client/server requests between GroupWise clients and the POA.

Requests Pending (for client/server processing): Displays the number of client/server requests from GroupWise clients the POA has not yet been able to respond to. If the number is large, see [“POA Statistics Box Shows Requests Pending”](#) in [“Post Office Agent Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

Users Timed Out (for client/server processing): Displays the number of GroupWise clients no longer communicating with the POA. If the number is large, see [“POA Statistics Box Shows Users Timed Out”](#) in [“Post Office Agent Problems”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

Message Files (for message file processing): Displays the total number of messages processed by the POA. This includes user messages, status messages, and service requests processed by the POA.

Undeliverable (for message file processing): Displays the number of messages that could not be delivered because the user was not found in that post office or because of other similar problems. Senders of undeliverable messages are notified. For assistance, see [“Message Has Undeliverable Status”](#) in [“Strategies for Message Delivery Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

Problem Messages (for message file processing): Displays the number of invalid message files that have problems not related to user error. It also displays requests the POA cannot process because of error conditions. For assistance, see [“Message Is Dropped in the problem Directory”](#) in [“Strategies for Message Delivery Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

Users Delivered: Displays the number of user messages delivered to recipients in the post office. A message with six recipients in the local post office is counted six times.

Statuses: Displays the number of status messages delivered to recipients in the post office.

Rules Executed: Displays the number of users’ rules executed by the POA.

POA Web Console: The [Status](#) page also displays this information. In addition, you can display detailed information about client/server connections and message file processing.

POA Log Message Box

The *POA Log Message* box displays the same information that is being written to the POA log file. The amount of information displayed in the *POA Log Message* box depends on the current log settings for the POA. See [Section 37.3, “Using POA Log Files,”](#) on page 551. The information scrolls up automatically.

Windows Note: To stop the automatic scrolling, click *Log*, then deselect *Auto Scroll*. You can then use the scroll bar to browse through the contents of the log message box.

POA Web Console: You can view and search POA log files on the [Log Files](#) page.

Informational Messages

When you first start the POA, you typically see informational messages that list current agent settings, current number of threads, TCP/IP options (client/server), and scheduled events. As the POA runs, it continues to provide status and delivery information in the *POA Log Message* box.

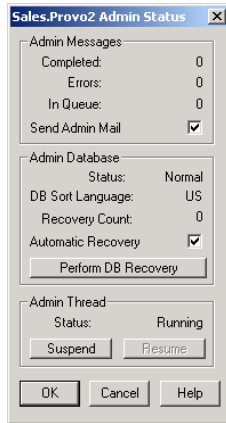
Error Messages

If the POA encounters a problem processing a message, it displays an error message in the *POA Log Message* box. See [“Post Office Agent Error Messages”](#) in *GroupWise 2012 Troubleshooting 1: Error Messages*.

POA Admin Thread Status Box

The POA admin thread updates the post office database (`wphost.db`) when users and/or user information are added, modified, or removed, and repairs it when damage is detected.

To display the *POA Admin Thread Status* box from the POA server console, click *Configuration > Admin Status*.



The following tasks pertain specifically to the POA admin thread:

- ♦ [“Suspending/Resuming the POA Admin Thread” on page 531](#)
- ♦ [“Displaying POA Admin Thread Status” on page 534](#)
- ♦ [“Recovering the Post Office Database Automatically or Immediately” on page 535](#)

POA Web Console: You can display POA admin thread status on the [Configuration](#) page. Under the *General Settings* heading, click *Admin Task Processing*. If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,” on page 540](#), you can change the admin settings for the current POA session.

37.1.2 Controlling the POA from the POA Server Console

You can perform the following tasks to monitor and control the POA from the POA server console at the server where the POA is running:

- ♦ [“Stopping the POA” on page 530](#)
- ♦ [“Suspending/Resuming the POA Admin Thread” on page 531](#)
- ♦ [“Displaying the POA Software Date” on page 531](#)
- ♦ [“Displaying Current POA Settings” on page 532](#)
- ♦ [“Displaying Detailed Statistics about POA Functioning” on page 532](#)
- ♦ [“Displaying Client/Server Information” on page 532](#)
- ♦ [“Listing Message Queue Activity” on page 533](#)
- ♦ [“Displaying Message Transfer Status” on page 533](#)
- ♦ [“Restarting the MTP Thread” on page 534](#)
- ♦ [“Displaying POA Admin Thread Status” on page 534](#)
- ♦ [“Recovering the Post Office Database Automatically or Immediately” on page 535](#)
- ♦ [“Recovering User and Message Databases Automatically” on page 536](#)

- ♦ “Updating QuickFinder Indexes” on page 536
- ♦ “Compressing QuickFinder Indexes” on page 537
- ♦ “Regenerating QuickFinder Indexes” on page 537
- ♦ “Browsing the Current POA Log File” on page 537
- ♦ “Viewing a Selected POA Log File” on page 537
- ♦ “Cycling the POA Log File” on page 538
- ♦ “Adjusting POA Log Settings” on page 538
- ♦ “Editing the POA Startup File” on page 539
- ♦ “Accessing Online Help for the POA” on page 539

Stopping the POA

You might need to stop and restart the POA for the following reasons:

- ♦ Updating the agent software
- ♦ Troubleshooting message flow problems
- ♦ Backing up GroupWise databases
- ♦ Rebuilding GroupWise databases

To stop the POA from the POA server console:

- 1 Click *File > Exit > Yes*.

Linux: If the Linux POA does not respond to *Exit*, follow the instructions in [“Stopping the Linux POA When It Is Running As a Daemon”](#) on page 530.

Windows: If the Windows POA does not respond to *Exit*, you can close the POA server console to stop the POA or use the Task Manager to terminate the POA task.

- 2 Restart the POA, as described in the following sections in the *GroupWise 2012 Installation Guide*:
 - ♦ [“Starting the Linux Agents as Daemons”](#)
 - ♦ [“Starting the Windows GroupWise Agents”](#)

Stopping the Linux POA When It Is Running As a Daemon

To stop the Linux POA when it is running in the background as a daemon and you started it using the `grpwise` script:

- 1 Make sure you are logged in as `root`.
- 2 Enter the following command:


```
rcgrpwise stop
```
- 3 Use the following command to verify that the POA has stopped.


```
rcgrpwise status
```

To stop the Linux POA when it is running in the background as a daemon and you started it manually (not using the `grpwise` script):

- 1 Make sure you are logged in as `root`.
- 2 Determine the process IDs (PIDs) of the POA:

```
ps -eaf | grep gwpoa
```

The PIDs for all gwpoa processes are listed.

You can also obtain this information from the [Environment](#) page of the POA Web console.

- 3 Kill the first POA process listed:

Syntax: `kill PID`

Example: `kill 1483`

It might take a few seconds for all POA processes to terminate.

- 4 Use the `ps` command to verify that the POA has stopped.

```
ps -eaf | grep gwpoa
```

- 5 (Conditional) If the initial `kill` command does not stop the POA, use the following command:

Syntax: `kill -9 PID`

Example: `kill -9 1483`

Suspending/Resuming the POA Admin Thread

You can cause the POA to stop accessing the post office database (`wphost.db`) without stopping the POA completely. For example, you could suspend the POA admin thread while backing up the post office database.

To suspend the POA admin thread:

- 1 At the POA server console, click *Configuration > Admin Status*.
- 2 Click *Suspend*.

The POA admin thread no longer accesses the post office database until you resume processing.

To resume the POA admin thread:

- 1 At the POA server console, click *Configuration > Admin Status*.
- 2 Click *Resume*.

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, "Setting Up the POA Web Console,"](#) on page 540, you can suspend and resume the POA admin thread from the [Configuration](#) page. Under the General Settings heading, click *Admin Task Processing > Suspend or Resume > Submit*.

Displaying the POA Software Date

It is important to keep the POA software up-to-date. You can display the date of the POA software from the POA server console.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Help > About POA*.

POA Web Console: You can check the POA software date on the [Environment](#) page.

Displaying Current POA Settings

You can list the current configuration settings of the POA at the POA server console.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Configuration > Agent Settings*.

The configuration information displays in the log message box and is written to the log file.

If information you need scrolls out of the log message box, you can scroll back to it. See [“Browsing the Current POA Log File” on page 537](#).

For information about POA configuration settings, see [Chapter 36, “Configuring the POA,” on page 481](#) and [Chapter 40, “Using POA Startup Switches,” on page 581](#).

POA Web Console: You can check the current POA settings on the [Configuration](#) page.

Displaying Detailed Statistics about POA Functioning

The POA server console displays essential information about the functioning of the POA. More detailed information is also available.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Statistics > Misc. Statistics*.
- 3 Review the Detailed Statistics dialog box. The following statistics are displayed and written to the log file for the current POA up time:
 - ◆ Databases rebuilt
 - ◆ Users deleted
 - ◆ Users moved
 - ◆ Moved messages processed
 - ◆ Statuses processed

POA Web Console: You can display statistics on the [Status](#) page.

Displaying Client/Server Information

When the POA and the GroupWise clients communicate in client/server mode, you can display statistics to indicate the performance level of the TCP/IP communication.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Statistics > Client/Server*.
- 3 In the menu, click the type of statistics to display.

The selected type of statistics for the current POA up time are listed in the message log box and are written to the POA log file.

If information you need scrolls out of the log message box, you can scroll back to it. See [“Browsing the Current POA Log File” on page 537](#).

All Statistics: Lists the information for *General Statistics*, *Throughput*, *Physical Connections*, and *Application Connections*, as described below.

General Statistics: Lists the DNS address and IP address of the server, along with the TCP port for the POA, the number of messages received, sent, and aborted, and the number of physical and application connections active and allowed.

Show Throughput: Lists the total number of messages processed by the POA for all users. Statistics are provided for the current elapsed time and as a per second average.

Clear Throughput: Resets the current elapsed time to zero.

Physical Connections: Lists the currently active physical connections. Physical connections are active TCP connections created whenever GroupWise users do something that requires communication and closed when the specific activities have been completed. By listing the physical connections, you can see what users are actively using GroupWise and how much throughput each user is generating. Users' IP addresses are also listed.

Application Connections: Lists the currently active application connections. Every user that starts GroupWise has an application connection for as long as GroupWise is running, even if GroupWise is not actively in use at the moment. By listing the application connections, you can see what users have started GroupWise and how much throughput each user is generating. Users' IP addresses are also listed.

Show Redirection List: Lists all POAs in your GroupWise system and indicates whether each is configured for TCP/IP. The list includes the IP address of each POA and the IP address of its proxy server outside the firewall, if applicable. This redirection information is obtained from the post office database (`wphost.db`).

Check Redirection List: Attempts to contact each POA in your GroupWise system and reports the results. If a POA is listed as "Connection Failed," see "Post Office Agent Problems" in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

POA Web Console: You can display client/server information on the [Configuration](#) page. You can list client/server users from the Status page using the *C/S Users* and *Remote/Caching Users* links.

Listing Message Queue Activity

The POA uses eight queues to process message files. You can view the activity in each of these queues. For more information about message queues, see "Post Office Directory" in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Actions > View MF Queues*.
- 3 View the queue activity in the message log box. Use the scroll bar if necessary to scroll through the information.

If information you need scrolls out of the log message box, you can scroll back to it. See "Browsing the Current POA Log File" on page 537.

The information is also written to the POA log file.

You can check queue activity on the Status page. Under the *Thread Status* heading, click the type of thread to view queue activity for.

Displaying Message Transfer Status

When the POA links to the MTA by way of TCP/IP, you can view the status of the TCP/IP link from the POA server console.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Configuration > Message Transfer Status*.
- 3 View the following information about the TCP/IP link:

Outbound TCP/IP Address: Displays the TCP/IP address and port where the MTA listens for messages from the POA.

Inbound TCP/IP Address: Displays the TCP/IP address and port where the POA listens for messages from the MTA.

Hold Directory: Displays the path to the directory where the POA stores messages if the TCP/IP link to the MTA is closed.

Current Status: Lists the current status of the TCP/IP link.

- ♦ **Open:** The POA and the MTA are successfully communicating by way of TCP/IP.
- ♦ **Closed:** The POA is unable to contact the MTA by way of TCP/IP
- ♦ **Unavailable:** The POA is not yet configured for TCP/IP communication with the MTA.
- ♦ **Unknown:** The POA is unable to contact the MTA in any way.

Messages Written: Displays the number of messages the POA has sent.

Message Read: Displays the number of messages the POA has received.

Last Closure Reason: Provides an explanation for why the post office was last closed. For assistance resolving closure problems, see “[Post Office Agent Error Messages](#)” in *GroupWise 2012 Troubleshooting 1: Error Messages*.

POA Web Console: You can display message transfer status on the [MTP Status](#) page.

Restarting the MTP Thread

When the POA links to the MTA by way of TCP/IP, you can restart the Message Transfer Protocol (MTP) thread that provides the link between the POA and the MTA.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Actions > Restart MTP*.

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540, you can restart the MTA thread from the [Configuration](#) page. Click *Message Transfer Protocol > Restart MTP > Submit*. In addition, you can control the send and receive threads separately on the [MTP Status](#) page. In the *Send* or *Receive* column, click the current status, then click *Stop/Start MTP Send/Receive > Submit*.

Displaying POA Admin Thread Status

Status information for the POA admin thread is displayed in a separate dialog box, rather than on the main POA server console.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Configuration > Admin Status*.

The following admin status information is displayed:

Admin Message Box

The *Admin Message* box provides the following information about the workload of the POA admin thread:

Completed: Number of administrative messages successfully processed.

Errors: Number of administrative messages not processed because of errors.

In Queue: Number of administrative messages waiting in the queue to be processed.

Send Admin Mail: Select this option to send a message to the administrator whenever a critical error occurs. See [Section 37.7, “Notifying the GroupWise Administrator,”](#) on page 557.

Admin Database Box

The *Admin Database* box provides the following information about the post office database (`wphost.db`):

Status: Displays one of the following statuses:

- ♦ **Normal:** The POA admin thread is able to access the post office database normally.
- ♦ **Recovering:** The POA admin thread is recovering the post office database.
- ♦ **DB Error:** The POA admin thread has detected a critical database error. The post office database cannot be recovered. Rebuild the post office database in ConsoleOne. See [Section 26.3, “Rebuilding Domain or Post Office Databases,” on page 405](#).

The POA admin thread does not process any more administrative messages until the database status has returned to Normal.

- ♦ **Unknown:** The POA admin thread cannot determine the status of the post office database. Exit the POA, then restart it, checking for errors on startup.

DB Sort Language: Displays the language code for the language that determines the sort order of lists displayed in ConsoleOne and the GroupWise Address Book.

Recovery Count: Displays the number of recoveries performed on the post office database by this POA for the current POA session.

Admin Thread Box

The Admin Thread box displays the following information:

Status: Displays one of the following statuses:

- ♦ **Running:** The POA admin thread is active.
- ♦ **Suspended:** The POA admin thread is not processing administrative messages.
- ♦ **Starting:** The POA admin thread is initializing.
- ♦ **Terminated:** The POA admin thread is not running.

POA Web Console: You can display POA admin thread status from the [Configuration](#) page. Under the *General Settings* heading, click *Admin Task Processing*.

Recovering the Post Office Database Automatically or Immediately

The POA admin thread can recover the post office database (`wphost.db`) when it detects a problem.

To enable or disable automatic post office database recovery:

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Configuration > Admin Status > Automatic Recovery* to toggle this feature on or off for the current POA session.

To change the setting permanently, see [Section 36.1.2, “Configuring the POA in ConsoleOne,” on page 484](#).

To recover the post office database immediately:

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Configuration > Admin Status > Perform DB Recovery*.

For additional database repair procedures, see [Chapter 26, “Maintaining Domain and Post Office Databases,” on page 401](#).

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,” on page 540](#), you can recover the post office database from the [Configuration](#) page. Under the *General Settings* heading, click *Admin Task Processing*. Select *Automatic Recovery* or *Perform DB Recovery* as needed.

Recovering User and Message Databases Automatically

The POA can automatically recover user databases (*userxxx.db*) and message databases (*msgnnn.db*) when it detects a problem because databases can be open during the recover process. This procedure is a “recover” rather than a “rebuild,” because a “rebuild” requires that all users and agents are out of the database being rebuilt. See [Chapter 27, “Maintaining User/Resource and Message Databases,” on page 409](#).

To enable/disable automatic message and user database recovery:

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Actions > Auto Rebuild* to toggle this feature on or off for the current POA session.

To change the setting permanently, see [Section 36.1.2, “Configuring the POA in ConsoleOne,” on page 484](#).

POA Web Console: You can see whether automatic message and user database recovery is enabled on the [Configuration](#) page under the *Performance Settings* heading.

Updating QuickFinder Indexes

GroupWise uses QuickFinder technology to index messages and documents stored in post offices. You can start indexing from the POA server console. For example, if you just imported a large number of documents, you could start indexing immediately, rather than waiting for the next scheduled indexing cycle.

To update QuickFinder indexes for the post office:

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Actions > QuickFinder > Update Indexes*.

To avoid overloading the POA with indexing processing, a maximum of 1000 items are indexed per database. If a very large number of messages are received regularly, or if a user with a very large mailbox is moved to a different post office (requiring the user’s messages to be added into the new post office indexes), you might need to repeat this action multiple times in order to get all messages indexed. If too many repetitions are required to complete the indexing task, see [Section 39.6, “Customizing Indexing,” on page 579](#) for assistance.

You can set up indexing to occur at regular intervals. See [Section 39.1, “Regulating Indexing,” on page 573](#).

If the indexing load on the POA is heavy, you can set up a separate POA just for indexing. See [Section 39.5, “Configuring a Dedicated Indexing POA \(Windows Only\),” on page 577](#).

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,” on page 540](#), you can update QuickFinder indexes from the [Configuration](#) page. Under the *General Settings* heading, click *QuickFinder Indexing*.

Compressing QuickFinder Indexes

QuickFinder indexes are automatically compressed at midnight each night to conserve disk space. You can start compression at any other time from the POA server console. For example, if you just imported and indexed a large number of documents and are running low on disk space, you could compress the indexes immediately, rather than waiting for it to happen at midnight.

To compress QuickFinder indexes for the post office:

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Actions > QuickFinder > Compress Indexes*.

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,” on page 540](#), you can compress QuickFinder indexes from the [Configuration](#) page. Under the *General Settings* heading, click *QuickFinder Indexing*.

Regenerating QuickFinder Indexes

If QuickFinder indexes become damaged, you can easily delete and re-create them.

To re-create QuickFinder indexes for the post office:

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Actions > QuickFinder > Delete and Regenerate Indexes*.

You can also press Ctrl+Q.

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,” on page 540](#), you can re-create QuickFinder indexes from the [Configuration](#) page. Under the *General Settings* heading, click *QuickFinder Indexing*.

Browsing the Current POA Log File

In the log message box, the POA displays the same information being written to the POA log file. The amount of information depends on the current log settings for the POA.

The information automatically scrolls up the screen as additional information is written. You can stop the automatic scrolling so you can manually scroll back through earlier information.

To browse the current POA log file and control scrolling:

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Log > Auto Scroll* to toggle automatic scrolling on or off.

For explanations of messages in the POA log file, see [“Post Office Agent Error Messages” in *GroupWise 2012 Troubleshooting 1: Error Messages*](#).

See also [Section 37.3, “Using POA Log Files,” on page 551](#).

POA Web Console: You can browse and search POA log files on the [Log Files](#) page.

Viewing a Selected POA Log File

Reviewing log files is an important way to monitor the functioning of the POA.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Log > View Log*.

The following information is provided:

Log Files: Lists the current POA log files, ordered from the oldest log file at the top to the newest log file at the bottom. The current log file is marked with an asterisk (*).

Date/Time: Displays the date and time of each POA log file.

Space Used: Displays the amount of disk space currently occupied by that POA's log files. You can control the amount of space consumed by POA log files during the current POA session. You can also control the default amount of disk space for POA log files in the POA Log Settings page in ConsoleOne or in the POA startup file. See [Section 37.3.2, "Configuring POA Log Settings and Switches,"](#) on page 552.

Log File Directory: Displays the full path of the directory where the POA writes its log files. See [Section 37.3.2, "Configuring POA Log Settings and Switches,"](#) on page 552.

- 3 In the log file list, select the POA log file you want to view.

Windows Note: For the Windows POA, you can select the viewer to use by providing the full path to the viewer program. The default viewer is Notepad.

- 4 Click *View*.

For explanations of messages in the POA log file, see ["Post Office Agent Error Messages"](#) in [GroupWise 2012 Troubleshooting 1: Error Messages](#).

See also [Section 37.3, "Using POA Log Files,"](#) on page 551.

POA Web Console: You can view and search POA log files on the [Log Files](#) page.

Cycling the POA Log File

You can have the POA start a new log file as needed.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Log > Cycle Log*.

Adjusting POA Log Settings

Default log settings are established when you start the POA. However, you can adjust the POA log settings for the current session from the POA server console. This overrides any settings provided in ConsoleOne or in the POA startup file. The modified settings remain in effect until you restart the POA, at which time the log settings specified in ConsoleOne or the startup file take effect again.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Log > Log Settings*.
- 3 Adjust the values as needed for the current POA session.
See [Section 37.3, "Using POA Log Files,"](#) on page 551.

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, "Setting Up the POA Web Console,"](#) on page 540, you can adjust POA log settings from the [Configuration](#) page. Click the *Log Settings* heading.

Editing the POA Startup File

You can change the configuration of the POA by editing the POA startup file from the POA server console.

- 1 At the server where the POA is running, display the POA server console.
- 2 Click *Configuration > Edit Startup File*.
- 3 Make the necessary changes, then save and exit the startup file.
- 4 Stop and restart the POA.

Accessing Online Help for the POA

Click *Help* on the menu bar for information about the POA server console. Click the *Help* button in any dialog box for additional information.

37.2 Using the POA Web Console

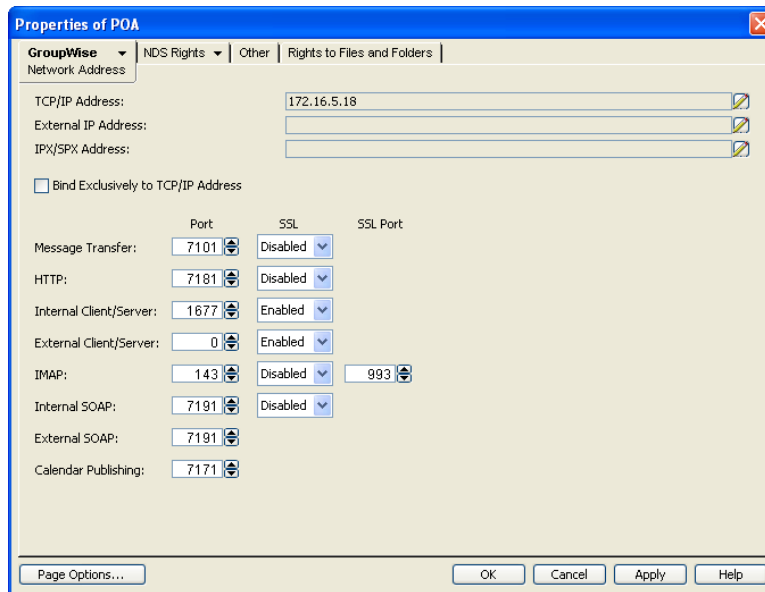
The POA Web console enables you to monitor and control the POA from any location where you have access to a Web browser and the Internet. This provides substantially more flexible access than the POA server console, which can only be accessed from the server where the POA is running.

- ♦ [Section 37.2.1, “Setting Up the POA Web Console,” on page 540](#)
- ♦ [Section 37.2.2, “Accessing the POA Web Console,” on page 541](#)
- ♦ [Section 37.2.3, “Monitoring the POA from the POA Web Console,” on page 542](#)
- ♦ [Section 37.2.4, “Controlling the POA from the POA Web Console,” on page 549](#)

37.2.1 Setting Up the POA Web Console

The default HTTP port for the POA Web console is established during POA installation. You can change the port number and increase security after installation in ConsoleOne.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.



If you configured the POA for TCP/IP links during installation, the *TCP/IP Address* field should display the POA server's network address. If it does not, follow the instructions in ["Using TCP/IP Links between the Post Office and the Domain"](#) on page 487. The POA must be configured for TCP/IP in order to provide the POA Web console.

- 3 Make a note of the IP address or DNS hostname in the *TCP/IP Address* field. You need this information to access the POA Web console.

The *HTTP Port* field displays the default port number of 7181.

- 4 If the default HTTP port number is already in use on the POA server, specify a unique port number.
- 5 Make a note of the HTTP port number. You need this information to access the POA Web console.
- 6 If you want to use an SSL connection for the POA Web console, which provides optimum security, select *Enabled* in the HTTP SSL drop-down list.

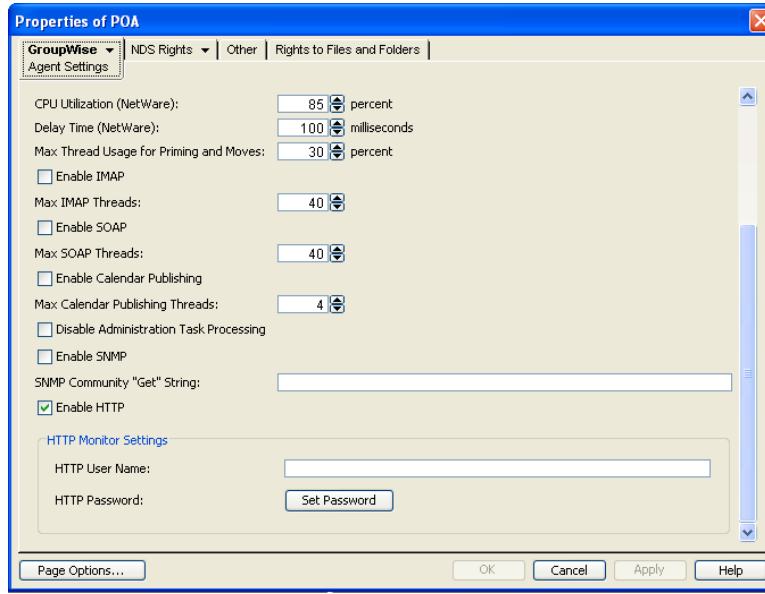
For additional instructions about using SSL connections, see [Section 83.2, "Server Certificates and SSL Encryption,"](#) on page 1107.

- 7 Click *Apply* to save your changes on the Network Address page.

If you want to limit access to the POA Web console, or if you want to be able to change configuration settings at the POA Web console, you must provide a user name and password.

IMPORTANT: Some fields in the POA Web console are displayed only when the Web console is password protected.

- 8 Click *GroupWise > Agent Settings*, then scroll down to *HTTP Settings*.



- 9 In the *HTTP Settings* box:
- 9a In the *HTTP User Name* field, specify a unique user name.
 - 9b Click *Set Password*.
 - 9c Type the password twice for verification.
 - 9d Click *Set Password*.

Unless you are using an SSL connection, do not use a Novell eDirectory user name and password because the information passes over the non-secure connection between your Web browser and the POA.

For convenience, use the same user name and password for all agents that you plan to monitor from GroupWise Monitor. This saves you from having to provide the user name and password information as Monitor accesses each agent.

IMPORTANT: A user name and password are required in order for you to change POA configuration settings in the POA Web console.

- 10 Click *OK* to save the POA Web console settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches: You can also use the `--httpport`, `--httpuser`, `--httppassword`, and `--httpssl` startup switches in the POA startup file to enable and secure the POA Web console. In addition, you can use the `--httprefresh` switch to control how often the POA refreshes the information provided to your Web browser.

37.2.2 Accessing the POA Web Console

To monitor the POA from your Web browser, view the URL where the POA is located by supplying the network address and port number as displayed on the Network Address page in ConsoleOne. For example:

<http://172.16.5.18:1677>
<http://172.16.5.18:7181>
<http://server1:7181>
<https://server2:1677>

When viewing the POA Web console, you can specify either the client/server port or the HTTP port.

GroupWise 2012 POA - Development.Provo1		
Status Configuration Environment Log Files Scheduled Events MTP Status Help		
GroupWise Post Office Agent		
Up Time: 2 Days 22 Hours 16 Minutes		
	Total	
C/S Users	1	
Application Connections	2	
Physical Connections	0	
SOAP Sessions	0	
Priority Queues	0	
Normal Queues	0	
GWCheck Auto Queues	0	
GWCheck Scheduled Queues	0	
Thread Status		
	Total	Busy
C/S Handler Threads	10	0
Message Worker Threads	6	0
GWCheck Worker Threads	4	0
SOAP Threads	3	0
Calendar Publishing Threads	3	0
Message Transfer Status	Open	
Statistics		
	Total	
C/S Requests	3682	
C/S Requests Pending	0	
Users Timed Out	4	
SOAP Requests	21	
SOAP Pending Requests	0	
GWEvents:	0	
Calendar Publishing Requests	8	
Rules Executed	0	
Users Delivered	0	
Message Files Processed	20	

37.2.3 Monitoring the POA from the POA Web Console

The POA Web console provides several pages of information to help you monitor the performance of the POA. The title bar at the top of the POA Web console displays the name of the POA and its post office. Below the title bar appears the POA Web console menu that lists the pages of information available in the POA Web console. Online help throughout the POA Web console helps you interpret the information being displayed and use the links provided.

- ◆ [“Monitoring POA Status” on page 543](#)
- ◆ [“Monitoring and Tracking POA Threads” on page 543](#)
- ◆ [“Checking the POA Operating System Environment” on page 544](#)
- ◆ [“Viewing and Searching POA Log Files” on page 544](#)
- ◆ [“Listing POA Scheduled Events” on page 545](#)
- ◆ [“Checking Link Status to the MTA” on page 545](#)
- ◆ [“Taking Performance Snapshots” on page 546](#)
- ◆ [“Monitoring SOAP Events” on page 547](#)

Monitoring POA Status

When you first access the POA Web console, the Status page is displayed. Online help on the Status page helps you interpret the status information being displayed.

GroupWise 2012 POA - Development.Provo1		
Status Configuration Environment Log Files Scheduled Events MTP Status Help		
GroupWise Post Office Agent		
Up Time: 2 Days 22 Hours 16 Minutes		
	Total	
C/S Users	1	
Application Connections	2	
Physical Connections	0	
SOAP Sessions	0	
Priority Queues	0	
Normal Queues	0	
GWCheck Auto Queues	0	
GWCheck Scheduled Queues	0	
Thread Status		
	Total	Busy
C/S Handler Threads	10	0
Message Worker Threads	6	0
GWCheck Worker Threads	4	0
SOAP Threads	3	0
Calendar Publishing Threads	3	0
Message Transfer Status	Open	
Statistics		
	Total	
C/S Requests	3682	
C/S Requests Pending	0	
Users Timed Out	4	
SOAP Requests	21	
SOAP Pending Requests	0	
GWEvents:	0	
Calendar Publishing Requests	8	
Rules Executed	0	
Users Delivered	0	
Message Files Processed	20	

Click any hyperlinked status items for additional details. The status information is much the same as that provided at the POA server console, as described in [Section 37.1.1, "Monitoring the POA from the POA Server Console,"](#) on page 525.

Monitoring and Tracking POA Threads

The POA Status page provides links to detailed POA thread status for the following types of threads:

- ◆ C/S handler threads
- ◆ Message worker threads
- ◆ GWCheck worker threads
- ◆ SOAP threads
- ◆ Calendar Publishing threads

GroupWise 2012 POA - Development.Provo1				
Status Configuration Environment Log Files Scheduled Events MTP Status Help				
C/S Handler Threads				
Threads	Thread ID	Request count	State	Time Elapsed (Secs)
WTCP-Deve-Handler_10	F06B	1437	Idle	
WTCP-Deve-Handler_9	F073	2245	Idle	
WTCP-Deve-Handler_8	F07B	0	Idle	
WTCP-Deve-Handler_7	F084	0	Idle	
WTCP-Deve-Handler_6	F08C	0	Idle	
WTCP-Deve-Handler_5	F094	0	Idle	
WTCP-Deve-Handler_4	F472	0	Idle	
WTCP-Deve-Handler_3	F09C	0	Idle	
WTCP-Deve-Handler_2	F0A4	0	Idle	
WTCP-Deve-Handler_1	F0AC	0	Idle	

The *Thread ID* column provides the information you need in order to track a specific thread through one or more POA log files, as described in “[Viewing and Searching POA Log Files](#)” on page 544.

Checking the POA Operating System Environment

On the POA Web console menu, click *Environment* to display information about the operating system where the POA is running.

On a Linux server, the following information is displayed:

GroupWise 2012 POA - Development.Provo1	
Status Configuration Environment Log Files Scheduled Events MTP Status Help	
Server Configuration	
Server	jbd-oes
OS Revision	Linux Release 2.6.16.60-0.54.5-default
OES Version	Novell Open Enterprise Server 2.0.3 (x86_64)
Main Thread Process ID	18431
Build Dates	
GroupWise Agent Build Version	12.0.0-98196
GroupWise Agent Build Date	11-26-11
GroupWise Resource Build Date	11-11-11

On a Windows server, the following information is displayed:

GroupWise 2012 POA - Sales.Provo2	
Status Configuration Environment Log Files Scheduled Events MTP Status Help	
OS Data	
Windows Version 6.1 (Build 7601)Service Pack 1	
Process ID	2728
Build Dates	
GroupWise Agent Build Version	12.0.0-98210
GroupWise Agent Build Date	11-29-11
GroupWise Engine Build Date	11-29-11
GroupWise Resource Build Date	11-29-11

Viewing and Searching POA Log Files

On the POA Web console menu, click *Log Files* to display and search POA log files.

Event logs		
<input type="checkbox"/>	Select all	
<input type="checkbox"/>	1101poa.001	11-02-11 00:00:01 0008189
<input type="checkbox"/>	1102poa.001	11-02-11 20:09:44 0009961
<input type="checkbox"/>	1107poa.001	11-07-11 15:17:28 0010051
<input type="checkbox"/>	1107poa.002	11-07-11 15:17:43 0009966
<input type="checkbox"/>	1107poa.003	11-08-11 00:00:01 0009719
<input type="checkbox"/>	1108poa.001	11-09-11 00:00:01 0008711
<input type="checkbox"/>	1109poa.001	11-10-11 00:00:01 0008268
<input type="checkbox"/>	1110poa.001	11-11-11 00:00:01 0008268
<input type="checkbox"/>	1111poa.001	11-12-11 00:00:01 0008269
<input type="checkbox"/>	1112poa.001	11-13-11 00:00:01 0008269
<input type="checkbox"/>	1113poa.001	11-14-11 00:00:01 0008269
<input type="checkbox"/>	1114poa.001	11-15-11 00:00:01 0008269
<input type="checkbox"/>	1115poa.001	11-16-11 00:00:01 0008269
<input type="checkbox"/>	1116poa.001	11-17-11 00:00:01 0008270
<input type="checkbox"/>	1117poa.001	11-17-11 12:52:22 0009823

To view a particular log file, select the log file, then click *View Events*.

To search all log files for a particular string, type the string in the *Events Containing* field, select *Select All*, then click *View Events*. You can also manually select multiple log files to search.

The results of the search are displayed on a separate page that can be printed.

Listing POA Scheduled Events

On the POA Web console menu, click *Scheduled Events* to view currently scheduled events and their status information.

GroupWise 2012 POA - Development.Provo1	
Status	Configuration
Environment	Log Files
Scheduled Events	MTP Status
Help	
GroupWise POA Scheduled Events	
DiskCheck	
Event Current Status	Idle
Event Next Start Time	12/01/2011 17:49:02
Event Schedule Interval	5 mins
# of Concurrent Events Allowed	1
QuickFinder Indexing	
Event Current Status	Idle
Event Next Start Time	12/01/2011 20:00:00
Event Schedule Interval	24 hour(s)
# of Concurrent Events Allowed	1
Remote Downloadable Address Book Generation	
Event Current Status	Idle
Event Next Start Time	12/02/2011 00:00:30
Event Schedule Interval	1 day(s)
# of Concurrent Events Allowed	1
Nightly User DB Upkeep (Phase 1)	
Event Current Status	Idle
Event Next Start Time	12/02/2011 00:00:30
Event Schedule Interval	1 day(s)
# of Concurrent Events Allowed	1

QuickFinder indexing and remote downloadable Address Book generation can be controlled using links from the Configuration page, if the POA Web console is password protected as described in [Section 37.2.1, "Setting Up the POA Web Console," on page 540](#). The Configuration page also displays information about disk check events and database maintenance events. However, scheduled events must be created and modified using ConsoleOne.

Checking Link Status to the MTA

On the POA Web console menu, click *MTP Status* to view status information about the link between the POA for the post office and MTA for the domain.

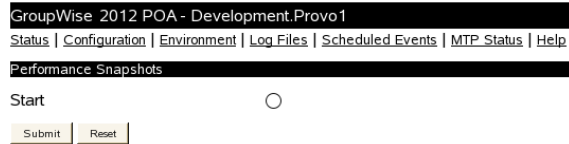
GroupWise 2012 POA - Development.Provo1		
Status	Configuration	
Environment	Log Files	
Scheduled Events	MTP Status	
Help		
Message Transfer Status		
	Send	Receive
Current Status	Open	Open
Last Closed		
Last Opened	11-28-11 19:18:58	11-28-11 19:18:58
Last Closure Reason		
Directory Paths and TCP/IP addresses		
Outbound TCP/IP	172.15.7.17:7100	
Inbound TCP/IP	172.15.7.17:7101	
Hold	/gwssystem/dev/wpcsin	
Message Transfer Statistics		
Written	7	
Read	20	

If the POA Web console is password protected as described in [Section 37.2.1, "Setting Up the POA Web Console," on page 540](#), the *Outbound TCP/IP* link displays the MTA Web console where you can get status information about the MTA. The *Hold* link displays the contents of the MTA input queue, so you can find out if messages are waiting for processing by the MTA.

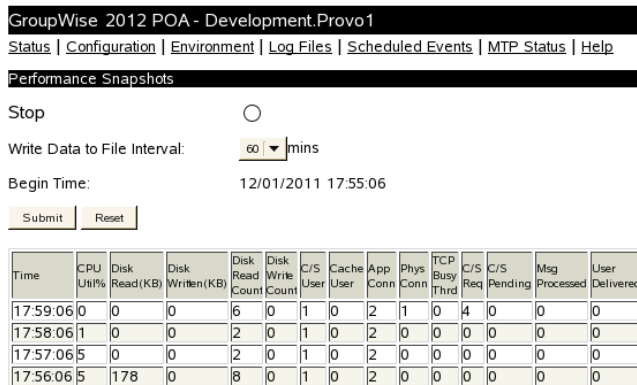
Taking Performance Snapshots

To help you assess the efficiency of the POA, you can configure the POA to gather statistics about CPU utilization, disk reads and writes, thread usage, message processing, and so on.

- 1 Make sure that the [POA Web console](#) is password protected, as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540.
- 2 In the POA Web console, on the Configuration page, click *Performance Snapshots* under the *Performance Settings* heading.



- 3 Select *Start*, then click *Submit*.



The POA takes a snapshot every 60 seconds.

- 4 Refresh your browser window to display data as it is collected.
- 5 Specify the interval at which you want to write data to a file on disk for permanent storage.

Performance data is saved to the `mmdsnap.nnn` file, where `mmd` represents the current month and date and `nnn` starts with 001 and increments each time you enable performance snapshots to start gathering data. The performance data file is stored in the `post_office\oftemp` directory in comma-separated value (CSV) format, so that you can bring the data into a spreadsheet program for analysis.

- 6 When you have gathered sufficient performance data, select *Stop*, then click *Submit*.

Because gathering performance data uses POA resources, you should turn the feature off when you have gathered sufficient data. It is turned off automatically when you restart the POA.

- 7 When you are finished using performance data files, delete them to conserve disk space.

The POA does not automatically clean up old performance data files.

Monitoring SOAP Events

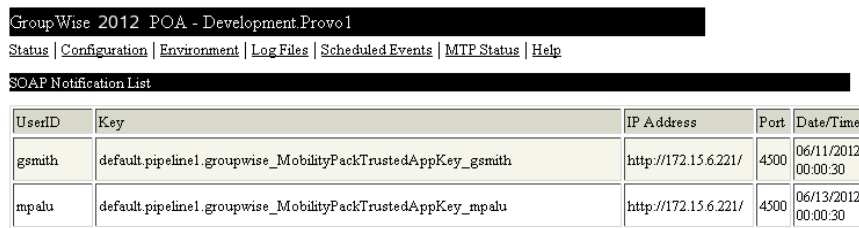
To help you work with third-party listener applications such as the Data Synchronizer Connector for GroupWise, the POA Web console lists SOAP notifications and SOAP events so that you can monitor the SOAP event traffic through the POA. These options are available if the POA Web console is password protected, as described in [Section 37.2.1, “Setting Up the POA Web Console,” on page 540](#).

- ♦ “[Listing SOAP Notifications](#)” on page 547
- ♦ “[Listing SOAP Event Configurations](#)” on page 548

Listing SOAP Notifications

The SOAP Notification List page shows the third-party listener applications that are notified by the POA when SOAP events occur.

- 1 On the Configuration page, click *SOAP Notification List*.



UserID	Key	IP Address	Port	Date/Time
gsmith	default.pipeline1.groupwise_MobilityPackTrustedAppKey_gsmith	http://172.15.6.221/	4500	06/11/2012 00:00:30
mpahu	default.pipeline1.groupwise_MobilityPackTrustedAppKey_mpahu	http://172.15.6.221/	4500	06/13/2012 00:00:30

The columns provide the following information:

User: Displays the name of the GroupWise user that is performing the event.

Key: Displays the ID of the event configuration created by the third-party application. The event configuration describes the events that are being tracked for the user, such as creation, deletion, or modification of records.

IP Address: Displays the IP address of the POA where the event took place.

Port: Displays the port number used for communication between the POA and the listener application.

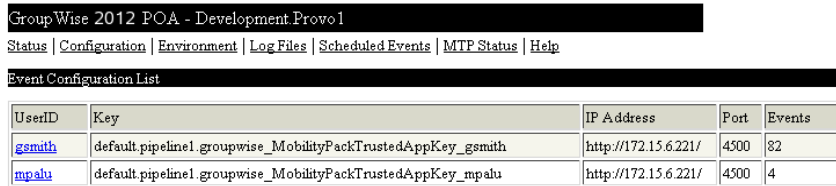
Date/Time: Displays the date and time when the event took place. An asterisk (*) after the date and time indicates that the user has pending notifications. After the notifications have been sent, the asterisk is removed.

Listing SOAP Event Configurations

The Event Configuration List page displays the event configurations that are registered to receive GroupWise events from the POA. An event configuration is listed when an external application such as the Novell Data Synchronizer Connector for GroupWise communicates with the POA and provides information about a specific type of event that it wants to receive.

For example, the Data Synchronizer Connector for Mobility works through the GroupWise Connector to synchronize GroupWise data to mobile devices. Whenever a user connects a mobile device to GroupWise through the Mobility Connector, an event configuration is created for that user and his or her mobile device. If the user has multiple mobile devices, there is an event configuration for each of the user's mobile devices.

- 1 On the Configuration page, click *Event Configuration List*.



UserID	Key	IP Address	Port	Events
gsmith	default.pipeline1.groupwise_MobilityPackTrustedAppKey_gsmith	http://172.15.6.221/	4500	82
mpalu	default.pipeline1.groupwise_MobilityPackTrustedAppKey_mpalu	http://172.15.6.221/	4500	4

The columns provide the following information:

UserID: Displays the name of the GroupWise user associated with the event configuration.

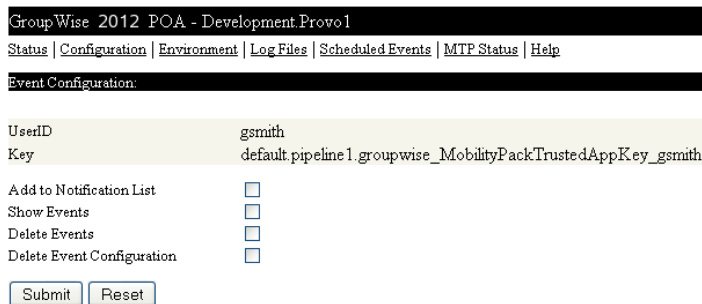
Key: Displays the ID of the event configuration created by the external application. For example, the GroupWise Connector uses a GroupWise trusted application key.

IP Address: Displays the IP address of the external application that the POA notifies when events take place.

Port: Displays the port number used for communication between the POA and the external application.

Events: Displays the number of events that have transferred from the POA to the external application.

- 2 To manage the event configuration for a specific user, click the user name.



GroupWise 2012 POA - Development.Prov01

[Status](#) | [Configuration](#) | [Environment](#) | [Log Files](#) | [Scheduled Events](#) | [MTP Status](#) | [Help](#)

Event Configuration:

UserID	gsmith
Key	default.pipeline1.groupwise_MobilityPackTrustedAppKey_gsmith

Add to Notification List

Show Events

Delete Events

Delete Event Configuration

The Event Configuration page helps you manage an event configuration and the associated events that are stored in a user's database for an external application such as the Data Synchronizer Connector for GroupWise.

- 3 Select *Add to Notification List*, then click *Submit* to cause the POA to notify the external application whenever a new GroupWise event needs to be picked up.
- 4 Select *Show Events*, then click *Submit* to display the currently stored events for the event configuration.

If the list is long, the external application might not be running.

- 5 Select *Delete Events*, then click *Submit* to delete any stored events for the event configuration.

Use this option only when a backlog of events needs to be cleared, such as when a problem occurred with the external application.

- 6 Click *Delete Event Configuration*, then click *Submit* to delete the displayed event configuration.

Use this option when the POA no longer needs to send events for the user associated with the event configuration. For example, if there was a problem removing a user from the GroupWise Connector, use this option to remove any residual events associated with the user.

37.2.4 Controlling the POA from the POA Web Console

At the POA Web console, you can change some POA configuration settings for the current POA session. You can also stop and start some specific POA threads.

IMPORTANT: In order to control the POA from the POA Web console, you must set up authentication for the POA Web console, as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540.

- ◆ [“Changing POA Configuration Settings”](#) on page 549
- ◆ [“Controlling the POA Admin Thread”](#) on page 550
- ◆ [“Controlling the POA MTP Threads”](#) on page 550
- ◆ [“Disconnecting a User Session from the POA”](#) on page 551

Changing POA Configuration Settings

On the POA Web console menu, click *Configuration*. Online help on the Configuration page helps you interpret the configuration information being displayed.

GroupWise 2012 POA - Development.Provo1	
Status Configuration Environment Log Files Scheduled Events MTP Status Help	
GroupWise POA Configuration Settings	
General Settings:	
Post Office Directory:	/gwsystem/dev
Post Office Access Mode:	Client/Server Only
Post Office Configuration Instance:	poa
Post Office Language:	en
Database Version:	12
Internet Domain Name:	yourcompanyname.com
Read Configuration from Database:	Yes
Error Mail to Administrator:	Yes
IPv6 Protocol:	Enabled
IP Address Redirection Table:	Show
QuickFinder Indexing:	Enabled
QuickFinder Document Converter Agent:	Started
QuickFinder Indexing Base Offset (hours from Midnight):	20 Hours 0 Mins (Default)
QuickFinder Indexing Interval:	24 Hours 0 Mins (Default)
Quarantine Files That Fail in Document Conversion:	Disabled
Simple Network Management Protocol (SNMP):	Disabled
Admin Task Processing:	Yes
Intruder Detection:	Enabled
Incorrect Login Attempts before Lockout:	5
Login Attempt Reset Interval:	30 mins
Intruder Lockout Reset Interval:	30 mins
GWCheck Processing:	Enabled
Post Office Security Requires Password:	Yes
LDAP Authentication:	Enabled
Move User (live) via TCP/IP:	Enabled
Startup File:	

If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540, you can click hyperlinked configuration items to change settings for the current agent session. The settings that can be modified are much the same as those that can be changed at the POA server console, as described in [Section 37.1.2, “Controlling the POA from the POA Server Console,”](#) on page 529.

Controlling the POA Admin Thread

On the Configuration page, click *Admin Task Processing*.

The screenshot shows the 'Admin Task Status' configuration page. At the top, there is a navigation bar with links: Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help. Below this is a section titled 'Admin Task Status'. It contains several sections: 'Admin Messages' with a table showing 'Completed' (14), 'Errors' (0), and 'In Queue' (0), and a 'Send Admin Mail' checkbox which is checked. The 'Admin Database' section includes 'Status' (Normal), 'DB Sort Language' (EN), 'Recovery Count' (0), and 'Automatic Recovery' (checked). The 'Admin Thread' section shows 'Status' (Running) and 'Suspend'/'Resume' radio buttons, both of which are currently unselected. At the bottom, there are 'Submit' and 'Reset' buttons.

Modify the functioning of the POA admin thread as needed, then click *Submit*. The changes remain in effect for the current POA session.

Controlling the POA MTP Threads

On the Configuration page, click *Message Transfer Protocol*.

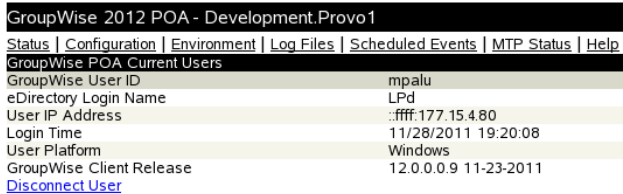
The screenshot shows the 'Message Transfer Protocol Settings' configuration page. It features a navigation bar with links: Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help. The main section is titled 'Message Transfer Protocol Settings'. It includes 'Outbound TCP/IP' settings with 'Address' (172.15.7.17) and 'Port' (7100) fields. Below that are 'Inbound TCP/IP' settings with 'Address' (172.15.7.17) and 'Port' (7101) fields. The 'Maximum File Transfer Send Size' is set to 0 MB. A 'Restart MTP' radio button is unselected. 'Submit' and 'Reset' buttons are at the bottom.

On this page, you can restart MTA processing between the POA and the MTA. On the MTP status page, you can restart the send and receive threads separately.

Disconnecting a User Session from the POA

In Online mode, the GroupWise Windows client establishes an active session with the POA. If you disable a user, as described in [Section 14.9, “Disabling and Enabling GroupWise Accounts,” on page 254](#) while the user is logged in, it does not terminate the user’s live session with the POA. Instead of needing to restart the POA to terminate the user’s live session, you can disconnect the user in the POA Web console after disabling the user in ConsoleOne.

On the Status page in the POA Web console, click *C/S Users*, then click *Disconnect User* for the user that you have already disabled in ConsoleOne.



The screenshot shows the POA Web console interface. At the top, there is a navigation bar with links for Status, Configuration, Environment, Log Files, Scheduled Events, MTP Status, and Help. Below this is a section titled "GroupWise POA Current Users". A table displays details for a user named "mpalu":

GroupWise User ID	mpalu
eDirectory Login Name	LPd
User IP Address	::ffff:177.15.4.80
Login Time	11/28/2011 19:20:08
User Platform	Windows
GroupWise Client Release	12.0.0.0.9 11-23-2011

At the bottom of the table, there is a blue link labeled "Disconnect User".

IMPORTANT: When you disable the user in ConsoleOne, the POA must receive the disable event and process it before the user can be disconnected in the POA Web console. If you are running the POA server console, you can see the disable event occur in the Log Message box. When you click *Disconnect User* successfully, the user is no longer listed in the POA Web console. If the user does not disappear from the list after you click *Disconnect User*, wait for the POA to process the disable event, then click *Disconnect User* again. A disconnected user receives an error message stating that GroupWise will exit.

37.3 Using POA Log Files

Error messages and other information about POA functioning are written to log files as well as displaying on the POA server console. Log files can provide a wealth of information for resolving problems with POA functioning or message flow. This section covers the following subjects to help you get the most from POA log files:

- ◆ [Section 37.3.1, “Locating POA Log Files,” on page 551](#)
- ◆ [Section 37.3.2, “Configuring POA Log Settings and Switches,” on page 552](#)
- ◆ [Section 37.3.3, “Viewing POA Log Files,” on page 552](#)
- ◆ [Section 37.3.4, “Interpreting POA Log File Information,” on page 552](#)

37.3.1 Locating POA Log Files

The default location of the POA log files varies by platform:

Linux: `/var/log/novell/groupwise/post_office_name.poa`

Windows: `post_office\wpcsout\ofs`

You can change the location where the POA creates its log files, as described in [Configuring POA Log Settings and Switches](#).

37.3.2 Configuring POA Log Settings and Switches

The following aspects of logging are configurable:

- ♦ Log File Path (`--log`)
- ♦ Disk Logging (`--logdiskoff`)
- ♦ Logging Level (`--loglevel`)
- ♦ Maximum Log File Age (`--logdays`)
- ♦ Maximum Log File Size (`--logmax`)

You can configure the log settings in the following ways:

- ♦ Using ConsoleOne to establish defaults (see [Section 36.1.8, “Adjusting the POA Logging Level and Other Log Settings,”](#) on page 493)
- ♦ Using startup switches to override ConsoleOne settings (see [Section 40, “Using POA Startup Switches,”](#) on page 581)
- ♦ Using the POA server console to override log settings for the current POA session (see [“Adjusting POA Log Settings”](#) on page 538)
- ♦ Using the POA Web console to override other settings for the current POA session (see [Section 37.2.4, “Controlling the POA from the POA Web Console,”](#) on page 549)

37.3.3 Viewing POA Log Files

You can view the contents of the POA log file from the POA server console and POA Web console. See the tasks presented in [Section 37.1.1, “Monitoring the POA from the POA Server Console,”](#) on page 525:

- ♦ [“Browsing the Current POA Log File”](#) on page 537
- ♦ [“Viewing a Selected POA Log File”](#) on page 537
- ♦ [“Cycling the POA Log File”](#) on page 538
- ♦ [“Viewing and Searching POA Log Files”](#) on page 544

On Linux, you can use the `tail` command to monitor a file named `poa.currentlog`, where `poa` is the name of the POA eDirectory object. This file is a symbolic link to the current POA log file, so that you do not need to keep track of the exact POA log file name, which includes the log file creation date and an incrementing extension for multiple log files created on the same date.

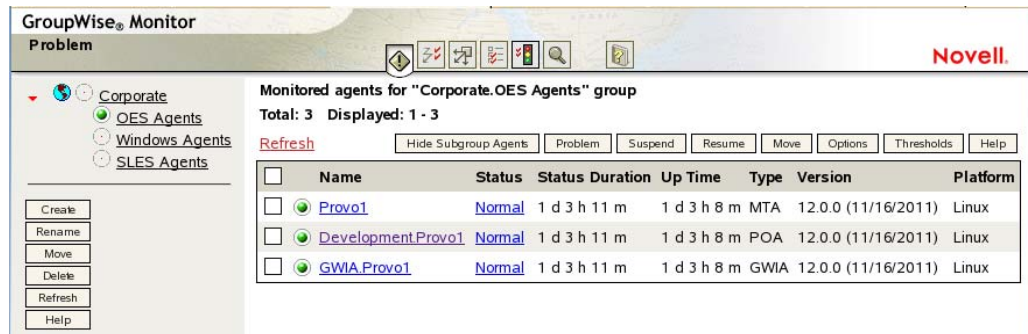
37.3.4 Interpreting POA Log File Information

On startup, the POA records the POA settings currently in effect. Thereafter, it logs events that take place, including errors. To look up error messages that appear in POA log files, see [“Post Office Agent Error Messages”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

Because the POA consists of multiple threads, you might find it useful to retrieve the log file into an editor and sort it on the thread ID that follows the date and time information. Sorting groups all messages together for the same POA thread. You can also use the search capability of the POA Web console to gather information about a specific POA thread. See [“Viewing and Searching POA Log Files”](#) on page 544.

37.4 Using GroupWise Monitor

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents and gateways from any location where you are connected to the Internet and have access to a Web browser. The POA Web console can be accessed from GroupWise Monitor, enabling you to monitor all POAs in your GroupWise system from one convenient location. In addition, GroupWise Monitor can notify you when agent problems arise.



For installation and setup instructions, see “Installing GroupWise Monitor” in the *GroupWise 2012 Installation Guide*. For usage instructions, see Part XV, “Monitor,” on page 939.

37.5 Using Novell Remote Manager

If the POA is running on Novell Open Enterprise Server (OES), you can use Novell Remote Manager to monitor the POA. For more information, see the *Novell Remote Manager for Linux Administration Guide* for your version of OES Linux (<http://www.novell.com/documentation/oes.html>).

37.6 Using an SNMP Management Console

You can monitor the POA from SNMP management and monitoring programs. When properly configured, the POA sends SNMP traps to network management consoles for display along with other SNMP monitored programs.

Although the POA is SNMP-enabled by default, the server where the POA is installed must be properly configured to support SNMP, and the POA object in eDirectory must also be properly configured. To set up SNMP services for your server, complete the following tasks:

- ♦ [Section 37.6.1, “Setting Up SNMP Services for the POA,”](#) on page 553
- ♦ [Section 37.6.2, “Copying and Compiling the POA MIB File,”](#) on page 555
- ♦ [Section 37.6.3, “Configuring the POA for SNMP Monitoring,”](#) on page 556

37.6.1 Setting Up SNMP Services for the POA

Select the instructions for the platform where the POA runs:

- ♦ [“Linux: Setting Up SNMP Services for the POA”](#) on page 554
- ♦ [“Windows: Setting Up SNMP Services for the POA”](#) on page 554

Linux: Setting Up SNMP Services for the POA

The Linux POA is compatible with NET-SNMP. An older version of SNMP called UCD-SNMP cannot be used with the Linux POA. NET-SNMP comes with OES Linux, but it does not come with SLES. If you are using SLES, you must update to NET-SNMP in order to use SNMP to monitor the Linux POA.

- 1 Make sure you are logged in as root.
- 2 If NET-SNMP is not already set up on your Linux server, use the following command to configure SNMP:

```
snmpconf -g basic_setup
```

The `snmpconf` command creates the `snmpd.conf` file in one of the following directories, depending on your version of Linux:

```
/usr/share/snmp  
/usr/local/share/snmp  
~/.snmp
```

- 3 Locate the `snmpd.conf` file on your Linux server.
- 4 In a text editor, open the `snmpd.conf` file and add the following line:

```
dlmod Gwsnmp /opt/novell/groupwise/agents/lib/libgwsnmp.so
```
- 5 Save the `snmpd.conf` file and exit the text editor.
- 6 Restart the SNMP daemon (`snmpd`) to put the changes into effect.

IMPORTANT: Make sure that the SNMP daemon always starts before the POA starts.

- 7 Skip to [Section 37.6.2, “Copying and Compiling the POA MIB File,”](#) on page 555.

Windows: Setting Up SNMP Services for the POA

SNMP support is provided for up to eight Windows POAs on the same Windows server. Upon startup, each instance of the POA is dynamically assigned a row in its SNMP table. View the contents of the POA MIB for a description of the SNMP variables in the table. See [Section 37.6.2, “Copying and Compiling the POA MIB File,”](#) on page 555 for more information about MIB files.

On Windows Server 2008, the SNMP Service is usually not included during the initial operating system installation. The SNMP Service can be easily added at any time. To add or configure the SNMP Service, you must be logged in as a member of the Administrator group.

To set up SNMP services for the Windows POA, complete the following tasks:

- ♦ [“Installing SNMP Support on Windows Server 2008”](#) on page 554
- ♦ [“Installing SNMP Support on Windows Server 2003”](#) on page 555
- ♦ [“Installing GroupWise Agent SNMP Support”](#) on page 555

Installing SNMP Support on Windows Server 2008

- 1 In the Control Panel, click *Programs and Features*.
- 2 Click *Turn Windows features on or off* to open the Server Manager.
- 3 Click *Features > Add Features*.
- 4 In the *Features* list, expand *SNMP Services*, then select *SNMP Service*.
- 5 Click *Next*, then click *Install*.

- 6 When the installation is finished, click *Close*, then exit the Server Manager.
- 7 Skip to [Installing GroupWise Agent SNMP Support](#).

Installing SNMP Support on Windows Server 2003

- 1 Click *Start > Control Panel > Add or Remove Programs*.
- 2 Click *Add/Remove Windows Components*.
- 3 Select *Management and Monitoring Tools*.
- 4 Click *Details*, then select *Simple Network Management Protocol*.
- 5 Follow the on-screen instructions to install the SNMP Service.
- 6 Continue with [Installing GroupWise Agent SNMP Support](#).

Installing GroupWise Agent SNMP Support

The GroupWise Agent Installation program includes an option for installing SNMP support. However, if the server where you installed the agents did not yet have SNMP set up, that installation option was not available. Now that you have set up SNMP, you can install GroupWise agent SNMP support.

At the Windows server where you want to install the GroupWise agent SNMP support:

- 1 Run *setup.exe* at the root of the downloaded *GroupWise 2012* software image.
- 2 Click *Install GroupWise System*, click *Yes* to accept the License Agreement, then click *Next* to perform a standard installation.
- 3 Select *Install individual components*, deselect *GroupWise Administration*, then click *Next*.
- 4 On the Installation Path page, browse to and select the path where the agent software is installed, then select *Install and Configure SNMP for GroupWise Agents*.
- 5 Continue through the rest of the installation process as prompted by the Agent Installation program.

The Agent Installation program copies the SNMP support files to the agent installation directory, makes the appropriate Windows registry entries, and restarts the Windows SNMP service.

- 6 Continue with [Copying and Compiling the POA MIB File](#).

37.6.2 Copying and Compiling the POA MIB File

An SNMP-enabled POA returns information contained in a Management Information Base (MIB). The MIB is an ASCII data structure that defines the information gathered. It also defines the properties that can be monitored and managed on the SNMP-enabled POA.

Before you can monitor an SNMP-enabled POA, you must compile the `gwpoa.mib` file using your SNMP management program. GroupWise agent MIB files are located in the `/agents/snmpmibs` directory of your GroupWise software distribution directory or the downloaded *GroupWise 2012* software image.

The MIB file contains all the Trap, Set, and Get variables used for communication between the POA and management console. The Trap variables provide warnings that point to current and potential problems. The Set variables allow you to configure portions of the application while it is still running. The Get variables display the current status of different processes of the application.

- 1 Copy the `gwpoa.mib` file to the location required by your SNMP management program.
- 2 Compile or import the `gwpoa.mib` file as required by your SNMP management program.
- 3 Continue with [Configuring the POA for SNMP Monitoring](#).

37.6.3 Configuring the POA for SNMP Monitoring

In order for SNMP monitoring programs to monitor the POA, the POA must be configured with a network address and SNMP community string.

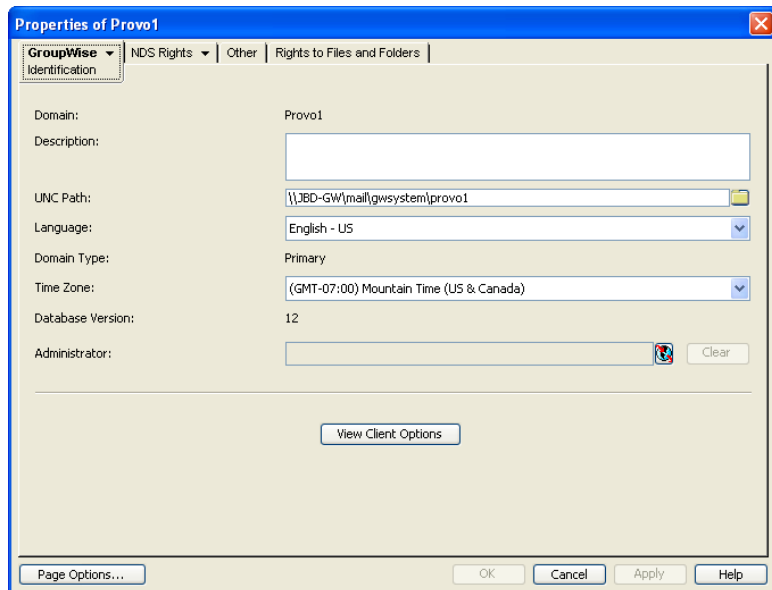
- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.
- 3 Click the pencil icon to provide the TCP/IP address of the server where the POA runs, then click *Apply*.
- 4 Click *GroupWise > Agent Settings*, then scroll to the bottom of the settings list.
- 5 Provide your system SNMP community GET string, then click *OK*.
- 6 Configure the SNMP Service with the same community GET string:
 - 6a On the Windows desktop, click *Start > Administrator Tools > Services*.
 - 6b Right-click *SNMP Service*, then click *Properties*.
 - 6c Click *Security*, then click *Add* in the *Accepted community names* list.
 - 6d In the *Community Name* field, specify your system SNMP community GET string.
 - 6e In the *Community Rights* drop-down list, select *READ WRITE*.
 - 6f Click *Add* to add the community string to the list, then click *OK* to close the SNMP Properties page.
- 7 Restart the POA.

The POA should now be visible to your SNMP monitoring program.

37.7 Notifying the GroupWise Administrator

If you want to be notified with an email message whenever POAs encounter critical errors, you can designate yourself as an administrator of the domain where the post offices are located.

- 1 In ConsoleOne, browse to and right-click the Domain object, then click *Properties* to display the Identification page.



- 2 In the *Administrator* field, browse to and select your GroupWise user ID.

A domain can have a single administrator, or you can create a group of users to function as administrators.

- 3 Click *OK* to save the administrator information.

The selected user or group then begins receiving email messages whenever POAs servicing post offices in the domain encounter critical errors.

Corresponding Startup Switches: By default, the POA generates error mail if an administrator has been assigned for the domain. Error mail can be turned off using the `--noerrormail` switch in the POA startup file.

POA Web Console: Another way to receive email notification of POA problems is to use GroupWise Monitor to access the POA Web console. See [Section 69.5.1, "Configuring Email Notification,"](#) on page 957.

37.8 Using the POA Error Message Documentation

POA error messages are documented with the source and explanation of the error, possible causes of the error, and actions to take to resolve the error. See ["Post Office Agent Error Messages"](#) in *GroupWise 2012 Troubleshooting 1: Error Messages*.

37.9 Employing POA Troubleshooting Techniques

If you are having a problem with the POA but are not receiving a specific error message, or if the suggested actions for the specific error did not resolve the problem, you can review more general troubleshooting strategies for dealing with POA problems. See [“Strategies for Agent Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

37.10 Using Platform-Specific POA Monitoring Tools

Each supported operating system for the GroupWise POA provides tools for monitoring programs.

Linux: You can use SNMP tools like `snmpget` and `snmpwalk` that allow you to retrieve the data about all the services registered with the SNMP service. These tools are part of the NET-SNMP package. See your Linux documentation for additional monitoring suggestions.

Windows: You can use the Performance Monitor in Windows Administrator Tools to gather similar information. See your Windows documentation for additional monitoring suggestions.

38 Optimizing the POA

You can adjust how the POA functions to optimize its performance. Before attempting optimization, you should run the POA long enough to observe its efficiency and its impact on other network applications running on the same server. See [Chapter 37, “Monitoring the POA,” on page 525](#).

Also, remember that optimizing your network hardware and operating system can make a difference in POA performance.

The following topics help you optimize the POA:

- ♦ [Section 38.1, “Optimizing Client/Server Processing,” on page 559](#)
- ♦ [Section 38.2, “Optimizing Message File Processing,” on page 564](#)
- ♦ [Section 38.3, “Optimizing Thread Management,” on page 566](#)
- ♦ [Section 38.4, “Optimizing Database Maintenance,” on page 567](#)
- ♦ [Section 38.5, “Optimizing Client Purge Operations,” on page 570](#)
- ♦ [Section 38.6, “Optimizing Calendar Publishing,” on page 571](#)

38.1 Optimizing Client/Server Processing

If you run only one POA for the post office, you can adjust the number of POA threads and connections for client/server processing. If client/server processing needs are extremely heavy for a post office, you can set up a dedicated client/server POA to meet those needs.

- ♦ [Section 38.1.1, “Adjusting the Number of POA Threads for Client/Server Processing,” on page 559](#)
- ♦ [Section 38.1.2, “Adjusting the Number of Connections for Client/Server Processing,” on page 561](#)
- ♦ [Section 38.1.3, “Configuring a Dedicated Client/Server POA \(Windows Only\),” on page 562](#)

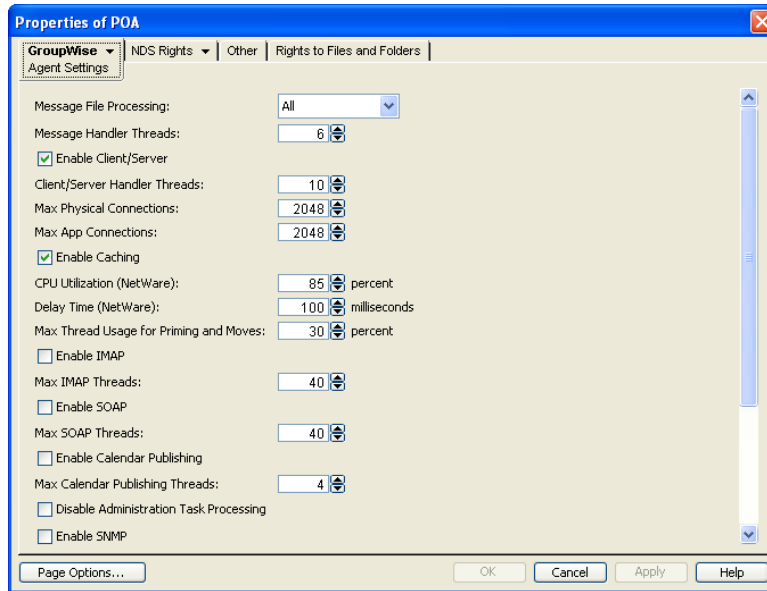
38.1.1 Adjusting the Number of POA Threads for Client/Server Processing

If the POA is configured with client/server processing enabled, it starts client/server handler threads to respond to current client/server requests, up to the number of threads specified by the *Client/Server Handler Threads* option. To respond to occasional heavy loads, the POA can increase the number of client/server handler threads above the specified amount if CPU utilization is below the threshold established by the *CPU Utilization* setting. When the POA rereads its configuration information, the number of client/server handler threads drops back within the configured limit. You can determine how often this happens by checking the Client/Server Pending Requests History page at the POA Web console.

If the POA is frequently not keeping up with the client/server requests from GroupWise client users, you can increase the maximum number of client/server handler threads so the POA can create additional threads as needed. The default is 10 client/server handler threads; valid values range from 1 to 99.

If GroupWise client users cannot connect to the POA immediately or if response is sluggish, you can increase the number of threads.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 3 Increase the number in the *Client/Server Handler Threads* field to increase the maximum number of threads the POA can create for client/server processing.

The optimum number of threads for a POA is affected by many factors, including available system resources, number of users in Caching mode, number of users priming Caching mailboxes, and so on.

Plan on at least one client/server handler thread per 20-30 client/server users. Or, you can increase the number of client/server handler threads in increments of three to five threads until acceptable throughput is reached. Another approach is to set the value high initially and then monitor thread usage with the *C/S Handler Threads* link on the [Status](#) page of the POA Web console. If some of the threads always have a count of 0 (zero), meaning they are never used, you can decrease the number of client/server handler threads accordingly.

- 4 Click *OK* to save the new thread setting.

ConsoleOne then notifies the POA to restart so the new thread setting can be put into effect.

Corresponding Startup Switches: You can also use the `--tcpthreads` switch in the POA startup file to adjust the number of POA client/server handler threads.

POA Web Console: The [Status](#) page helps you assess whether the POA is currently meeting the client/server needs of the post office. Under the *Thread Status* heading, click *C/S Handler Threads* to display the workload and status of the client/server handler threads.

If the POA Web console is password protected as described in [Section 37.2.1, "Setting Up the POA Web Console,"](#) on page 540, you can change the number of client/server handler threads on the [Configuration](#) page. Under *Performance Settings*, click *C/S Handler Threads*.

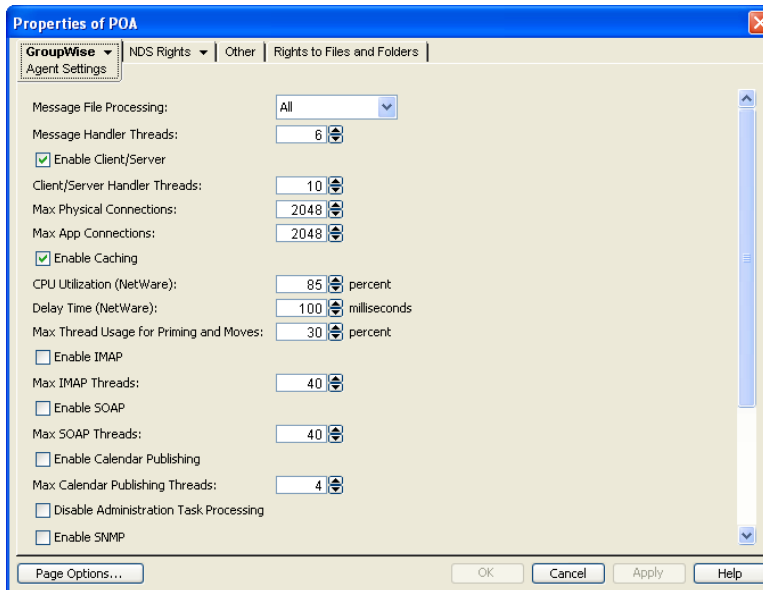
38.1.2 Adjusting the Number of Connections for Client/Server Processing

Connections are the number of “sockets” through which client/server requests are communicated from the GroupWise client to the POA.

- ♦ **Application connections:** Each GroupWise user uses one application connection when he or she starts GroupWise. Depending on what activities the user is doing in the GroupWise client, additional application connections are used. For example, the GroupWise Address Book and GroupWise Notify use individual application connections. The default maximum number of application connections is 2048. You should plan about 3 to 4 application connections per user, so the default is appropriate for a post office of about 500 users.
- ♦ **Physical connections:** Each GroupWise user could have zero or multiple active physical connections. One physical connection can accommodate multiple application connections. Inactive physical connections periodically time out and are then closed by the clients and the POA. The default maximum number of physical connections is 2048. You should plan about 1 to 2 physical connections per user, so the default is appropriate for a post office of about 500 users.

If the POA is configured with too few connections to accommodate the number of users in the post office, the POA can encounter an error condition such as “[GWPOA: Application connection table full](#)”.

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 3 Increase the number in the *Max Physical Connections* field to increase the amount of TCP/IP traffic the POA can accommodate.
- 4 Increase the number in the *Max App Connections* field to increase the number of activities the attached users can perform concurrently.
- 5 Click *OK* to save the new connection settings.

ConsoleOne then notifies the POA to restart so the new connection settings can be put into effect.

Corresponding Startup Switches: You can also use the `--maxappconns` and `--maxphysconns` switches in the POA startup file to adjust the POA client/server processing.

POA Web Console: The [Status](#) page helps you assess whether the POA is currently meeting the client/server needs of the post office. Under the *Statistics* heading, click *C/S Requests Pending*. You can also manually select multiple log files to search in order to display a history of times during the last 24 hours when the POA was unable to respond immediately to client/server requests.

38.1.3 Configuring a Dedicated Client/Server POA (Windows Only)

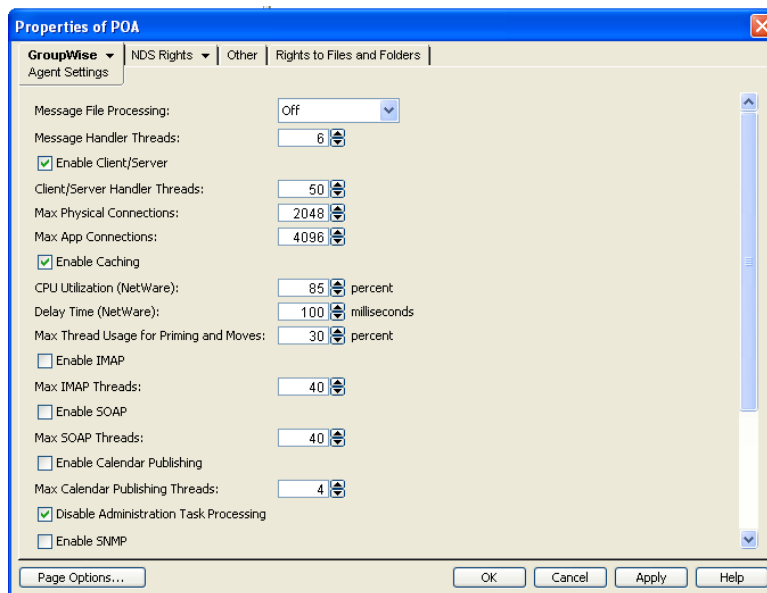
NOTE: The powerful multi-threaded processing capabilities of Linux make multiple POAs unnecessary on that operating system.

When GroupWise users access the post office in client/server mode, the responsiveness of the GroupWise client depends entirely on the ability of the POA to handle the load placed upon it by the users. When you configure a dedicated client/server POA, GroupWise client users do not compete with other POA activities.

Because many POA functions are disabled when a POA is dedicated to client/server processing, you must run at least one other POA for the post office to take care of the POA functions that the dedicated client/server POA is not performing. This additional POA could be a multipurpose POA, or you could configure additional POAs dedicated to specific types of processing.

To configure a dedicated client/server POA:

- 1 Create a new POA object for the post office as described in [Section 36.1.1, “Creating a POA Object in eDirectory,” on page 482](#).
- 2 Right-click the new POA object, then click *Properties*.
- 3 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 4 Make sure *Enable Client/Server* is selected.
- 5 Increase the number in the *Client/Server Handler Threads* field as needed to increase the maximum number of threads the POA can create.

The optimum number of threads for a POA is affected by many factors, including available system resources, number of users in Caching mode, number of users priming Caching mailboxes, and so on.

Plan on at least one client/server handler thread per 20-30 client/server users. Or, you can increase the number of client/server handler threads in increments of three to five threads until acceptable throughput is reached. Another approach is to set the value high initially and then monitor thread usage with the *C/S Handler Threads* link on the [Status](#) page of the POA Web console. If some of the threads always have a count of 0 (zero), meaning they are never used, you can decrease the number of client/server handler threads accordingly.

- 6 Increase the number in the *Max Physical Connections* field as needed to increase the amount of TCP/IP traffic the POA can accommodate.

Plan on one to two physical connections per user in the post office.

- 7 Increase the number in the *Max App Connections* field as needed to increase the number of activities the attached users can perform concurrently.

Plan on three to four application connections per user in the post office.

- 8 Set *Message File Processing* to *Off*. Make sure another POA handles message file processing.
- 9 Select *Disable Administration Task Processing*, so that this POA does not run an admin thread. Make sure that another POA handles administration tasks.
- 10 Click *Apply* to save the updated information on the Agent Settings page.
- 11 Click *GroupWise > QuickFinder*.
- 12 Deselect *Enable QuickFinder Indexing*, then click *Apply*. Make sure another POA handles indexing.
- 13 Click *GroupWise > Maintenance*.
- 14 Deselect *Enable Automatic Database Recovery*. Make sure another POA handles database recovery.
- 15 Set *Maintenance Handler Threads* to 0 (zero). Make sure another POA handles database maintenance and disk space management.
- 16 Deselect *Perform User Upkeep* and deselect *Generate Address Book for Remote*. Make sure another POA handles these tasks.
- 17 Click *OK* to save the new settings for dedicated client/server processing.
- 18 Install the POA software on a *different* server from where the original POA for the post office is already running. See “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.
- 19 Add the `--name` switch to the POA startup file and specify the name designated when you created the new POA object.
- 20 For the original POA:
 - 20a Add the `--name` switch to the original POA startup file to differentiate it from the new POA you have set up.
 - 20b Deselect *Enable Client/Server* for the original POA object.
 - 20c Restart the original POA, so that it no longer performs the client/server activities you have set up a dedicated POA to perform.
- 21 Start the dedicated client/server POA.

Corresponding Startup Switches: You can also use the `--nomf`, `--noqf`, `--norecover`, `--nogwchk`, `--nonuu`, and `--nordab` switches in the POA startup file to disable non-client/server processing, then use the `--tcpthreads`, `--maxappconns`, and `--maxphysconns` switches to adjust the POA client/server processing.

38.2 Optimizing Message File Processing

If you run only one POA for the post office, you can adjust the number of POA threads for message file processing. If message file processing needs are extremely heavy for a post office, you can set up a dedicated message file processing POA to meet those needs.

- ♦ [Section 38.2.1, “Adjusting the Number of POA Threads for Message File Processing,” on page 564](#)
- ♦ [Section 38.2.2, “Configuring a Dedicated Message File Processing POA \(Windows Only\),” on page 565](#)

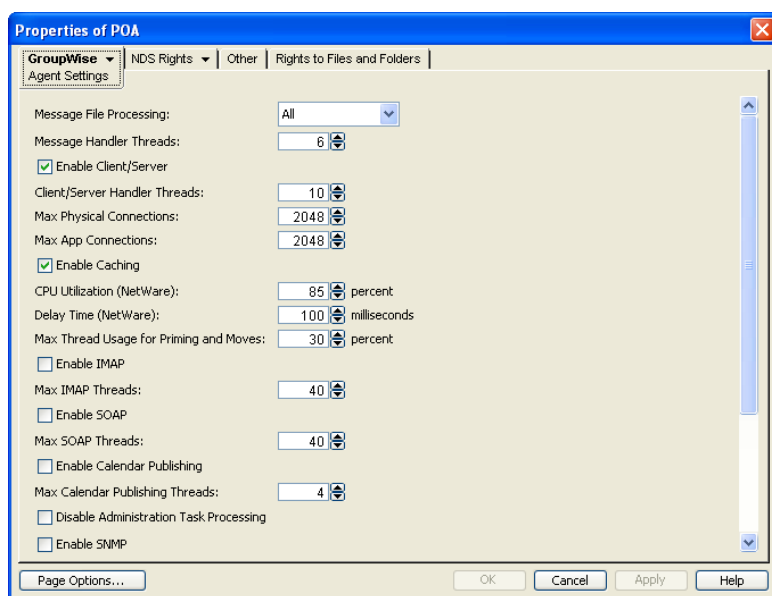
38.2.1 Adjusting the Number of POA Threads for Message File Processing

If the POA is configured for message file processing, it starts the number of threads specified by the *Message Handler Threads* option. Message handler threads deliver messages to users mailboxes. The default number of message handler threads is 6; valid values range from 1 to 20. The default value of 6 is appropriate for a multipurpose POA. The maximum value of 20 is appropriate for a POA that has been customized to process only message files.

The more message threads the POA uses, the faster it can process messages. However, the more threads the POA uses, the fewer resources are available to other processes running on the server.

To adjust the number of POA message handler threads:

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 3 Increase the number in the *Message Handler Threads* field.

For example, you could increase the number of threads in increments of three to five threads until acceptable throughput is reached. The optimum number of threads for a POA is affected by many factors, including available system resources. The more message handler threads the POA uses, the more incoming messages it can process simultaneously. However, the more threads the POA uses, the fewer threads are available to other processes running on the same server.

- 4 Click *OK* to save the new thread setting.

ConsoleOne then notifies the POA to restart so the new setting can be put into effect.

Corresponding Startup Switches: You can also use the `--threads` switch in the POA startup file to adjust the number of message handler threads.

POA Web Console: The [Status](#) page helps you assess whether the POA is currently meeting the message file processing needs of the post office. Under the *Thread Status* heading, click *Message Worker Threads* to display the workload and status of the message handler threads.

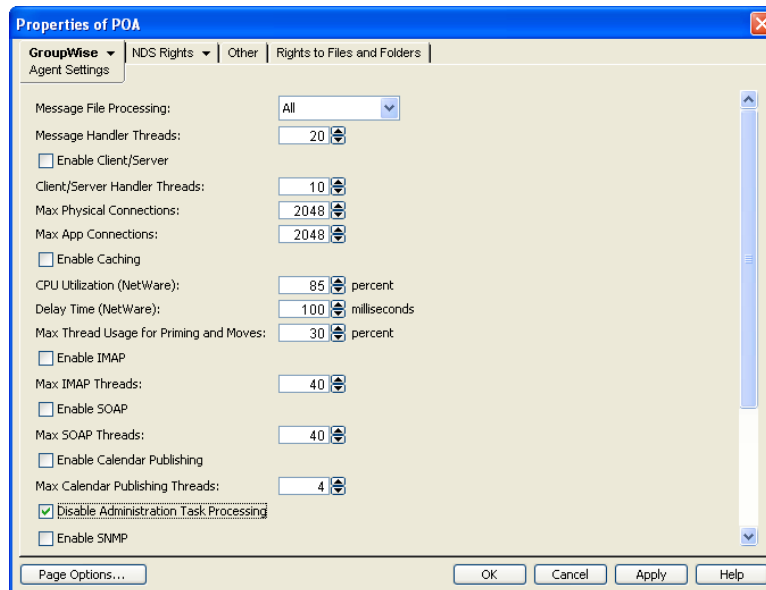
If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540, you can change the number of message handler threads on the [Configuration](#) page. Under *Performance Settings*, click *Message Worker Threads*.

38.2.2 Configuring a Dedicated Message File Processing POA (Windows Only)

NOTE: The powerful multi-threaded processing capabilities of Linux make multiple POAs unnecessary on that operating system.

If client/server processing is being handled by a dedicated client/server POA, you can set up one or more other POAs to handle other POA functions such as message file processing.

- 1 Create a new POA object for the post office as described in [Section 36.1.1, “Creating a POA Object in eDirectory,”](#) on page 482.
- 2 Right-click the new POA object, then click *Properties*.
- 3 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 4 Set *Message File Processing* to the desired level for this message file processing POA.

If you are using just one message file processing POA, set *Message File Processing* to *All*.

For additional load balancing, you could set up two message file processing POAs, one with *Message File Processing* set to *High* to promptly handle Busy Searches and requests from Remote client users, and a second with *Message File Processing* set to *Low* to handle regular message delivery in the post office.

- 5 Increase the number in the *Message Handler Threads* field as needed.
You can configure as many as 20 message handler threads. The optimum number is affected by many factors, including available system resources.
- 6 Deselect *Enable Client/Server*. Make sure another POA handles client/server processing.
- 7 Select *Disable Administration Task Processing*, so that this POA does not run an admin thread. Make sure that another POA handles administration tasks.
- 8 Click *Apply* to save the updated information on the Agent Settings page.
- 9 Click *GroupWise > QuickFinder*.
- 10 Deselect *Enable QuickFinder Indexing*, then click *Apply*. Make sure another POA handles indexing.
- 11 Click *GroupWise > Maintenance*.
- 12 Deselect *Enable Automatic Database Recovery*. Make sure another POA handles database recovery.
- 13 Set *Maintenance Handler Threads* to 0 (zero). Make sure another POA handles database maintenance and disk space management.
- 14 Deselect *Perform User Upkeep* and deselect *Generate Address Book for Remote*. Make sure another POA handles these tasks.
- 15 Click *OK* to save the new settings for dedicated message file processing.
- 16 Install the POA software on a *different* server from where the original POA for the post office is already running. See “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.
- 17 Add the `--name` switch to the POA startup file and specify the name designated when the new POA object was created.
- 18 For the original POA:
 - 18a Add the `--name` switch to the original POA startup file to differentiate it from the new POA you have set up.
 - 18b Set *Message File Processing* to *Off* for the original POA object.
 - 18c Restart the original POA, so that it no longer performs the message file processing activities you have set up a dedicated POA to perform.
- 19 Start the dedicated message file processing POA.

Corresponding Startup Switches: You can also use the `--notcpip`, `--noqf`, `--norecover`, `--nogwchk`, `--nonuu`, and `--nordab` switches in the POA startup file to disable non-message file processing, then use the `--nomfhigh` and `--nomflow` switches in the POA startup file to adjust the POA message file processing.

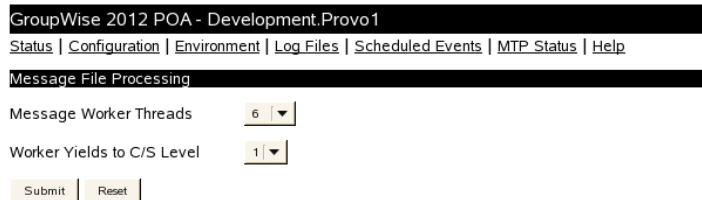
38.3 Optimizing Thread Management

The availability of client/server threads affects a GroupWise user’s experience in the GroupWise client. When the POA is working under a heavy load, users can experience degraded performance when sufficient client/server threads are not available. To maintain the best possible performance for GroupWise users, the POA automatically favors client/server processing over message handling. By default, under a heavy load, the POA automatically decreases the number of message handler

threads and increases the number of client/server threads to favor client connections while keeping the total number of threads constant. This behavior benefits users because they are more aware of client performance than they are of messages that they have not yet received.

However, one result of this default behavior is that the message queues can back up during times of heavy client activity. If necessary, you can manually adjust the POA's ratio of client/server threads and message handler threads to help the POA clear out its message queues.

- 1 Make sure that the [POA Web console](#) is password protected, as described in [Section 37.2.1, "Setting Up the POA Web Console,"](#) on page 540.
- 2 In the POA Web console, click *Configuration > Message Worker Threads*.



- 3 Increase the number in the *Worker Yields to C/S Level* field to increase the amount of time that the POA waits before reallocating message worker threads as client/server threads.

Increasing this setting configures the POA to continue processing message queues rather than focusing on client/server processing. Valid values range from 0 (zero) to five. Select 0 to turn off the automatic thread adjustments. The settings of 1 through 5 represent increasing amounts of time, but not a specific number of seconds or minutes.

- 4 Click *Submit* after changing the setting.
The POA automatically restarts to put the new setting into effect.
- 5 Experiment with the setting until you achieve a proper balance between client/server processing and message processing.

38.4 Optimizing Database Maintenance

If you run only one POA for the post office, you can adjust the number of database maintenance threads. If database maintenance needs are extremely heavy for a post office, you can set up a dedicated database maintenance POA to meet those needs.

- ♦ [Section 38.4.1, "Adjusting the Number of POA Threads for Database Maintenance,"](#) on page 567
- ♦ [Section 38.4.2, "Configuring a Dedicated Database Maintenance POA \(Windows Only\),"](#) on page 568

38.4.1 Adjusting the Number of POA Threads for Database Maintenance

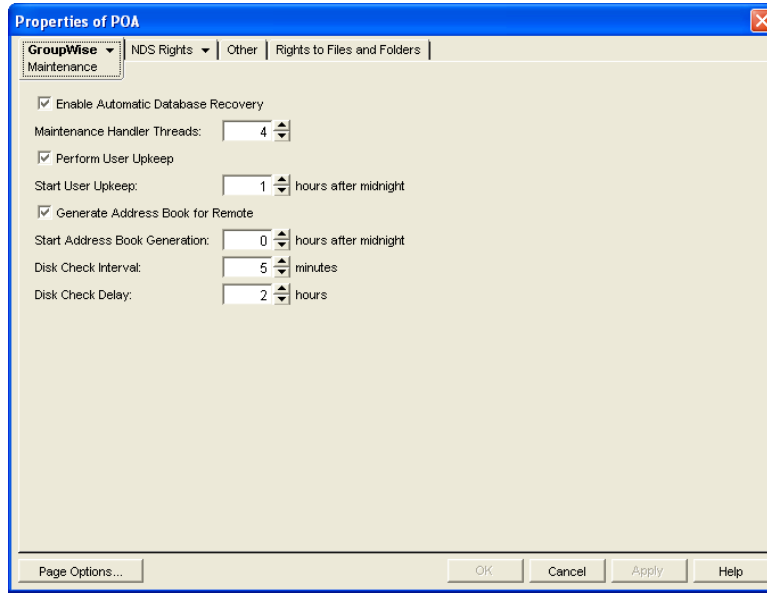
The POA by default performs a certain amount of database maintenance. In addition, you can create your own customized maintenance events as described in [Section 36.4.1, "Scheduling Database Maintenance,"](#) on page 517 and [Section 36.4.2, "Scheduling Disk Space Management,"](#) on page 520.

By default, the POA starts one thread to handle all POA scheduled events and also all usage of the Mailbox/Library Maintenance feature in ConsoleOne.

To adjust the number of POA database maintenance handler threads:

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.

- 2 Click *GroupWise > Maintenance* to display the Maintenance page.



- 3 Increase the number in the *Maintenance Handler Threads* field.
- 4 Click *OK* to save the new thread setting.

ConsoleOne then notifies the POA to restart so the new setting can be put into effect.

Corresponding Startup Switches: You can also use the `--gwchkthreads` switch in the POA startup file to increase the number of POA threads started for database maintenance activities.

POA Web Console: The [Status](#) page helps you assess whether the POA is currently meeting the database maintenance needs of the post office. Under the *Thread Status* heading, click *GWCheck Worker Threads* to display the workload and status of the database maintenance handler threads.

If the POA Web console is password protected as described in [Section 37.2.1, "Setting Up the POA Web Console,"](#) on page 540, you can change the number of database maintenance handler threads on the [Configuration](#) page. Under *Performance Settings*, click *Maximum GWCheck Worker Threads*.

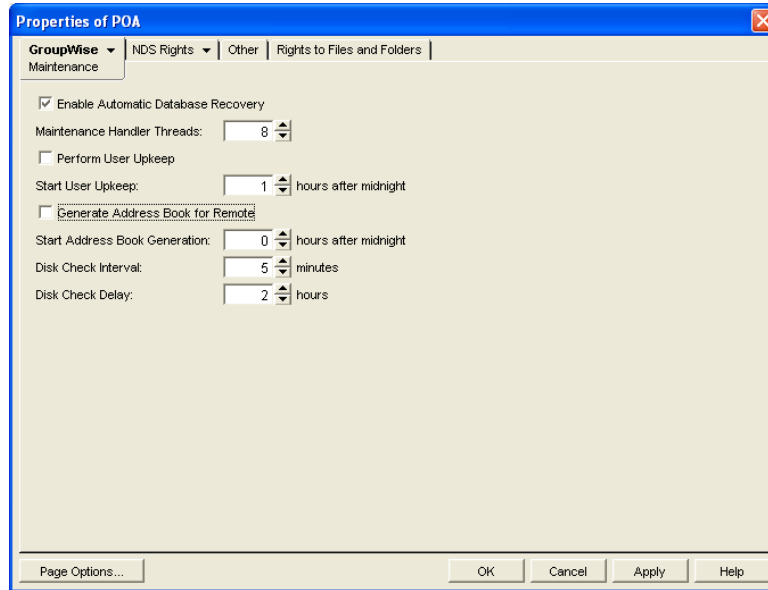
38.4.2 Configuring a Dedicated Database Maintenance POA (Windows Only)

NOTE: The powerful multi-threaded processing capabilities of Linux make multiple POAs unnecessary on that operating system.

If a large amount of database maintenance needs to be performed for a post office, you can set up a dedicated database maintenance POA so that the database maintenance activities do not impact other POA activities, such as responding to GroupWise client users.

- 1 Create a new POA object for the post office as described in [Section 36.1.1, "Creating a POA Object in eDirectory,"](#) on page 482.
- 2 Right-click the new POA object, then click *Properties*.

- 3 Click *GroupWise > Maintenance* to display the Maintenance page.



- 4 Make sure *Enable Automatic Database Recovery* is selected.
- 5 Set *Maintenance Handler Threads* as needed.
The maximum number of threads you can start for database maintenance is 8.
- 6 Deselect *Perform User Upkeep* and deselect *Generate Address Book for Remote*. Make sure another POA handles these tasks.
- 7 Set *Disk Check Interval* and *Disk Check Delay* as appropriate for the database maintenance events you plan to schedule.
- 8 Click *Apply* to save the updated information on the Maintenance page.
- 9 Click *GroupWise > Scheduled Events*, then create database maintenance events as needed, as described in [Section 36.4.1, "Scheduling Database Maintenance,"](#) on page 517 and [Section 36.4.2, "Scheduling Disk Space Management,"](#) on page 520.
- 10 Click *GroupWise > Agent Settings*.
- 11 Deselect *Enable Client/Server* and set *Client/Server Handler Threads* to 0. Make sure another POA handles client/server processing.
- 12 Click *Apply* to save the updated information on the Agent Settings page.
- 13 Click *GroupWise > QuickFinder*.
- 14 Deselect *Enable QuickFinder Indexing*. Make sure another POA handles indexing.
- 15 Click *OK* to save the new settings for dedicated database maintenance processing.
- 16 Install the POA software on a *different* server from where the original POA for the post office is already running. See "[Installing GroupWise Agents](#)" in the *GroupWise 2012 Installation Guide*.
- 17 Add the `--name` switch to the POA startup file and specify the name designated when you created the new POA object.

- 18 For the original POA:
 - 18a Add the `--name` switch to the original POA startup file to differentiate it from the new POA you have set up.
 - 18b Deselect *Enable Automatic Database Recovery* for the original POA object.
 - 18c Restart the original POA, so that it no longer performs the database maintenance activities you have set up a dedicated POA to perform.
- 19 Start the dedicated database maintenance POA.

Corresponding Startup Switches: You can also use the `--nomf`, `--notcpip`, `--noqf`, `--nonuu`, and `--nordab` switches in the POA startup file to disable unwanted processing, then use the `--gwchktthreads` switch to increase the number of database maintenance handler threads.

38.5 Optimizing Client Purge Operations

If enough users empty a very large number of items from their mailboxes all at once, the POA can become very busy purging the items, rather than responding to other user requests in a timely manner. Similarly, when many users log in to GroupWise at about the same time (for example, first thing in the morning), many clients might need to start an Auto-Archive task (which includes purge operations as part of the archive task), and this can also make the POA very busy until the purge operations are completed.

By default, the POA is configured to efficiently handle a typical amount of purging. However, if the default configuration is unacceptably slow during periods of heavy purging, you can prevent users' client response time from degrading. You can configure the POA to restrict the amount of purging that can take place concurrently.

- 1 Make sure that the [POA Web console](#) is password protected, as described in [Section 37.2.1, "Setting Up the POA Web Console,"](#) on page 540.
- 2 In the POA Web console, click *Configuration > Mass Purge Items Threshold*.

GroupWise 2012 POA - Development.Provo1
 Status | Configuration | Environment | Log Files | Scheduled Events | MTP Status | Help

Mass Purge Operation Control

Purge Items Threshold

Max Concurrent Threads Limit

The default settings are typically appropriate.

- 3 (Conditional) If users are experiencing sluggish response time at the beginning of the day, increase the settings until satisfactory response time is achieved.

Purge Items Threshold: Select the maximum number of items that the POA immediately purges from a mailbox. The default number of items to purge immediately is less than 10. Valid values range from 5 to 50.

Max Concurrent Threads Limit: Select the maximum number of concurrent threads that the POA can start for purging batches of items that exceed the Mass Purge Items Threshold setting. The default number of concurrent threads for purging items is 3. Valid values range from 1 to 8.

- 4 Click *Submit* after changing the setting.

The POA automatically restarts to put the new setting into effect.

38.6 Optimizing Calendar Publishing

See [“Configuring a POA for Calendar Publishing”](#) in [“Installing the GroupWise Calendar Publishing Host”](#) in the *GroupWise 2012 Installation Guide*.

39 Managing Indexing of Attachment Content

If you run only one POA for the post office, you can adjust the indexing schedule. You can choose to have indexing performed by the POA's internal Document Converter Agent (DCA) or by the independent Document Viewer Agent (DVA). If indexing needs are extremely heavy for a post office, you can set up a dedicated indexing POA to meet those needs.

- ♦ [Section 39.1, "Regulating Indexing," on page 573](#)
- ♦ [Section 39.2, "Configuring the Document Converter Agent \(DCA\)," on page 575](#)
- ♦ [Section 39.3, "Enabling the Document Viewer Agent \(DVA\) for Indexing," on page 576](#)
- ♦ [Section 39.4, "Controlling Maximum Document Conversion Size and Time," on page 577](#)
- ♦ [Section 39.5, "Configuring a Dedicated Indexing POA \(Windows Only\)," on page 577](#)
- ♦ [Section 39.6, "Customizing Indexing," on page 579](#)

NOTE: To facilitate the Find feature in the GroupWise client, the POA searches unindexed messages as well as those that have already been indexed, so that all messages are immediately available to users whenever they perform a search. The POA does not search unindexed documents, so documents cannot be located using the client Find feature until after indexing has been performed.

For a list of the file types that the POA can index, see [Oracle Outside In Technology Supported Formats \(http://www.oracle.com/technetwork/middleware/content-management/ds-oitfiles-133032.pdf\)](http://www.oracle.com/technetwork/middleware/content-management/ds-oitfiles-133032.pdf).

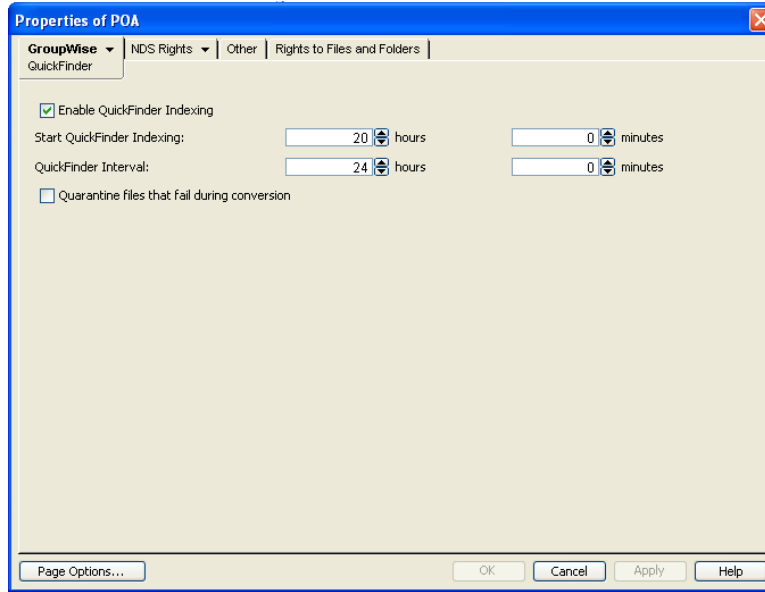
39.1 Regulating Indexing

By default, the POA indexes messages and documents in the post office every 24 hours at 8:00 p.m. You can modify this interval if users need messages and documents indexed more quickly. To start indexing immediately, see ["Updating QuickFinder Indexes" on page 536](#).

To adjust the interval at which indexing occurs:

- 1 In ConsoleOne, browse to and right-click the POA object, then click *Properties*.

- 2 Click *GroupWise > QuickFinder* to display the QuickFinder page.



- 3 Make sure *Enable QuickFinder Indexing* is selected.
- 4 In the *Start QuickFinder Indexing* field, specify the number of hours and minutes after midnight you want the POA to start its indexing cycle.

For example, if you set *QuickFinder Interval* to 6 and *Start QuickFinder Indexing* to 1 hour, indexing cycles occurs at 1:00 a.m., 7:00 a.m., 1:00 p.m., and 7:00 p.m.

- 5 Decrease the number of hours and minutes in the *QuickFinder Interval* field so indexing occurs more frequently.

The interval is measured from the start of one indexing cycle to the next, so that indexing starts at regular intervals, no matter how long each indexing session takes. By default, the start point of the cycle is 8:00 p.m.

To avoid overloading the POA with indexing processing, a maximum of 1000 items are indexed per database for each indexing cycle. If a very large number of messages are received regularly, you should configure the POA with frequent indexing cycles in order to get all messages indexed in a timely manner.

To handle occasional heavy indexing requirements, you can start indexing manually. See [“Updating QuickFinder Indexes” on page 536](#).

- 6 Click *OK* to save the new indexing settings.

ConsoleOne then notifies the POA to restart so the new settings can be put into effect.

Corresponding Startup Switches: You can also use the `--qfinterval`, `--qfintervalinminute`, `--qfbaseoffset`, and `--qfbaseoffsetinminute` switches in the POA startup file to regulate indexing.

POA Web Console: If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,” on page 540](#), you can control indexing for the current POA session on the [Configuration](#) page. Under the *General Settings* heading, click *QuickFinder Indexing*. If indexing is currently in progress, you can check the status of the indexing process on the [Scheduled Events](#) page.

39.2 Configuring the Document Converter Agent (DCA)

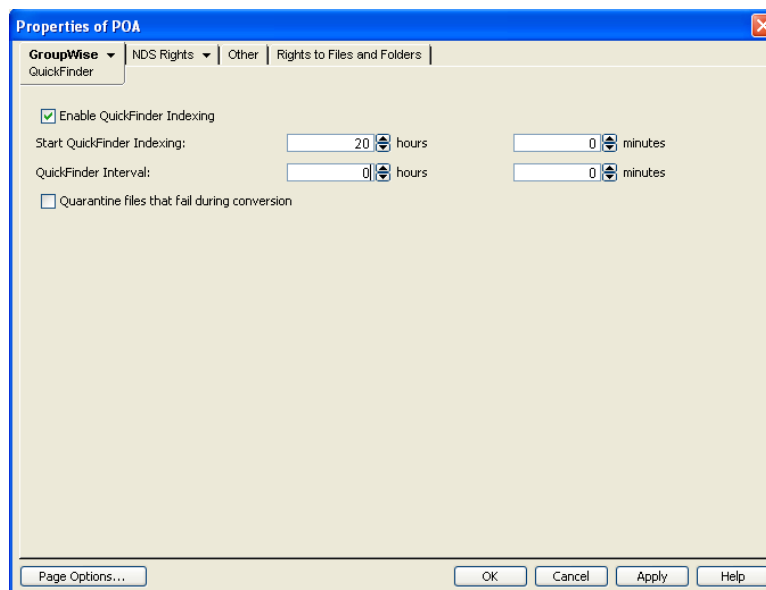
By default, POA can index the file types listed in *Oracle Outside In Technology Supported Formats* (<http://www.oracle.com/technetwork/middleware/content-management/ds-oifiles-133032.pdf>).

In addition, the POA uses the Document Converter Agent (DCA) to index attached PDF files, OpenOffice files, and Microsoft Office 2007 files by converting these file types into HTML in order to index them. The POA decrypts attachment files and places them in the `post_office/oftemp/gwdca/in` directory. The DCA converts the files into HTML and moves them to the `post_office/oftemp/gwdca/out` directory, where the POA picks them up and performs QuickFinder indexing on the HTML version. Then the HTML version is deleted. The DCA reports errors in the `mmdddca.nnn` log file.

The DCA can occasionally fail to convert a document into HTML. By default, documents that fail the conversion into HTML are deleted from the `post_office/oftemp/gwdca/in` directory and are not indexed. However, you can configure the POA to quarantine failed attachments for further examination. Quarantined documents are moved to the `post_office/oftemp/gwdca/problem` directory and are not encrypted.

For security reasons, you should enable the quarantine only to collect sample problem documents in order to submit them to Novell for investigation. Then you should turn off the quarantine to reestablish appropriate security for attached documents.

- 1 In ConsoleOne, browse to and right-click the POA object where you want to turn on the quarantine, then click *Properties*.
- 2 Click *GroupWise > QuickFinder*.



- 3 Select *Quarantine Files That Fail during Conversion*, then click *OK*.
- 4 Collect problem files for investigation.
- 5 Disable the quarantine to return to normal POA operations with full security for attached files.

Corresponding Startup Switches: You can use the `--nodca` switch in the POA startup file to prevent the DCA from starting. You can use the `--dcamaxsize` and `--dcamaxtime` switches to control file size and processing time that the DCA dedicates to converting large files.

POA Web Console: You can see whether the quarantine is on or off on the [Configuration](#) page. If the POA Web console is password protected as described in [Section 37.2.1, “Setting Up the POA Web Console,”](#) on page 540, you can control the maximum amount of time allowed for the conversion of a single document file and the maximum size of a document file for which conversion is attempted.

GroupWise Client in Caching Mode: When users from the Windows client are in Caching Mode, the DCA runs locally on their workstations. Temporary files are stored under the following directories on users’ workstations:

Windows 7: `c:\Users\user_name\AppData\Roaming\Temp\gwdca`

Windows Vista: `c:\Users\user_name\AppData\Local\Temp\gwdca`

Windows XP: `c:\Documents and Settings\user_name\Local Settings\Temp\gwdca`

If temporary files accumulate in these directories, they can be safely deleted.

39.3 Enabling the Document Viewer Agent (DVA) for Indexing

By default, the POA uses [Oracle Outside In Technology](http://www.oracle.com/technetwork/middleware/content-management/ds-oitfiles-133032.pdf) (<http://www.oracle.com/technetwork/middleware/content-management/ds-oitfiles-133032.pdf>) and the [Document Converter Agent \(DCA\)](#) to convert documents into HTML format for indexing. As an alternative to the DCA, which is a process internal to the POA, you can use the independent Document Viewer Agent (DVA) for HTML conversion.

Using the DVA instead of the DCA has the following advantages:

- ♦ **Simplicity:** GroupWise WebAccess requires the DVA to convert attached documents into HTML format for viewing in a Web browser. If you configure the POA to use an existing DVA, you eliminate the need for a DCA.
- ♦ **Fault Tolerance:** You can configure the POA to contact as many as three DVAs. If the DVA that the POA is communicating with stops responding, the POA contacts the next DVA in the list.
- ♦ **Improved Performance:** You can run the DVA on a server other than where the POA runs to lessen the processing load on the POA server.

For complete information about the DVA, see [Part XI, “Document Viewer Agent,”](#) on page 709.

You configure the POA to use the DVA instead of the DCA by using startup switches in the POA startup file. For background information, see [Chapter 40, “Using POA Startup Switches,”](#) on page 581.

- 1 Use the `--usedva` switch to configure the POA to use the DVA instead of the DCA. If the DVA becomes unavailable, the POA falls back to using the DCA for document conversion.
- 2 Use the `--dvanipaddr` and `--dvanport` switches to identify from one to three DVAs.
Replace *n* with 1, 2, or 3. Three DVAs is recommended. Multiple POAs can communicate with the same DVA simultaneously.
- 3 (Conditional) If you want to use a secure SSL connection between the POA and the DVA, use the `--dvanssl` switch.
By default, SSL is not used. Set the switch to `enable` to enable a secure SSL connection. For more information about using SSL with the POA, see [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.
- 4 After you edit the POA startup file, restart the POA in order to put the changes into effect.

39.4 Controlling Maximum Document Conversion Size and Time

By default, the POA sends all attached documents for HTML conversion for indexing, regardless of the size of the document, and by default, the POA waits as long as 10 minutes to receive the HTML version.

You control the maximum document conversion size and time using startup switches in the POA startup file. After you edit the POA startup file, you must restart the POA in order to put the changes into effect.

Use the `--dcamaxsize` switch to restrict the size of documents that it sends for conversion. Set the `--dcamaxsize` switch to the maximum document size in kilobytes. For example, you would use 20480 for 20 MB.

Use the `--dcamaxtime` switch to change the amount of time the POA waits for the HTML version. Set the `--dcamaxtime` switch to the number of seconds that you want the POA wait. The default is 600 seconds.

These switches control how the POA hands off documents for HTML conversion, regardless of whether it is configured to use the DCA or the DVA.

39.5 Configuring a Dedicated Indexing POA (Windows Only)

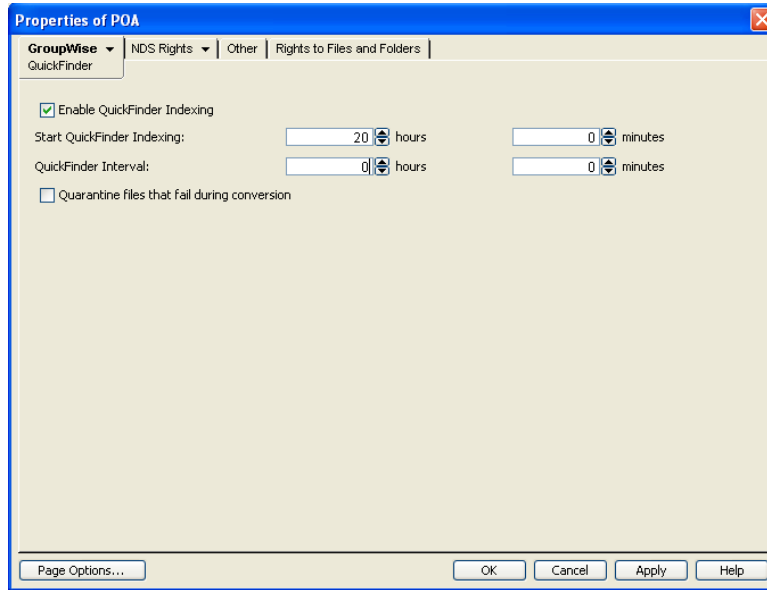
NOTE: The powerful multi-threaded processing capabilities of Linux make multiple POAs unnecessary on that operating system.

If your GroupWise client users rely heavily on indexed documents, you can set up a dedicated indexing POA so that indexing can be performed without impacting other POA functions on the server. A dedicated indexing POA is beneficial if the typical indexing load is adversely affecting the POA's performance in servicing GroupWise client users.

To configure a dedicated indexing POA:

- 1 Create a new POA object for the post office as described in [Section 36.1.1, "Creating a POA Object in eDirectory,"](#) on page 482.
- 2 Right-click the new POA object, then click *Properties*.

- 3 Click *GroupWise > QuickFinder* to display the QuickFinder page.



- 4 Make sure *Enable QuickFinder Indexing* is selected.
- 5 In the *Start QuickFinder Indexing* field, specify the number of hours and minutes after midnight you want the POA to start its indexing cycle.
The default is 20, meaning at 8:00 p.m.
- 6 Set *QuickFinder Update Interval* low enough to keep up with the indexing demands of your GroupWise client users.
To avoid overloading the POA with indexing processing, a maximum of 1000 items are indexed per database for each indexing cycle. If a very large number of messages are received regularly, you should configure the POA with very frequent indexing cycles in order to get all messages indexed in a timely manner.
For continuous QuickFinder indexing, set *QuickFinder Update Interval* to 0 (zero).
- 7 Click *Apply* to save the updated QuickFinder settings.
- 8 Click *GroupWise > Agent Settings*.
- 9 Set *Message File Processing* to *Off*. Make sure another POA handles message file processing.
- 10 Deselect *Enable Client/Server* and set *Client/Server Handler Threads* to 0. Make sure another POA handles client/server processing.
- 11 Select *Disable Administration Task Processing*, so that this POA does not run an admin thread. Make sure that another POA handles administration tasks.
- 12 Click *Apply* to save the updated agent settings.
- 13 Click *GroupWise > Maintenance*.
- 14 Deselect *Enable Automatic Database Recovery*. Make sure another POA handles database recovery.
- 15 Set *Maintenance Handler Threads* to 0 (zero). Make sure another POA handles database maintenance and disk space management.
- 16 Deselect *Perform User Upkeep* and deselect *Generate Address Book for Remote*. Make sure another POA handles these tasks.
- 17 Click *OK* to save the new settings for dedicated indexing.

- 18 Install the POA software on a *different* server from where the original POA for the post office is already running. See “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.
- 19 Add the `--name` switch to the POA startup file and specify the name designated when the new POA object was created.
- 20 For the original POA:
 - 20a Add the `--name` switch to the original POA startup file to differentiate it from the new POA you have set up.
 - 20b Deselect *Enable QuickFinder Indexing* for the original POA object.
 - 20c Restart the original POA, so that it no longer performs the QuickFinder indexing activities you have set up a dedicated POA to perform.
- 21 Start the dedicated indexing POA.

Corresponding Startup Switches: You can also use the `--nomf`, `--notcpip`, `--norecover`, `--nonuu`, and `--nordab` switches in the POA startup file to disable unwanted processing, then use the `--qfinterval`, `--qfintervalinminute`, `--qfbaseoffset`, and `--qfbaseoffsetinminute` switches to control the indexing schedule.

39.6 Customizing Indexing

By default, the POA indexes 500 items in a user or library database, then moves on to the next database during each QuickFinder indexing cycle. The indexing cycle is established on the QuickFinder property page of the POA object. By default, QuickFinder indexing is performed once a day at 8:00 p.m. If a database has more than 500 items that need to be indexed, items beyond 500 wait for the next indexing cycle.

Occasionally, circumstances arise where indexing needs are especially heavy for a short period of time. This can occur when you move users to a different post office or if the QuickFinder indexes for a post office become damaged. Startup switches are available for temporary use in the POA startup file to customize the way the POA handles indexing. In general, they are not intended for long-term use. You might want to set up a separate POA just to handle the temporary indexing needs, as described in [Section 39.5, “Configuring a Dedicated Indexing POA \(Windows Only\),”](#) on page 577, and use these switches only with the dedicated indexing POA.

Because the switches are placed in the POA startup file, you must stop and then start the POA to put the settings into effect.

- ♦ [Section 39.6.1, “Determining What to Index,”](#) on page 579
- ♦ [Section 39.6.2, “Determining Indexing Priority,”](#) on page 580
- ♦ [Section 39.6.3, “Reclaiming Disk Space,”](#) on page 580

39.6.1 Determining What to Index

You can configure the POA to index just user mailbox contents or just library contents. Use the `--qfnousers` switch to focus on indexing library contents. Use the `--qfnolib` switch to focus on indexing user mailbox contents. Use the `--qfnopreproc` switch to suppress even the generation of document word lists that are normally written to user databases that reference documents.

When you have a large number of user databases that need to be indexed, you can configure the POA to index a specific range of databases based on user FIDs. For a task of this magnitude, you should run multiple dedicated indexing POAs with each POA configured to process a specific range of

databases. Use the `--qfuserfidbeg` and `--qfuserfidend` switches to define the range for each POA. You can determine the FID numbers of the databases by listing the user databases (`userxxx.db`) in the `ofuser` directory. The `xxx` part of the user database name is the FID.

You could also use these switches to single out a specific user database for indexing. Specify the same FID for both switches. To determine a user's FID, click *Help > About GroupWise* in the GroupWise client. In Online mode, the FID is displayed after the user name. In Caching or Remote mode, the FID is the last three characters of the Caching or Remote directory name (for example, `gwstr7bh`).

39.6.2 Determining Indexing Priority

The POA carries on many processes at once. If you are not using a dedicated indexing POA, you can configure the POA to make indexing a higher or lower priority task than responding to users' activities in their mailboxes. You can also control how many items the POA indexes in each database that it processes. Use the `--qflevel` switch to control indexing priority. The table below explains the priority levels:

Priority Level	Description
0	Index a maximum of 1000 items at a time, rather than the default of 500.
1	Index a maximum of 500 items at time, using a low-priority thread. This keeps frequent daytime indexing cycles from interfering with users' activities in their mailboxes.
2	Index a maximum of 1000 items at a time, using a medium-priority thread. This allows additional items in each database to be processed in each indexing cycle. Using a medium-priority thread makes indexing more important than some user activities in mailboxes. Users might notice some slowness in response from the GroupWise client.
3	Index a maximum of 2000 items at a time, using a high-priority thread. Using a high-priority thread makes indexing more important than many user activities in mailboxes. Users will notice some slowness in response from the GroupWise client. This is warranted only when the immediate completion of indexing is extremely important.
999	Index constantly until all databases have been indexed, then wait until the next indexing cycle set on the QuickFinder property page of the POA object before starting to index again.

If you have users who consistently receive more items than are processed during your current daily indexing cycle, you could implement an appropriate `--qflevel` setting for permanent use.

39.6.3 Reclaiming Disk Space

The POA uses `.idx` files to store compressed indexes. It uses `.inc` files to store incremental indexes that have not yet been compressed. At regular intervals, the POA compresses the contents of the `.inc` files and adds the data to the `.idx` files. Afterwards, it retains the previous `.idx` and `.inc` files for a period of time. Use the `--qfdeleteold` switch to delete the previous versions of the `.idx` and `.inc` files to conserve disk space during periods of heavy indexing. It is primarily applicable when using `--qflevel=1` where indexing is a lower priority task. For `--qflevel=2` and `--qflevel=3`, indexing itself is a higher priority than compression and deletion cleanup tasks.

40 Using POA Startup Switches

You can override settings provided in ConsoleOne by using startup switches in the POA startup file. The default location for the startup file varies by platform.

Linux: `/opt/novell/groupwise/agents/share`

Windows: `c:\Program Files\Novell\GroupWise Server\Agents`

When you run the Agent Installation program, an initial POA startup file is created. It is named using the first 8 characters of the post office name with a `.poa` extension. This initial startup file includes the `--home` startup switch set to the location of the post office directory.

When you update the POA software, the existing POA startup file can be retained or overwritten as needed.

Linux: When you use both the *Install* and *Configure* options in the Agent Installation program, the existing POA startup file is backed up and then overwritten. When you use only the *Install* option, the existing POA startup file is retained.

Windows: When you select *Install the software files, but do not configure the agents* in the Agent Installation program, the existing POA startup file is retained. When you do not select this option, the existing POA startup file is backed up and then overwritten.

Startup switches specified on the command line override those in the startup file. Startup switches in the startup file override corresponding settings in ConsoleOne. You can view the POA startup file from the Configuration page of the POA Web console.

The table below summarizes POA startup switches for all platforms and how they correspond to configuration settings in ConsoleOne.

Switch starts with: `a b c d e f g h i j k l m n o p q r s t u v w x y z`

Linux POA	Windows POA	ConsoleOne Settings
<code>@file_name</code>	<code>@file_name</code>	N/A
<code>--attemptsresetinterval</code>	<code>/attemptsresetinterval</code>	<i>Incorrect Login Reset Time</i>
<code>--certfile</code>	<code>/certfile</code>	<i>Certificate File</i>
<code>--dcamaxsize</code>	<code>/dcamaxsize</code>	N/A
<code>--dcamaxtime</code>	<code>/dcamaxtime</code>	N/A
<code>--dvanipaddr</code>	<code>--dvanipaddr</code>	N/A
<code>--dvanport</code>	<code>--dvanport</code>	N/A
<code>--dvanssl</code>	<code>--dvanssl</code>	N/A

Linux POA	Windows POA	ConsoleOne Settings
--cluster	/cluster	N/A
--enforceclientversion	/enforceclientversion	<i>Lock Out Older GroupWise Clients</i>
--evocontrol	/evocontrol	N/A
--externalclientssl	/externalclientssl	<i>Internet Client/Server SSL</i>
--gwchkthreads	/gwchkthreads	<i>Maintenance Handler Threads</i>
--gwclientreleasedate	/gwclientreleasedate	<i>Minimum Client Release Date</i>
--gwclientreleaseversion	/gwclientreleaseversion	<i>Minimum Client Release Version</i>
--help	/help	N/A
--home	/home	N/A
--httppassword	/httppassword	<i>HTTP Password</i>
--httpport	/httpport	<i>HTTP Port</i>
--httprefresh	/httprefresh	N/A
--httpssl	/httpssl	<i>HTTP SSL</i>
--httpuser	/httpuser	<i>HTTP User Name</i>
--imap	/imap	<i>IMAP</i>
--imapmaxthreads	/imapmaxthreads	<i>Max IMAP Threads</i>
--imapport	/imapport	<i>IMAP Port</i>
--imapreadlimit	/imapreadlimit	N/A
--imapreadnew	/imapreadnew	N/A
--imapssl	/imapssl	<i>IMAP SSL</i>
--imapsslport	/imapsslport	<i>IMAP SSL Port</i>
--incorrectloginattempts	/incorrectloginattempts	<i>Incorrect Logins Allowed</i>
--internalclientssl	/internalclientssl	<i>Local Intranet Client SSL</i>
--intruderlockout	/intruderlockout	<i>Enable Intruder Detection</i>
--ip	/ip	N/A
--keyfile	/keyfile	<i>SSL Key File</i>
--keypassword	/keypassword	<i>SSL Key File Password</i>
--language	/language	N/A
--ldapdisablepwdchg	/ldapdisablepwdchg	<i>Disable LDAP Password Changing</i>
--ldapipaddr	/ldapipaddr	<i>LDAP Server Address</i>
--ldapippooln	/dapippooln	<i>Select LDAP Servers</i>
--ldappoolresetime	/dappoolresetime	<i>LDAP Pool Server Reset Timeout</i>
--ldapport	/dapport	<i>LDAP Server Address</i>

Linux POA	Windows POA	ConsoleOne Settings
--ldapportpooln	/ldapportpooln	LDAP Server Address
--ldappwd	/ldappwd	LDAP Password
--ldapssl	/ldapssl	Use SSL
--ldapsslpooln	/ldapsslpooln	Use SSL
--ldapsslkey	/ldapsslkey	SSL Key File
--ldapsslkeypooln	/ldapsslkeypooln	SSL Key File
--ldaptimeout	/ldaptimeout	Inactive Connection Timeout
--ldapuser	/ldapuser	LDAP User Name
--ldapuserauthmethod	/ldapuserauthmethod	User Authentication Method
--lockoutresetinterval	/lockoutresetinterval	Lockout Reset Time
--log	/log	Log File Path
--logdays	/logdays	Max Log File Age
--logdiskoff	/logdiskoff	Logging Level
--loglevel	/loglevel	Logging Level
--logmax	/logmax	Max Log Disk Space
--maxappconns	/maxappconns	Max Application Connections
--maxphysconns	/maxphysconns	Max Physical Connections
--mtpinipaddr	/mtpinipaddr	IP Address (POA)
--mtpinport	/mtpinport	Message Transfer Port (POA)
--mtpoutipaddr	/mtpoutipaddr	IP Address (MTA)
--mtpoutport	/mtpoutport	Message Transfer Port (MTA)
--mtpsendmax	/mtpsendmax	Maximum Send Message Size
--mtpssl	/mtpssl	Message Transfer SSL
--name	/name	N/A
--noada	/noada	N/A
--nocache	/nocache	Enable Caching
--noconfig	/noconfig	N/A
--nodca	/nodca	N/A
--noerrormail	/noerrormail	N/A
--nogwchk	/nogwchk	N/A
--nomf	/nomf	Message File Processing
--nomfhigh	/nomfhigh	Message File Processing
--nomflow	/nomflow	Message File Processing

Linux POA	Windows POA	ConsoleOne Settings
--nomtp	/nomtp	N/A
--nonuu	/nonuu	<i>Perform User Upkeep</i>
--noqf	/noqf	<i>Enable QuickFinder Indexing</i>
--nordab	/nordab	<i>Generate Address Books for Remote</i>
--norecover	/norecover	<i>Enable Auto DB Recovery</i>
--nosnmp	/nosnmp	<i>Enable SNMP</i>
--notcpip	/notcpip	<i>Enable Client/Server</i>
--nuuoffset	/nuuoffset	<i>Start User Upkeep</i>
--password	/password	<i>Remote Password</i>
--port	/port	<i>Client/Server Port</i>
--primingmax	/primingmax	<i>Max Thread Usage for Priming and Moves</i>
--qfbaseoffset	/qfbaseoffset	<i>Start QuickFinder Indexing</i>
--qfbaseoffsetinminute	/qfbaseoffsetinminute	<i>Start QuickFinder Indexing</i>
--qfdeleteold	/qfdeleteold	N/A
--qfinterval	/qfinterval	<i>QuickFinder Interval</i>
--qfintervalinminute	/qfintervalinminute	<i>QuickFinder Interval</i>
--qflevel	/qflevel	N/A
--qfnolib	/qfnolib	N/A
--qfnopreproc	/qfnopreproc	N/A
--qfnusers	/qfnusers	N/A
--qfuserfidbeg	/qfuserfidbeg	N/A
--qfuserfidend	/qfuserfidend	N/A
--rdaboffset	/rdaboffset	<i>Start Address Book Generation</i>
--rights	/rights	N/A
--show	N/A	N/A
--soap	/soap	<i>Enable SOAP</i>
--soapmaxthreads	/soapmaxthreads	<i>Max SOAP Threads</i>
--soapport	/soapport	<i>SOAP Port</i>
--soapsizelimit	/soapsizelimit	N/A
--soapssl	/soapssl	<i>SOAP SSL</i>
--soapthreads	/soapthreads	N/A
--tcpthreads	/tcpthreads	<i>Client/Server Handler Threads</i>
--threads	/threads	<i>Message Handler Threads</i>

Linux POA	Windows POA	ConsoleOne Settings
<code>--usedva</code>	<code>/usedva</code>	N/A
<code>--user</code>	<code>/user</code>	N/A

40.1 @file_name

Specifies the location of the POA startup file.

Linux: The startup file always resides in the `/opt/novell/groupwise/agents/share` directory.

Windows: The full path must be included if the file does not reside in the same directory with the POA program.

The startup file must reside on the same server where the POA is installed.

Linux POA	Windows POA
Syntax: <code>@[/dir]file</code>	<code>@[drive:][\dir]file</code>
Example: <code>./gwpoa @../share/lnxpost.poa</code>	<code>gwpoa.exe @sales.poa</code> <code>gwpoa.exe @d:\agt\sales.poa</code>

40.2 --attemptsresetinterval

Specifies the length of time during which unsuccessful login attempts are counted, leading to lockout. The default is 30 minutes; valid values range from 15 to 60. See [Section 36.3.5, “Enabling Intruder Detection,”](#) on page 516.

Linux POA	Windows POA
Syntax: <code>--attemptsresetinterval minutes</code>	<code>/attemptsresetinterval-minutes</code>
Example: <code>--attemptsresetinterval 45</code>	<code>/attemptsresetinterval-60</code>

See also [--intruderlockout](#), [--incorrectloginattempts](#), and [--lockoutresetinterval](#).

40.3 --certfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the POA and other programs. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.

Linux POA	Windows POA
Syntax: <code>--certfile /dir/file</code>	<code>/certfile-[drive:]\dir\file</code> <code>/certfile-\\svr\sharename\dir\file</code>

Linux POA	Windows POA
Example: --certfile /certs/gw.crt	/certfile-\ssl\gw.crt /certfile-m:\ssl\gw.crt certfile-\\server2\c\ssl\gw.crt

See also [--keyfile](#) and [--keypassword](#).

40.4 --cluster

Informs the POA that it is running in a cluster. When communicating with a clustered POA, the GroupWise client extends the retry period for reconnection. A clustered POA automatically binds to the IP address configured for the POA object even if the *Bind Exclusively to TCP/IP Address* option is not selected on the POA Network Address page in ConsoleOne. This prevents unintended connections to other IP addresses, such as the loopback address or the node's physical IP address. For information about clustering the POA, see the [GroupWise 2012 Interoperability Guide](#).

Linux POA	Windows POA
Syntax: --cluster	/cluster

See also [--ip](#).

40.5 --dcamaxsize

Sets the maximum size for attached documents that the POA hands off to the DCA or the DVA for conversion into HTML format so that the documents can be indexed. By default, there is no maximum size limit. See [Section 39.4, "Controlling Maximum Document Conversion Size and Time," on page 577](#).

Linux POA	Windows POA
Syntax: --dcamaxsize <i>kilobytes</i>	/dcamaxsize- <i>kilobytes</i>
Example: --dcamaxsize 20480	/dcamaxsize-40960

See also [--dcamaxtime](#).

40.6 --dcamaxtime

Sets the maximum time that the POA waits to receive documents converted into HTML by the DCA or the DVA. The default is 600 seconds (10 minutes). See [Section 39.4, "Controlling Maximum Document Conversion Size and Time," on page 577](#).

Linux POA	Windows POA
Syntax: --dcamaxtime <i>seconds</i>	/dcamaxtime- <i>seconds</i>
Example: --dcamaxtime 20480	/dcamaxtime-40960

See also [--dcamaxsize](#).

40.7 --dvanipaddr

Specifies the IP address of a DVA that the POA can use to convert documents into HTML format for indexing. You can configure the POA to communicate with up to three DVAs. In the switch, replace *n* with 1, 2, or 3 to identify multiple DVAs. See [Section 39.3, “Enabling the Document Viewer Agent \(DVA\) for Indexing,”](#) on page 576.

	Linux POA	Windows POA
Syntax:	<code>--dvanipaddr ip_address</code>	<code>/dvanipaddr-ip_address</code>
Example:	<code>--dva1ipaddr 172.17.5.18</code>	<code>/dva2ipaddr-172.17.5.19</code>

See also [--dvanport](#), [--dvanssl](#), and [--usedva](#).

40.8 --dvanport

Specifies the port number used for the POA to communicate with the corresponding DVA. The default port number is 8301. In the switch, replace *n* with 1, 2, or 3 to identify multiple DVAs. See [Section 39.3, “Enabling the Document Viewer Agent \(DVA\) for Indexing,”](#) on page 576.

	Linux POA	Windows POA
Syntax:	<code>--dvanport port_number</code>	<code>/dvanport-port_number</code>
Example:	<code>--dva2port 8302</code>	<code>/dva3port-8303</code>

See also [--dvanipaddr](#), [--dvanssl](#) and [--usedva](#).

40.9 --dvanssl

Sets the availability of SSL communication between the POA and the corresponding DVA. Valid values are `enable` and `disable`. SSL is disabled by default. In the switch, replace *n* with 1, 2, or 3 to identify multiple DVAs. See [Section 39.3, “Enabling the Document Viewer Agent \(DVA\) for Indexing,”](#) on page 576.

	Linux POA	Windows POA
Syntax:	<code>--dvanssl setting</code>	<code>/dvanssl-setting</code>
Example:	<code>--dva2ssl enable</code>	<code>/dva3ssl-enable</code>

See also [--dvanipaddr](#), [--dvanport](#), and [--usedva](#).

40.10 --enforceclientversion

Enforces the minimum client release version and/or date so that users of older clients are forced to update in order to access their GroupWise mailboxes. Valid settings are version, date, both, and disabled. See [Section 36.2.5, “Checking What GroupWise Clients Are in Use,”](#) on page 502.

	Linux POA	Windows POA
Syntax:	--enforceclientversion <i>setting</i>	/enforceclientversion- <i>setting</i>
Example:	--enforceclientversion date	/enforceclientversion-both

See also [--gwclientreleasedate](#), and [--gwclientreleaseversion](#).

40.11 --evocontrol

Determines which versions of Evolution are allowed to access the post office. Users might experience problems using Evolution to connect to their GroupWise mailboxes if they are using Evolution 2.6.0 or earlier. In addition, earlier versions of Evolution can cause high utilization on GroupWise servers.

To encourage users to update to the latest version of Evolution, you can use the --evocontrol switch to configure the POA to allow only specified versions of Evolution. For information about configuring a post office to support Evolution, see [Section 36.2.4, “Supporting SOAP Clients,”](#) on page 499.

	Linux POA	Windows POA
Syntax:	--evocontrol-Evolution- <i>version.date</i> --evocontrol-Evolution-Data-Server- <i>version-date</i>	/evocontrol-Evolution- <i>version.date</i> /evocontrol-Evolution-Data-Server- <i>version-date</i>
Example:	--evocontrol Evolution-1.10-2006-12-04 --evocontrol Evolution-Data-Server-1.10-2006-12-04	/evocontrol-Evolution-1.10-2006-12-04 /evocontrol-Evolution-Data-Server-1.10-2006-12-04

You can put as many as 10 entries in the startup file, so that you can list as many as 10 versions of Evolution. Entries beyond 10 are ignored. You can view the current entries at the POA Web console with the other SOAP settings. The POA log file lists the settings in the Soap Session section.

40.12 --externalclientsssl

Sets the availability of SSL communication between the POA and GroupWise clients that are running outside your firewall. Valid values are enabled, required, and disabled. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.

	Linux POA	Windows POA
Syntax:	--externalclientsssl <i>setting</i>	/externalclientsssl- <i>setting</i>
Example:	--externalclientsssl disabled	/externalclientsssl-required

See also [--certfile](#), [--keyfile](#), [--keypassword](#), and [--port](#).

40.13 --gwchkthreads

Specifies the number of threads the POA starts for Mailbox/Library Maintenance activities. The default is 4; valid values range from 1 to 8. See [Section 38.4.1, “Adjusting the Number of POA Threads for Database Maintenance,”](#) on page 567.

	Linux POA	Windows POA
Syntax:	--gwchkthreads <i>number</i>	/gwchkthreads- <i>number</i>
Example:	--gwchkthreads 6	/gwchkthreads-8

See also [--nogwchk](#).

40.14 --gwclientreleasedate

Specifies the date of the approved GroupWise client software for your system. See [Section 36.2.5, “Checking What GroupWise Clients Are in Use,”](#) on page 502.

	Linux POA	Windows POA
Syntax:	--gwclientreleasedate <i>mm-dd-yyyy</i>	/gwclientreleasedate- <i>mm-dd-yyyy</i>
Example:	--gwclientreleasedate 10-24-2008	/gwclientreleasedate-10-24-2008

See also [--gwclientreleaseversion](#) and [--enforceclientversion](#).

40.15 --gwclientreleaseversion

Specifies the version of the approved GroupWise client software for your system. See [Section 36.2.5, “Checking What GroupWise Clients Are in Use,”](#) on page 502.

	Linux POA	Windows POA
Syntax:	--gwclientreleaseversion <i>n.n.n</i>	/gwclientreleaseversion- <i>n.n.n</i>
Example:	--gwclientreleaseversion 6.5.6	/gwclientreleaseversion-7.0.0

See also [--gwclientreleasedate](#) and [--enforceclientversion](#).

40.16 --help

Displays the POA startup switch Help information. When this switch is used, the POA does not start.

	Linux POA	Windows POA
Syntax:	--help	/help or /?
Example:	./gwpoa --help	gwpoa.exe /help

40.17 --home

Specifies the post office directory, where the POA can find the message and user databases to service. There is no default location. You must use this switch in order to start the POA.

	Linux POA	Windows POA
Syntax:	<code>--home /dir</code>	<code>/home-[drive:]\dir</code> <code>/home-\\sv\sharename\dir</code>
Example:	<code>--home /gwsystem/sales</code>	<code>/home-\sales</code> <code>/home-m:\sales</code> <code>/home-\\server2\c\sales</code>

If you specify a UNC path with the `--home` switch when you run the POA as a Windows service, you must configure the POA service to run under a specific Windows user account. If you specify a local directory or a mapped drive, you can configure the POA service to run under the local system account. However, running as the Administrator account is highly recommended.

40.18 --httppassword

Specifies the password for the POA to prompt for before allowing POA status information to be displayed in your Web browser. Do not use an existing eDirectory password because the information passes over the non-secure connection between your Web browser and the POA. See [Section 37.2, "Using the POA Web Console,"](#) on page 539.

	Linux POA	Windows POA
Syntax:	<code>--httppassword <i>unique_password</i></code>	<code>/httppassword-<i>unique_password</i></code>
Example:	<code>--httppassword AgentWatch</code>	<code>/httppassword-AgentWatch</code>

See also [--httpuser](#), [--httpport](#), [--httprefresh](#), and [--httpsl](#).

40.19 --httpport

Sets the HTTP port number used for the POA to communicate with your Web browser. The default is 7181; the setting must be unique. See [Section 37.2, "Using the POA Web Console,"](#) on page 539.

	Linux POA	Windows POA
Syntax:	<code>--httpport <i>port_number</i></code>	<code>/httpport-<i>port_number</i></code>
Example:	<code>--httpport 7183</code>	<code>/httpport-7184</code>

See also [--httpuser](#), [--httppassword](#), [--httprefresh](#), and [--httpsl](#).

40.20 --httpprefresh

Specifies the rate at which the POA refreshes the status information in your Web browser. The default is 60 seconds. See [Section 37.2, “Using the POA Web Console,”](#) on page 539.

	Linux POA	Windows POA
Syntax:	--httpprefresh <i>seconds</i>	/httpprefresh- <i>seconds</i>
Example:	--httpprefresh 90	/httpprefresh-120

See also [--httpuser](#), [--httppassword](#), [--httpport](#), and [--https](#).

40.21 --https

Sets the availability of secure SSL communication between the POA and the POA Web console displayed in your Web browser. Valid values are enabled and disabled. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.

	Linux POA	Windows POA
Syntax:	--https <i>setting</i>	/https- <i>setting</i>
Example:	--https enabled	/https-enabled

See also [--certfile](#), [--keyfile](#), and [--keypassword](#).

40.22 --httpuser

Specifies the user name for the POA to prompt for before allowing POA status information to be displayed in a Web browser. Providing a user name is optional. Do not use an existing eDirectory user name because the information passes over the non-secure connection between your Web browser and the POA. See [Section 37.2, “Using the POA Web Console,”](#) on page 539.

	Linux POA	Windows POA
Syntax:	--httpuser <i>unique_name</i>	/httpuser- <i>unique_name</i>
Example:	--httpuser GWWebCon	/httpuser-GWWebCon

See also [--httppassword](#), [--httpport](#), [--httpprefresh](#), and [--https](#).

40.23 --imap

Enables IMAP so that the POA can communicate with IMAP clients. Valid settings are enabled and disabled. See [Section 36.2.3, “Supporting IMAP Clients,”](#) on page 498.

	Linux POA	Windows POA
Syntax:	--imap enabled or disabled	/imap-enabled or disabled

Linux POA	Windows POA
Example: --imap disabled	/imap-enabled

See also [--imapmaxthreads](#), [--imapport](#), [--imapreadlimit](#), [--imapreadnew](#), [--imapssl](#), and [--imapsslport](#).

40.24 --imapmaxthreads

Specifies the maximum number of IMAP threads the POA can create to service IMAP clients. The default is 40. This setting is appropriate for most systems. See [Section 36.2.3, “Supporting IMAP Clients,”](#) on page 498.

Linux POA	Windows POA
Syntax: --imapmaxthreads <i>number</i>	/imapmaxthreads- <i>number</i>
Example: --imapmaxthreads 30	/imapmaxthreads-35

See also [--imap](#), [--imapport](#), [--imapreadlimit](#), [--imapreadnew](#), [--imapssl](#), and [--imapsslport](#).

40.25 --imapreadlimit

Specifies in thousands the maximum number of messages that can be downloaded by an IMAP client. For example, specifying 10 represents 10,000. The default is 20,000. The maximum allowed limit is 65. The server caches all downloaded items, so setting a high limit could consume more server resources than you would prefer the POA to use.

Linux POA	Windows POA
Syntax: --imapreadlimit <i>number</i>	/imapreadlimit- <i>number</i>
Example: --imapreadlimit 20	/imapreadlimit-50

See also [--imap](#), [--imapmaxthreads](#), [--imapport](#), [--imapreadnew](#), [--imapssl](#), and [--imapsslport](#).

40.26 --imapreadnew

By default, the IMAP agent reads items in a folder from the oldest to the newest. As a result, if a folder contains more items than are allowed by the [--imapreadlimit](#) setting, users receive the older items but not the newer items. Enable this switch so that the POA reads items from the newest to the oldest. This ensures that users receive all their new items in a timely manner.

Linux POA	Windows POA
Syntax: --imapreadnew	/imapreadnew

See also [--imap](#), [--imapmaxthreads](#), [--imapreadlimit](#), [--imapport](#), [--imapssl](#), and [--imapsslport](#).

40.27 --imapport

Sets the TCP port number used for the POA to communicate with IMAP clients when using a non-SSL connection. The default is 143. See [Section 36.2.3, “Supporting IMAP Clients,”](#) on page 498.

	Linux POA	Windows POA
Syntax:	<code>--imapport <i>port_number</i></code>	<code>/imapport-<i>port_number</i></code>
Example:	<code>--imapport 146</code>	<code>/imapport-147</code>

See also `--imap`, `--imapmaxthreads`, `--imapreadlimit`, `--imapreadnew`, `--imapssl`, and `--imapsslport`.

40.28 --imapssl

Sets the availability of secure SSL communication between the POA and IMAP clients. Valid settings are enable and disable. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.

	Linux POA	Windows POA
Syntax:	<code>--imapssl <i>setting</i></code>	<code>/imapssl-<i>setting</i></code>
Example:	<code>--imapssl enable</code>	<code>/imapssl-enable</code>

See also `--imap`, `--imapmaxthreads`, `--imapport`, `--imapreadlimit`, `--imapreadnew`, and `--imapsslport`.

40.29 --imapsslport

Sets the TCP port number used for the POA to communicate with IMAP clients when using an SSL connection. The default is 993. See [Section 36.2.3, “Supporting IMAP Clients,”](#) on page 498.

	Linux POA	Windows POA
Syntax:	<code>--imapsslport <i>port_number</i></code>	<code>/imapsslport-<i>port_number</i></code>
Example:	<code>--imapsslport 995</code>	<code>/imapsslport-996</code>

See also `--imap`, `--imapmaxthreads`, `--imapport`, `--imapreadlimit`, `--imapreadnew`, and `--imapssl`.

40.30 --incorrectloginattempts

Specifies the number of unsuccessful login attempts after which lockout occurs. The default is 5 attempts; valid values range from 3 to 10. See [Section 36.3.5, “Enabling Intruder Detection,”](#) on page 516.

	Linux POA	Windows POA
Syntax:	<code>--incorrectloginattempts <i>number</i></code>	<code>/incorrectloginattempts-<i>number</i></code>
Example:	<code>--incorrectloginattempts 10</code>	<code>/incorrectloginattempts-10</code>

See also [--intruderlockout](#), [--attemptsresetinterval](#), and [--lockoutresetinterval](#).

40.31 --internalclientssl

Sets the availability of secure SSL communication between the POA and GroupWise clients that are running inside your firewall. Valid values are enabled, required, and disabled. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.

	Linux POA	Windows POA
Syntax:	<code>--internalclientssl <i>setting</i></code>	<code>/internalclientssl-<i>setting</i></code>
Example:	<code>--internalclientssl required</code>	<code>/internalclientssl-required</code>

See also [--certfile](#), [--keyfile](#), [--keypassword](#), and [--port](#).

40.32 --intruderlockout

Turns on intruder lockout processing, using defaults that can be overridden by the [--incorrectloginattempts](#), [--attemptsresetinterval](#), and [--lockoutresetinterval](#) switches. See [Section 36.3.5, “Enabling Intruder Detection,”](#) on page 516.

	Linux POA	Windows POA
Syntax:	<code>--intruderlockout</code>	<code>/intruderlockout</code>

40.33 --ip

Binds the POA to a specific IP address when the server where it runs uses multiple IP addresses, such as in a clustering environment. The specified IP address is associated with all ports used by the POA (HTTP, IMAP, LDAP, and so on.) Without the `--ip` switch, the POA binds to all available IP addresses and users can access the post office through all available IP addresses. See [Section 36.1.4, “Binding the POA to a Specific IP Address,”](#) on page 490.

	Linux POA	Windows POA
Syntax:	<code>--ip <i>IP_address</i></code> <code>--ip "<i>full_DNS_name</i>"</code>	<code>/ip-<i>IP_address</i></code> <code>/ip-"<i>full_DNS_name</i>"</code>
Example:	<code>--ip 172.16.5.18</code> <code>--ip "poasvr.provo.novell.com"</code>	<code>/ip-172.16.5.18</code> <code>/ip-"poasvr.provo.novell.com"</code>

See also [--cluster](#).

40.34 --keyfile

Specifies the full path to the private file used to provide secure SSL communication between the POA and other programs. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.

	Linux POA	Windows POA
Syntax:	<code>--keyfile /dir/file</code>	<code>/keyfile-[drive:]\dir\file</code> <code>/keyfile-\\svr\sharename\dir\file</code>
Example:	<code>--keyfile /certs/gw.key</code>	<code>/keyfile-\\ss\gw.key</code> <code>/keyfile-m:\ss\gw.key</code> <code>/keyfile-\\server2\c\ss\gw.key</code>

See also [--certfile](#) and [--keypassword](#).

40.35 --keypassword

Specifies the password used to encrypt the private SSL key file when it was created. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.

	Linux POA	Windows POA
Syntax:	<code>--keypassword password</code>	<code>/keypassword-password</code>
Example:	<code>--keypassword gwssl</code>	<code>/keypassword-gwssl</code>

See also [--certfile](#) and [--keyfile](#).

40.36 --language

Specifies the language to run the POA in, using a two-letter language code. You must install the POA in the selected language in order for the POA to display in the selected language.

The initial default is the language used in the post office. If that language has not been installed, the second default is the language used by the operating system. If that language has not been installed, the third default is English. You only need to use this switch if you need to override these defaults.

	Linux POA	Windows POA
Syntax:	<code>--language code</code>	<code>/language-code</code>
Example:	<code>--language de</code>	<code>/language-fr</code>

Contact your local Novell sales office for information about language availability. See [Chapter 7, “Multilingual GroupWise Systems,”](#) on page 123 for a list of language codes.

40.37 --ldapdisablepwdchg

Prevents GroupWise users from changing their LDAP passwords by using the Password dialog box in the GroupWise client. See [“Enabling LDAP Authentication for a Post Office” on page 512](#).

	Linux POA	Windows POA
Syntax:	--ldapdisablepwdchg	/ldapdisablepwdchg

See also [--ldapipaddr](#), [--ldapport](#), [--ldapuser](#), [--ldappwd](#), [--ldapuserauthmethod](#), [--ldapsl](#), [--ldapsslkey](#), and [--ldaptimeout](#).

40.38 --ldapipaddr

Specifies the LDAP server's network address as either an IP address or a DNS hostname. You can specify multiple network addresses to provide failover capabilities for your LDAP servers. See [“Specifying Failover LDAP Servers \(Non-SSL Only\)” on page 515](#).

	Linux POA	Windows POA
Syntax:	--ldapipaddr <i>network_address</i>	/ldapipaddr- <i>network_address</i>
Example:	--ldapipaddr 172.16.5.19 --ldapipaddr server1 server2	/ldapipaddr-172.16.5.20 /ldapipaddr-server1 server2

If you specify multiple LDAP servers, use a space between each address. When so configured, the POA tries to contact the first LDAP server in order to authenticate a user to GroupWise. If that LDAP server is down, the POA tries the next LDAP server in the list, and so on until it is able to authenticate.

See also [--ldapport](#), [--ldapuser](#), [--ldappwd](#), [--ldapuserauthmethod](#), [--ldapdisablepwdchg](#), [--ldapsl](#), [--ldapsslkey](#), and [--ldaptimeout](#).

40.39 --ldapipooln

Specifies a pooled LDAP server's network address as either an IP address or a DNS hostname. As many as five LDAP servers can participate together as a pool; therefore, *n* ranges from 1 to 5. See [“Configuring a Pool of LDAP Servers” on page 514](#).

	Linux POA	Windows POA
Syntax:	--ldapipooln <i>network_address</i>	/ldapipooln- <i>network_address</i>
Example:	--ldapipool1 172.16.5.18 --ldapipool2 server1 --ldapipool3 172.16.5.19	/ldapipool1-172.16.5.18 /ldapipool2-server1 /ldapipool3-172.16.5.19

See also [--ldapportpooln](#), [--ldapsslpooln](#), [--ldapsslkeypooln](#), and [--ldappoolresetime](#).

40.40 --ldappoolresetime

Specifies the number of minutes between the time when the POA receives an error response from a pooled LDAP server and the time when that LDAP server is reinstated into the pool of available LDAP servers. The default is 5 minutes; valid values range from 1 to 30. See [“Configuring a Pool of LDAP Servers” on page 514](#).

	Linux POA	Windows POA
Syntax:	--ldappoolresetime <i>minutes</i>	/ldappoolresetime- <i>minutes</i>
Example:	--ldappoolresetime 20	/ldappoolresetime-30

See also [--ldappippool*n*](#), [--ldapportpool*n*](#), [--ldapsslpool*n*](#), and [--ldapsslkeypool*n*](#).

40.41 --ldapport

Specifies the port number that the LDAP server listens on for authentication. The default is 389. See [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510](#).

	Linux POA	Windows POA
Syntax:	--ldapport <i>port_number</i>	/ldapport- <i>port_number</i>
Example:	--ldapport 391	/ldapport-392

See also [--ldapipaddr](#), [--ldapuser](#), [--ldappwd](#), [--ldapuserauthmethod](#), [--ldapdisablepwdchg](#), [--ldapssl](#), [--ldapsslkey](#), and [--ldaptimeout](#).

40.42 --ldapportpool*n*

Specifies the port number that pooled LDAP server *n* listens on for authentication. The default is 389. See [“Configuring a Pool of LDAP Servers” on page 514](#).

	Linux POA	Windows POA
Syntax:	--ldapportpool <i>n</i> <i>port</i>	/ldapportpool <i>n</i> - <i>port</i>
Example:	--ldapportpool3 391	/ldapportpool4-392

See also [--ldappippool*n*](#), [--ldappoolresetime](#), [--ldapsslpool*n*](#), and [--ldapsslkeypool*n*](#).

40.43 --ldappwd

Provides the password for the LDAP user that the POA uses to log in to the LDAP server. See [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510](#).

	Linux POA	Windows POA
Syntax:	--ldappwd <i>LDAP_password</i>	/ldappwd- <i>LDAP_password</i>

Linux POA	Windows POA
Example: --ldappwd gwldap	/ldappwd-gwldap

See also [--ldapipaddr](#), [--ldapport](#), [--ldapuser](#), [--ldapuserauthmethod](#), [--ldapdisablepwdchg](#), [--ldapssl](#), [--ldapsslkey](#), and [--ldaptimeout](#).

40.44 --ldapssl

Indicates to the POA that the LDAP server it is logging in to is using SSL. See [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,”](#) on page 510.

Linux POA	Windows POA
Syntax: --ldapssl	/ldapssl

See also [--ldapipaddr](#), [--ldapport](#), [--ldapuser](#), [--ldappwd](#), [--ldapuserauthmethod](#), [--ldapdisablepwdchg](#), [--ldapsslkey](#) and [--ldaptimeout](#).

40.45 --ldapsslpooln

Indicates to the POA that the pooled LDAP server it is logging in to is using SSL. See [“Configuring a Pool of LDAP Servers”](#) on page 514.

Linux POA	Windows POA
Syntax: --ldapsslpooln	/ldapsslpooln
Example: --ldapsslpool3	/ldapsslpool4

See also [--ldapippooln](#), [--ldapportpooln](#), [--ldappoolresettime](#), and [--ldapsslkeypooln](#).

40.46 --ldapsslkey

Specifies the full path to the SSL key file used with LDAP authentication. See [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,”](#) on page 510.

Linux POA	Windows POA
Syntax: --ldapsslkey <i>/dir/file</i>	/ldapsslkey-[drive:] <i>dir\file</i> /ldapsslkey-\\svl\sharename\dir\file
Example: --ldapsslkey /certs/gwkey.der	/ldapsslkey-ldap\gwkey.der /ldapsslkey-m:\ldap\gwkey.der /ldapsslkey-\\server2\c\ldap\gwkey.der

See also [--ldapipaddr](#), [--ldapport](#), [--ldapuser](#), [--ldappwd](#), [--ldapuserauthmethod](#), [--ldapdisablepwdchg](#), [--ldapssl](#) and [--ldaptimeout](#).

40.47 --ldapsslkeypool*n*

Specifies the full path to the SSL key file used with pooled LDAP server *n* for authentication. See [“Configuring a Pool of LDAP Servers” on page 514](#).

	Linux POA	Windows POA
Syntax:	<code>--ldapsslkeypool<i>n</i>-/dir/file</code>	<code>/ldapsslkeypool<i>n</i>-[drive:]\dir\file</code> <code>/ldapsslkeypool<i>n</i>-\\svr\sharename\dir\file</code>
Example:	<code>--ldapsslkeypool4 /certs/gwkey.der</code>	<code>/ldapsslkeypool4-\ldap\gwkey.der</code> <code>/ldapsslkeypool4-m:\ldap\gwkey.der</code> <code>/ldapsslkeypool4-\\svr2\c\ldap\gwkey.der</code>

See also `--ldapippooln`, `--ldapportpooln`, `--ldappoolresetime`, and `--ldapsslpooln`.

40.48 --ldaptimeout

Specifies the number of seconds that the POA connection to the LDAP server can be idle before the POA drops the connection. The default is 30 seconds. See [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510](#).

	Linux POA	Windows POA
Syntax:	<code>--ldaptimeout <i>seconds</i></code>	<code>/ldaptimeout-<i>seconds</i></code>
Example:	<code>--ldaptimeout 70</code>	<code>/ldaptimeout-80</code>

See also `--ldapipaddr`, `--ldapport`, `--ldapuser`, `--ldappwd`, `--ldapuserauthmethod`, `--ldapdisablepwdchg`, `--ldapssl`, and `--ldapsslkey`.

40.49 --ldapuser

Specifies the user name that the POA can use to log in to the LDAP server in order to authenticate GroupWise client users. See [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510](#).

	Linux POA	Windows POA
Syntax:	<code>--ldapuser <i>LDAP_user_ID</i></code>	<code>/ldapuser-<i>LDAP_user_ID</i></code>
Example:	<code>--ldapuser GWAAuth</code>	<code>/ldapuser-GWAAuth</code>

See also `--ldapipaddr`, `--ldapport`, `--ldappwd`, `--ldapuserauthmethod`, `--ldapdisablepwdchg`, `--ldapssl`, and `--ldapsslkey`, and `--ldaptimeout`.

40.50 --ldapuserauthmethod

Specifies the LDAP user authentication method you want the POA to use when accessing an LDAP server. Valid settings are bind and compare. See [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,”](#) on page 510.

	Linux POA	Windows POA
Syntax:	--ldapuserauthmethod <i>method</i>	/ldapuserauthmethod- <i>method</i>
Example:	--ldapuserauthmethod bind	/ldapuserauthmethod-compare

See also [--ldapuser](#), [--ldapipaddr](#), [--ldapport](#), [--ldappwd](#), [--ldapdisablepwdchg](#), [--ldapsl](#), and [--ldapslkey](#), and [--ldaptimeout](#).

40.51 --lockoutresetinterval

Specifies the length of time the user login is disabled after lockout. The default is 30 minutes; the minimum setting is 15; there is no maximum setting. The login can also be manually re-enabled in ConsoleOne in the GroupWise Account page of the User object. If --lockoutresetinterval is set to 0 (zero), the login must be re-enabled manually through ConsoleOne. See [Section 36.3.5, “Enabling Intruder Detection,”](#) on page 516.

	Linux POA	Windows POA
Syntax:	--lockoutresetinterval <i>minutes</i>	/lockoutresetinterval- <i>minutes</i>
Example:	--lockoutresetinterval 60	/lockoutresetinterval-90

See also [--intruderlockout](#), [--incorrectloginattempts](#), and [--attemptsresetinterval](#).

40.52 --log

Specifies the directory where the POA stores its log files. The default location varies by platform.

Linux: `/var/log/novell/groupwise/post_office_name.poa`

Windows: `post_office\wpcsout\ofs`

For more information, see [Section 37.3, “Using POA Log Files,”](#) on page 551.

	Linux POA	Windows POA
Syntax:	--log <i>dir</i>	/log-[<i>drive:</i>] <i>dir</i> /log-\\sv\ <i>sharename</i> \ <i>dir</i>
Example:	--log /gwsystem/logs	/log- <i>agt</i> \log /log-m: <i>agt</i> \log /log-\\server2\c\mail\i <i>agt</i> \log

You typically find multiple log files in the specified directory. The first four characters represent the date. The next three characters identify the agent. A three-digit extension allows for multiple log files created on the same day. For example, a log file named 0518poa.001 indicates that it is a POA log file, created on May 18. If you restarted the POA on the same day, a new log file is started, named 0518poa.002.

See also [--loglevel](#), [--logdiskoff](#), [--logdays](#), and [--logmax](#).

40.53 --logdays

Specifies how many days to keep POA log files on disk. The default is 30 days. See [Section 37.3, “Using POA Log Files,”](#) on page 551.

	Linux POA	Windows POA
Syntax:	<code>--logdays days</code>	<code>/logdays-days</code>
Example:	<code>--logdays 45</code>	<code>/logdays-60</code>

See also [--log](#), [--loglevel](#), [--logdiskoff](#), and [--logmax](#).

40.54 --logdiskoff

Turns off disk logging for the POA so no information about the functioning of the POA is stored on disk. The default is for logging to be turned on. See [Section 37.3, “Using POA Log Files,”](#) on page 551.

	Linux POA	Windows POA
Syntax:	<code>--logdiskoff</code>	<code>/logdiskoff</code>

See also [--loglevel](#).

40.55 --loglevel

Controls the amount of information logged by the POA. Logged information is displayed in the log message box and written to the POA log file during the current agent session.

The default is Normal, which displays only the essential information suitable for a smoothly running POA. Use Verbose to display the essential information, plus additional information helpful for troubleshooting. Verbose logging does not degrade POA performance, but log files saved to disk consume more disk space when verbose logging is in use. Diagnostic logging turns on *Extensive Logging Options* and *SOAP Logging Options* on the POA Web console Log Settings page. See [Section 37.3, “Using POA Log Files,”](#) on page 551.

	Linux POA	Windows POA
Syntax:	<code>--loglevel level</code>	<code>/loglevel-level</code>
Example:	<code>--loglevel verbose</code>	<code>/loglevel-diagnostic</code>

See also [--log](#), [--logdiskoff](#), [--logdays](#), and [--logmax](#).

40.56 --logmax

Sets the maximum amount of disk space for all POA log files. When the specified disk space is consumed, the POA deletes existing log files, starting with the oldest. The default is 102400 KB (100 MB). The maximum allowable setting is 102400000 (1 GB). Specify 0 (zero) for unlimited disk space. See [Section 37.3, “Using POA Log Files,”](#) on page 551.

	Linux POA	Windows POA
Syntax:	--logmax <i>kilobytes</i>	/logmax- <i>kilobytes</i>
Example:	--logmax 130000	/logmax-16000

See also [--log](#), [--loglevel](#), [--logdiskoff](#), and [--logdays](#).

40.57 --maxappconns

Sets the maximum number of application connections allowed between the POA and the GroupWise clients run by GroupWise users. The default maximum number of application connections is 2048. See [Section 38.1.2, “Adjusting the Number of Connections for Client/Server Processing,”](#) on page 561.

	Linux POA	Windows POA
Syntax:	--maxappconns <i>number</i>	/maxappconns- <i>number</i>
Example:	--maxappconns 4096	/maxappconns-5120

See also [--maxphysconns](#).

40.58 --maxphysconns

Sets the maximum number of physical TCP/IP connections allowed between the POA and the GroupWise clients run by GroupWise users. The default maximum number of physical connections is 2048. See [Section 38.1.2, “Adjusting the Number of Connections for Client/Server Processing,”](#) on page 561.

	Linux POA	Windows POA
Syntax:	--maxphysconns <i>number</i>	/maxphysconns- <i>number</i>
Example:	--maxphysconns 4096	/maxphysconns-5120

See also [--maxappconns](#).

40.59 --mtpinipaddr

Specifies the network address of the server where the POA runs, as either an IP address or a DNS hostname. See [“Using TCP/IP Links between the Post Office and the Domain” on page 487](#).

	Linux POA	Windows POA
Syntax:	<code>--mtpinipaddr network_addr</code>	<code>/mtpinipaddr-network_addr</code>
Example:	<code>--mtpinipaddr 172.16.5.19</code> <code>--mtpinipaddr server2</code>	<code>/mtpinipaddr-172.16.5.20</code> <code>/mtpinipaddr-server3</code>

See also [--mtpinport](#), [--mtpoutipaddr](#), [--mtpoutport](#), [--mtpsendmax](#), and [--nomtp](#).

40.60 --mtpinport

Sets the message transfer port number the POA listens on for messages from the MTA. The default is 7101. See [“Using TCP/IP Links between the Post Office and the Domain” on page 487](#).

	Linux POA	Windows POA
Syntax:	<code>--mtpinport port_number</code>	<code>/mtpinport-port_number</code>
Example:	<code>--mtpinport 7202</code>	<code>/mtpinport-7203</code>

See also [--mtpinipaddr](#), [--mtpoutipaddr](#), [--mtpoutport](#), [--mtpsendmax](#), and [--nomtp](#).

40.61 --mtpoutipaddr

Specifies the network address of the server where the MTA for the domain runs, as either an IP address or a DNS hostname. See [“Using TCP/IP Links between the Post Office and the Domain” on page 487](#).

	Linux POA	Windows POA
Syntax:	<code>--mtpoutipaddr network_address</code>	<code>/mtpoutipaddr-network_address</code>
Example:	<code>--mtpoutipaddr 172.16.5.19</code> <code>--mtpoutipaddr server3</code>	<code>/mtpoutipaddr-172.16.5.19</code> <code>/mtpoutipaddr-server4</code>

See also [--mtpinipaddr](#), [--mtpinport](#), [--mtpoutport](#), [--mtpsendmax](#), and [--nomtp](#).

40.62 --mtpoutport

Specifies the message transfer port number the MTA listens on for messages from the POA. The default is 7100. See [“Using TCP/IP Links between the Post Office and the Domain” on page 487](#).

	Linux POA	Windows POA
Syntax:	--mtpoutport <i>port_number</i>	/mtpoutport- <i>port_number</i>
Example:	--mtpoutport 7300	/mtpoutport-7400

See also [--mtpinipaddr](#), [--mtpinport](#), [--mtpoutipaddr](#), [--mtpsendmax](#), and [--nomtp](#).

40.63 --mtpsendmax

Sets the maximum size in megabytes for messages being sent outside the post office. By default, messages of any size can be transferred to the MTA. See [Section 36.2.7, “Restricting Message Size between Post Offices,” on page 504](#).

	Linux POA	Windows POA
Syntax:	--mtpsendmax <i>megabytes</i>	/mtpsendmax- <i>megabytes</i>
Example:	--mtpsendmax 4	/mtpsendmax-6

See also [--mtpinipaddr](#), [--mtpinport](#), [--mtpoutipaddr](#), [--mtpoutport](#), and [--nomtp](#).

40.64 --mtpssl

Sets the availability of secure SSL communication between the POA and its MTA. Valid settings are enabled and disabled. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,” on page 508](#).

	Linux POA	Windows POA
Syntax:	--mtpssl <i>setting</i>	/mtpssl- <i>setting</i>
Example:	--mtpssl enabled	/mtpssl-enabled

See also [--certfile](#), [--keyfile](#) and [--keypassword](#).

40.65 --name

Specifies the object name of the POA object in the post office. If you have multiple POAs configured for the same post office, you must use this switch to specify which POA configuration to use when the POA starts. Several useful configurations include multiple POAs for a single post office, as described in the following sections:

- ♦ [Section 38.1.3, “Configuring a Dedicated Client/Server POA \(Windows Only\),” on page 562](#)
- ♦ [Section 38.2.2, “Configuring a Dedicated Message File Processing POA \(Windows Only\),” on page 565](#)

- ♦ [Section 39.5, “Configuring a Dedicated Indexing POA \(Windows Only\),”](#) on page 577
- ♦ [Section 38.4.2, “Configuring a Dedicated Database Maintenance POA \(Windows Only\),”](#) on page 568

	Linux POA	Windows POA
Syntax:	<code>--name <i>object_name</i></code>	<code>/name-<i>object_name</i></code>
Example:	<code>--name POA2</code>	<code>/name-POA2</code>

40.66 --noada

Disables the POA admin thread. For an explanation of the POA admin thread, see [“POA Admin Thread Status Box”](#) on page 529.

The POA admin thread must run for at least one POA for each post office. However, it can be disabled for POAs with specialized functioning where the database update and repair activities of the POA admin thread could interfere with other, more urgent processing.

	Linux POA	Windows POA
Syntax:	<code>--noada</code>	<code>/noada</code>

Historical Note: In GroupWise 5.2 and earlier, a separate agent, the Administration Agent (ADA), handled the functions now consolidated into the POA admin thread. Hence the switch name, `--noada`.

40.67 --nocache

Disables database caching. The default is for caching to be turned on. Use this switch if your backup system cannot back up open files.

	Linux POA	Windows POA
Syntax:	<code>--nocache</code>	<code>/nocache</code>

40.68 --noconfig

Ignores any configuration information provided for the POA in ConsoleOne and uses only settings from the POA startup file. The default is for the POA to use the information provided in ConsoleOne, overridden as needed by settings provided in the startup file or on the command line.

	Linux POA	Windows POA
Syntax:	<code>--noconfig</code>	<code>/noconfig</code>

40.69 --nodca

Prevents the POA from starting the Document Converter Agent (DCA). The default is for the POA to start the DCA, as described in [Section 39.2, “Configuring the Document Converter Agent \(DCA\),”](#) on page 575.

	Linux POA	Windows POA
Syntax:	--nodca	/nodca

40.70 --noerrormail

Prevents problem files from being sent to the GroupWise administrator. The default is for error mail to be sent to the administrator. See [Section 37.7, “Notifying the GroupWise Administrator,”](#) on page 557.

	Linux POA	Windows POA
Syntax:	--noerrormail	/noerrormail

40.71 --nogwchk

Turns off Mailbox/Library Maintenance processing for the POA. The default is for the POA to perform Mailbox/Library Maintenance tasks requested from ConsoleOne and configured as POA scheduled events.

	Linux POA	Windows POA
Syntax:	--nogwchk	/nogwchk

See also [--gwchkthreads](#).

40.72 --nomf

Turns off all message file processing for the POA. The default is for the POA to process all message files.

Two specialized configurations that require turning off message files are described in [Section 38.1.3, “Configuring a Dedicated Client/Server POA \(Windows Only\),”](#) on page 562 and [Section 39.5, “Configuring a Dedicated Indexing POA \(Windows Only\),”](#) on page 577.

	Linux POA	Windows POA
Syntax:	--nomf	/nomf

See also [--nomfhigh](#) and [--nomflow](#).

40.73 --nomfhigh

Turns off processing high priority messages files (message queues 0 and 1). For information about message queues, see “Post Office Directory” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

	Linux POA	Windows POA
Syntax:	--nomfhigh	/nomfhigh

See also [--nomf](#) and [--nomflow](#).

40.74 --nomflow

Turns off processing lower priority messages files (message queues 2 through 7). For information about message queues, see “Post Office Directory” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

	Linux POA	Windows POA
Syntax:	--nomflow	/nomflow

See also [--nomf](#) and [--nomfhigh](#).

40.75 --nomtp

Disables Message Transfer Protocol, so that a TCP/IP link cannot be used between the POA and the MTA. See [Section 36.1.3, “Changing the Link Protocol between the Post Office and the Domain,”](#) on page 487.

	Linux POA	Windows POA
Syntax:	--nomtp	/nomtp

See also [--mtpinipaddr](#), [--mtpinport](#), [--mtpoutipaddr](#), [--mtpoutport](#), and [--mtpsendmax](#).

40.76 --nonuu

Disables nightly user upkeep. See [Section 36.4.3, “Performing Nightly User Upkeep,”](#) on page 523.

	Linux POA	Windows POA
Syntax:	--nonuu	/nonuu

See also [--nuuoffset](#).

40.77 --noqf

Disables the periodic QuickFinder indexing done by the POA. The default is for periodic indexing to be turned on. See [Section 39.1, “Regulating Indexing,”](#) on page 573.

	Linux POA	Windows POA
Syntax:	--noqf	/noqf

See also [--qfinterval](#), [--qfintervalinminute](#), [--qfbaseoffset](#), and [--qfbaseoffsetinminute](#).

40.78 --nordab

Disables daily generation of the GroupWise Address Book for Remote users. See [Section 36.4.3, “Performing Nightly User Upkeep,”](#) on page 523.

	Linux POA	Windows POA
Syntax:	--nordab	/nordab

See also [--rdaboffset](#).

40.79 --norecover

Disables automatic database recovery. The default is for automatic database recovery to be turned on.

If the POA detects a problem with a database when automatic database recovery has been turned off, the POA notifies the administrator, but it does not recover the problem database. The administrator can then recover or rebuild the database as needed. See [Chapter 26, “Maintaining Domain and Post Office Databases,”](#) on page 401.

Two specialized configurations that require turning off automatic database recovery are described in [Section 38.1.3, “Configuring a Dedicated Client/Server POA \(Windows Only\),”](#) on page 562 and [Section 39.5, “Configuring a Dedicated Indexing POA \(Windows Only\),”](#) on page 577.

	Linux POA	Windows POA
Syntax:	--norecover	/norecover

40.80 --nosnmp

Disables SNMP for the POA. The default is to have SNMP enabled. See [Section 37.6, “Using an SNMP Management Console,”](#) on page 553.

	Linux POA	Windows POA
Syntax:	--nosnmp	/nosnmp

40.81 --notcpip

Disables TCP/IP communication for the POA. The default is to have TCP/IP communication enabled. Use this switch if you do not want this POA to communicate with GroupWise clients using TCP/IP.

Linux POA	Windows POA
Syntax: --notcpip	/notcpip

Two specialized configurations that require turning off automatic database recovery are described in [Section 38.2.2, “Configuring a Dedicated Message File Processing POA \(Windows Only\),”](#) on page 565 and [Section 39.5, “Configuring a Dedicated Indexing POA \(Windows Only\),”](#) on page 577.

40.82 --nuuoffset

Specifies the number of hours after midnight for the POA to start performing user upkeep. The default is 1 hour; valid values range from 0 to 23. See [Section 36.4.3, “Performing Nightly User Upkeep,”](#) on page 523.

Linux POA	Windows POA
Syntax: --nuuoffset <i>hours</i>	/nuuoffset- <i>hours</i>
Example: --nuuoffset 3	/nuuoffset-4

See also [--nonuu](#).

40.83 --password

Provides the password for the POA to use when accessing post offices or document storage areas on remote servers. You can also provide user and password information on the Post Office Settings page in ConsoleOne.

Linux POA	Windows POA
Syntax: --password <i>network_password</i>	/password- <i>network_password</i>
Example: --password Gwise	/password-Gwise

See also [--user](#).

40.84 --port

Sets the TCP port number used for the POA to communicate with GroupWise clients in client/server access mode. The default is 1677. See [Section 36.2.1, “Using Client/Server Access to the Post Office,”](#) on page 494.

Linux POA	Windows POA
Syntax: --port <i>port_number</i>	/port- <i>port_number</i>

Linux POA	Windows POA
Example: --port 1679	/port-1680

See also [--ip](#).

40.85 --primingmax

Sets the maximum number of client/server handler threads that POA can use for priming users' Caching mailboxes. The default is 30 per cent. See [Section 36.2.6, "Supporting Forced Mailbox Caching,"](#) on page 503.

Linux POA	Windows POA
Syntax: --primingmax <i>percentage</i>	/primingmax- <i>percentage</i>
Example: --primingmax 50	/primingmax-60

See also [--tcpthreads](#).

40.86 --qfbaseoffset

Specifies the number of hours after midnight for the POA to start its indexing cycle as specified by the [--qfinterval](#) or [--qfintervalinminute](#) switch. The default is 20 hours (meaning at 8:00 p.m.); valid values range from 0 to 23. See [Section 39.1, "Regulating Indexing,"](#) on page 573.

Linux POA	Windows POA
Syntax: --qfbaseoffset <i>hours</i>	/qfbaseoffset- <i>hours</i>
Example: --qfbaseoffset 2	/qfbaseoffset-3

See also [--qfbaseoffsetinminute](#), [--qfinterval](#), [--qfintervalinminute](#), and [--noqf](#).

40.87 --qfbaseoffsetinminute

Specifies the number of minutes after midnight for the POA to start its indexing cycle as specified by the [--qfinterval](#) or [--qfintervalinminute](#) switch. The default is 20 hours (1200 minutes, meaning at 8:00 p.m.). The maximum setting is 1440 (24 hours). See [Section 39.1, "Regulating Indexing,"](#) on page 573.

Linux POA	Windows POA
Syntax: --qfbaseoffsetinminute <i>minutes</i>	/qfbaseoffsetinminute- <i>minutes</i>
Example: --qfbaseoffset 45	/qfbaseoffset-90

See also [--qfbaseoffset](#), [--qfinterval](#), [--qfintervalinminute](#), and [--noqf](#).

40.88 --qfdeleteold

Deletes previous versions of QuickFinder `.idx` and `.inc` files to conserve disk space during periods of heavy indexing. In general, it is applicable for use only with `--qflevel=1`, where indexing activities are a lower priority task than user activities in their mailboxes. See [“Reclaiming Disk Space” on page 580](#).

	Linux POA	Windows POA
Syntax:	<code>--qfdeleteold</code>	<code>/qfdeleteold</code>

See also `--qflevel`, `--qfnolib`, `--qfnopreproc`, `--qfnousers`, `--qfusefidbeg`, and `--qfusefidend`.

40.89 --qfinterval

Specifies the interval in hours for the POA to update the QuickFinder indexes in the post office. The default is 24 hours. See [Section 39.1, “Regulating Indexing,” on page 573](#).

	Linux POA	Windows POA
Syntax:	<code>--qfinterval hours</code>	<code>/qfinterval-hours</code>
Example:	<code>--qfinterval-6</code>	<code>/qfinterval-2</code>

See also `--qfbaseoffset`, `--qfbaseoffsetinminute`, `--qfintervalinminute`, and `--noqf`.

40.90 --qfintervalinminute

Specifies the interval in minutes for the POA to update the QuickFinder indexes in the post office. The default is 24 hours (1440 minutes). See [Section 39.1, “Regulating Indexing,” on page 573](#).

	Linux POA	Windows POA
Syntax:	<code>--qfintervalinminute minutes</code>	<code>/qfintervalinminute-minutes</code>
Example:	<code>--qfintervalinminute 30</code>	<code>/qfintervalinminute-120</code>

See also `--qfinterval`, `--qfbaseoffset`, `--qfbaseoffsetinminute`, and `--noqf`.

40.91 --qflevel

Customizes the way the POA performs indexing. Valid levels are 0 through 3 and 999. See [“Determining Indexing Priority” on page 580](#)

	Linux POA	Windows POA
Syntax:	<code>--qflevel level</code>	<code>/qflevel-level</code>
Example:	<code>--qflevel 3</code>	<code>/qflevel-999</code>

The following table describes the functionality of each level:

Priority Level	Description
0	Index a maximum of 1000 items at a time, rather than the default of 500.
1	Index a maximum of 500 items at time using a low priority thread. This keeps frequent daytime indexing cycles from interfering with users' activities in their mailboxes.
2	Index a maximum of 1000 items at a time using a medium priority thread. This allows additional items in each database to be processed in each indexing cycle. Use of a medium priority thread makes indexing more important than some user activities in their mailboxes. Users might notice some slowness in response from the GroupWise client.
3	Index a maximum of 2000 items at a time using a high priority thread. Use of a high priority thread makes indexing more important than many users activities in their mailboxes. Users will notice some slowness in response from the GroupWise client. This is warranted only when the completion of the indexing immediately is extremely important.
999	Index constantly until all databases have been indexed, then wait until the next indexing cycle set on the QuickFinder property page of the POA object before starting to index again.

See also [--qfdeleteold](#), [--qfnolib](#)s, [--qfnopreproc](#), [--qfnousers](#), [--qfusefidbeg](#), and [--qfuserfidend](#).

40.92 --qfnolib

Suppresses QuickFinder indexing of documents in libraries in favor of indexing user mailbox contents. For full suppression, use [--qfnopreproc](#) as well. See [“Determining What to Index” on page 579](#)

	Linux POA	Windows POA
Syntax:	<code>--qfnolib</code> s	<code>/qfnolib</code> s

See also [--qfdeleteold](#), [--qflevel](#), [--qfnopreproc](#), [--qfnousers](#), [--qfusefidbeg](#), and [--qfuserfidend](#).

40.93 --qfnopreproc

Suppresses generation of document word lists that are normally written to user databases when libraries are indexed. Use with [--qfnolib](#)s. See [“Determining What to Index” on page 579](#).

	Linux POA	Windows POA
Syntax:	<code>--qfnopreproc</code>	<code>/qfnopreproc</code>

See also [--qfdeleteold](#), [--qflevel](#), [--qfnolib](#)s, [--qfnousers](#), [--qfusefidbeg](#), and [--qfuserfidend](#).

40.94 --qfnousers

Suppresses QuickFinder indexing of user mailbox contents in favor of indexing documents in libraries. See [“Determining What to Index” on page 579](#).

	Linux POA	Windows POA
Syntax:	--qfnousers	/qfnouser

See also [--qfdeleteold](#), [--qflevel](#), [--qfnolib](#), [--qfnopreproc](#), [--qfusefidbeg](#), and [--qfuserfidend](#).

40.95 --qfuserfidbeg

Specifies the beginning of a range of FIDs associated with user databases ([userxxx.db](#)) that you want to index. The *xxx* in the user database file name is the FID. To determine what FIDs are in use, list the contents of the [ofuser](#) directory in the post office directory. See [“Determining What to Index” on page 579](#).

	Linux POA	Windows POA
Syntax:	--qfuserfidbeg <i>fid</i>	/qfuserfidbeg- <i>fid</i>
Example:	--qfuserfidbeg 7ck	/qfuserfidbeg-7j6

See also [--qfdeleteold](#), [--qflevel](#), [--qfnolib](#), [--qfnopreproc](#), [--qfnousers](#), and [--qfuserfidend](#).

40.96 --qfuserfidend

Specifies the end of a range of FIDs associated with user databases ([userxxx.db](#)) that you want to index. The *xxx* in the user database file name is the FID. To determine what FIDs are in use, list the contents of the [ofuser](#) directory in the post office directory. See [“Determining What to Index” on page 579](#).

	Linux POA	Windows POA
Syntax:	--qfuserfidend <i>fid</i>	/qfuserfidend- <i>fid</i>
Example:	--qfuserfidend x9c	/qfuserfidend-zzf

If you want to index just one user database, use the same FID with the [--qfuserfidbeg](#) switch and the [--qfuserfidend](#) switch. To determine a user’s FID, click *Help > About GroupWise* in the GroupWise client. In Online mode, the FID is displayed after the user name. In Caching or Remote mode, the FID is the last three characters of the Caching or Remote directory name (for example, *gwstr7bh*).

See also [--qfdeleteold](#), [--qflevel](#), [--qfnolib](#), [--qfnopreproc](#), [--qfnousers](#), and [--qfuserfidbeg](#).

40.97 --rdaboffset

Specifies the number of hours after midnight for the POA to generate the daily copy of the GroupWise Address Book for Remote users. The default is 0; valid values range from 0 to 23. See [Section 36.4.3, “Performing Nightly User Upkeep,” on page 523](#).

	Linux POA	Windows POA
Syntax:	--rdaboffset <i>hours</i>	/rdaboffset- <i>hours</i>
Example:	--rdaboffset 3	/rdaboffset-4

See also [--nordab](#).

40.98 --rights

Verifies that the POA has the required network rights or permissions to all directories where it needs access in the post office directory.

When it is started with this switch, the POA lists directories it is checking, which can be a lengthy process. Use this switch on an as needed basis, not in the POA startup file. If the POA encounters inadequate rights or permissions, it indicates the problem and shuts down.

	Linux POA	Windows POA
Syntax:	--rights	/rights

40.99 --show

Starts the Linux POA with a server console interface similar to that provided for the Windows POA. This user interface requires that the X Window System and Open Motif are running on the Linux server.

	Linux POA	Windows POA
Syntax:	--show	N/A

The --show switch cannot be used in the POA startup file. However, if you want the POA to start with a user interface when you run the `grpwise` script or when the server reboots, you can configure the GroupWise High Availability service (gwaha) to accomplish this, as described in [“Configuring the GroupWise High Availability Service in the gwaha.conf File”](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.

40.100 --soap

Enables SOAP so that the POA can communicate with SOAP clients. Valid settings are enabled and disabled. See [Section 36.2.4, “Supporting SOAP Clients,” on page 499](#).

	Linux POA	Windows POA
Syntax:	--soap enabled or disabled	/soap-enabled or disabled
Example:	--soap enabled	/soap-disabled

See also [--soapmaxthreads](#), [--soapport](#), [--soapsizelimit](#), [--soapssl](#), and [--soapthreads](#).

40.101 --soapmaxthreads

Specifies the maximum number of SOAP threads the POA can create to service SOAP clients. The default is 4; the maximum is 40. This setting is appropriate for most systems. See [Section 36.2.4, “Supporting SOAP Clients,” on page 499](#).

	Linux POA	Windows POA
Syntax:	--soapmaxthreads <i>number</i>	/soapmaxthreads- <i>number</i>
Example:	--soapmaxthreads 20	/soapmaxthreads-30

See also [--soap](#), [--soapport](#), [--soapsizelimit](#), [--soapssl](#), and [--soapthreads](#).

40.102 --soapport

Sets the TCP port number used for the POA to communicate with SOAP clients. The default is 7191. See [Section 36.2.4, “Supporting SOAP Clients,” on page 499](#).

	Linux POA	Windows POA
Syntax:	--soapport <i>port_number</i>	/soapport- <i>port_number</i>
Example:	--soapport 146	/soapport-147

See also [--soap](#), [--soapmaxthreads](#), [--soapsizelimit](#), [--soapssl](#), and [--soapthreads](#).

40.103 --soapsizelimit

Sets the maximum amount of data that the POA can return in a single request from a SOAP client. The default is 1024 KB (1 MB), which is the recommended setting. The maximum allowed setting is 65534 (64 MB). Specify 0 (zero) if you do not want the POA to check the data size.

	Linux POA	Windows POA
Syntax:	--soapsizelimit <i>kilobytes</i>	/soapsizelimit- <i>kilobytes</i>
Example:	--soapsizelimit 2048	/soapsizelimit-2048

See also [--soap](#), [--soapmaxthreads](#), [--soapport](#), [--soapssl](#), and [--soapthreads](#).

40.104 --soapssl

Sets the availability of secure SSL communication between the POA and SOAP clients. Valid settings are enable and disable. See [Section 36.3.3, "Securing the Post Office with SSL Connections to the POA,"](#) on page 508.

	Linux POA	Windows POA
Syntax:	<code>--soapssl <i>setting</i></code>	<code>/soapssl-<i>setting</i></code>
Example:	<code>--soapssl enable</code>	<code>/soapssl-enable</code>

See also [--soap](#), [--soapmaxthreads](#), [--soapport](#), [--soapsizelimit](#), and [--soapthreads](#).

40.105 --soapthreads

Sets the initial number of SOAP threads that the POA starts to service SOAP clients. The default is 4. The POA automatically starts additional threads as needed. See [Section 36.2.4, "Supporting SOAP Clients,"](#) on page 499.

	Linux POA	Windows POA
Syntax:	<code>--soapthreads <i>number</i></code>	<code>/soapthreads-<i>number</i></code>
Example:	<code>--soapthreads 8</code>	<code>/soapthreads-10</code>

See also [--soap](#), [--soapmaxthreads](#), [--soapport](#), [--soapsizelimit](#), and [--soapssl](#).

40.106 --tcpthreads

Specifies the maximum number of client/server handler threads the POA can create to service client/server requests. The default is 10; valid values range from 1 to 99. Plan on about one client/server handler thread per 20-30 client/server users. See [Section 38.1.1, "Adjusting the Number of POA Threads for Client/Server Processing,"](#) on page 559.

	Linux POA	Windows POA
Syntax:	<code>--tcpthreads <i>number</i></code>	<code>/tcpthreads-<i>number</i></code>
Example:	<code>--tcpthreads 30</code>	<code>/tcpthreads-50</code>

See also [--primingmax](#).

40.107 --threads

Specifies the maximum number of message handler threads the POA can create. The default is 8; valid values range from 1 to 20. See [Section 38.2.1, “Adjusting the Number of POA Threads for Message File Processing,”](#) on page 564.

	Linux POA	Windows POA
Syntax:	--threads <i>number</i>	/threads- <i>number</i>
Example:	--threads 15	/threads-20

40.108 --usedva

Configures the POA to use the DVA instead of the DCA to convert documents into HTML format for indexing. See [Section 39.3, “Enabling the Document Viewer Agent \(DVA\) for Indexing,”](#) on page 576.

	Linux POA	Windows POA
Syntax:	--usedva	/usedva

See also [--dvanipaddr](#), [--dvanport](#), and [--dvanssl](#).

40.109 --user

Provides the network user ID for the POA to use when accessing post offices and/or document storage areas on remote servers. You can also provide user and password information on the Post Office Settings page in ConsoleOne.

	Linux POA	Windows POA
Syntax:	--user <i>Linux_user_ID</i>	/user- <i>Windows_user_ID</i>
Example:	--user GWAgents	/user-GWAgents

Linux: On OES Linux, the *Linux_user_ID* is a Linux-enabled user that the POA can use to log in to the remote OES Linux server. On SLES Linux, it is a standard Linux user.

Windows: The *Windows_user_ID* is a user that the POA can use to log in to the remote Windows server.

See also [--password](#).

Windows Note: The Windows POA gains access to the post office directory when it starts. However, a particular user might attempt to access a remote document storage area to which the POA does not yet have a drive mapping available. By default, the POA attempts to map a drive using the same user ID and password it used to access the post office directory. If the user ID and password for the remote storage area are different from the post office, use the --user and --password switches to specify the needed user ID and password. You can also provide user and password information on the Post Office Settings page in ConsoleOne. However, it is preferable to use the same user ID and password on all servers where the POA needs access.

X Message Transfer Agent

- ♦ Chapter 41, “Understanding Message Transfer between Domains and Post Offices,” on page 621
- ♦ Chapter 42, “Configuring the MTA,” on page 627
- ♦ Chapter 43, “Monitoring the MTA,” on page 659
- ♦ Chapter 44, “Optimizing the MTA,” on page 685
- ♦ Chapter 45, “Using MTA Startup Switches,” on page 693

For a complete list of port numbers used by the MTA, see [Section A.4, “Message Transfer Agent Port Numbers,”](#) on page 1169.

For detailed Linux-specific MTA information, see [Appendix C, “Linux Commands, Directories, and Files for GroupWise Administration,”](#) on page 1179.

For additional assistance in managing the MTA, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

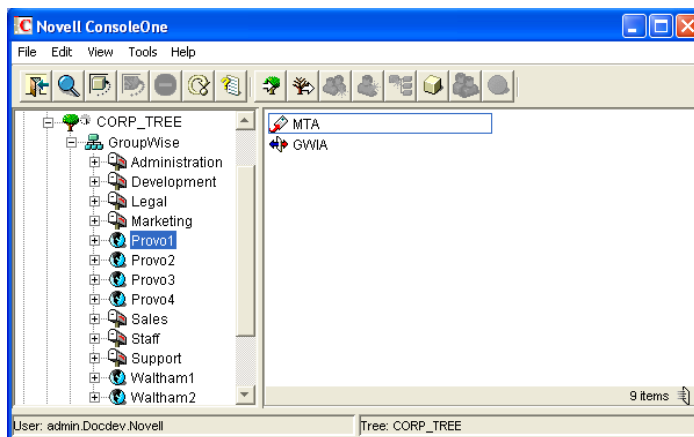
41 Understanding Message Transfer between Domains and Post Offices

A domain organizes post offices into a logical grouping for addressing, routing, and administration purposes in your GroupWise system. Messages are transferred between post offices and domains by the Message Transfer Agent (MTA). The following topics help you understand domains and the functions of the MTA:

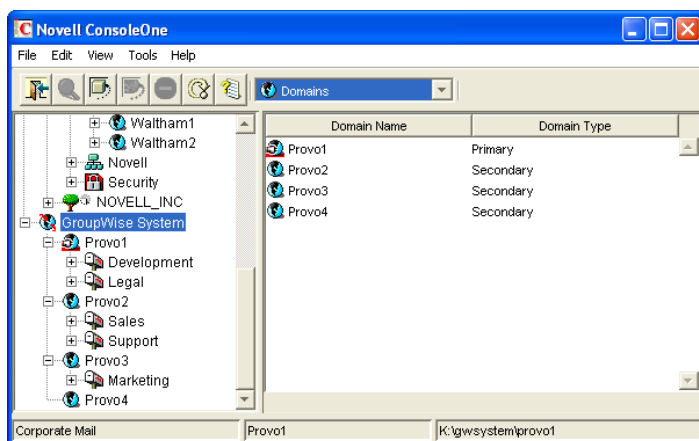
- ◆ Section 41.1, “Domain Representation in ConsoleOne,” on page 621
- ◆ Section 41.2, “Domain Directory Structure,” on page 622
- ◆ Section 41.3, “Information Stored in the Domain,” on page 622
- ◆ Section 41.4, “Role of the Message Transfer Agent,” on page 624
- ◆ Section 41.5, “Link Configuration between Domains and Post Offices,” on page 624
- ◆ Section 41.6, “Message Flow between Domains and Post Offices,” on page 624

41.1 Domain Representation in ConsoleOne

In ConsoleOne, domains are container objects that contain an MTA object, as well as other domain-related objects, as shown below:



Although each post office is linked to a domain, it does not display as subordinate to the domain in the Console View. However, using the GroupWise View, you can display post offices as subordinate to the domains to which they are linked in your GroupWise system.



41.2 Domain Directory Structure

Physically, a domain consists of a set of directories that house all the information stored in the domain. See “[Domain Directory](#)” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

41.3 Information Stored in the Domain

The following types of information are stored in the domain:

- [Section 41.3.1, “Domain Database,”](#) on page 622
- [Section 41.3.2, “Agent Input/Output Queues in the Domain,”](#) on page 623
- [Section 41.3.3, “Gateways,”](#) on page 623

No messages are stored in the domain, so GroupWise client users do not need access to the domain directory. The only person who needs file access to the domain directory is the GroupWise administrator.

41.3.1 Domain Database

The domain database (`wpdomain.db`) contains all administrative information for the domain, including:

- Address information about all GroupWise objects (such as users, resources, post offices, and gateways in the domain)
- System configuration and linking information for the domain’s MTA
- Address and message routing information to other domains

The first domain you create is the primary domain. In the primary domain, the `wpdomain.db` file contains all administrative information for your entire GroupWise system (all its domains, post offices, users, and so on). Because the `wpdomain.db` file in the primary domain is so crucial, you should back it up regularly and keep it secure. See [Section 31.1, “Backing Up a Domain,”](#) on page 431.

You can re-create your entire GroupWise system from the primary domain `wpdomain.db` file; however, if the primary domain `wpdomain.db` file becomes unusable, you can no longer make administrative updates to your GroupWise system.

Secondary domains are automatically synchronized to match the primary domain.

41.3.2 Agent Input/Output Queues in the Domain

Each domain contains agent input/output queues where messages are deposited and picked up for processing by the MTA.

For a mapped or UNC link between domains, the MTA requires read/write access rights to its input/output queues in the other domains. For a TCP/IP link, no access rights are required because messages are communicated by way of TCP/IP.

For illustrations of the processes presented below, see [Section 41.6, “Message Flow between Domains and Post Offices,”](#) on page 624.

MTA Input Queue in the Domain

The MTA input queue in the local domain (*domain\wpcsin*) is where MTAs for other domains deposit user messages for the local MTA to route to local post offices or to route to other domains. Thus, the MTA input queue in the local domain is the output queue for the MTAs in many other domains.

The MTA does not have an output queue for user messages in the local domain. Because its primary task is routing messages, the local MTA has output queues in all post offices in the domain. See [“POA Input Queue in the Post Office”](#) on page 475. The local MTA also has output queues in all domains to which it is directly linked.

MTA Output Queue in the Domain

The MTA output queue in the local domain (*domain\wpcout\ads*) is where the MTA deposits administrative messages from other domains for the MTA admin thread to pick up.

MTA Admin Thread Input Queue in the Domain

The MTA admin thread input queue (*domain\wpcout\ads*) is, of course, the same as the MTA output queue in the local domain. The MTA admin thread picks up administrative messages deposited in the queue by the MTA and updates the domain database.

MTA Admin Thread Output Queue in the Domain

The MTA admin thread output queue (*domain\wpcsin*) is the same as the MTA input queue in the local domain. The MTA admin thread deposits administrative messages in the queue for replication to other domains.

41.3.3 Gateways

Gateways are installed and configured at the domain level of your GroupWise system.

NOTE: GroupWise gateways are legacy products that are not supported with the current GroupWise version.

41.4 Role of the Message Transfer Agent

You must run an MTA for each domain. The MTA:

- ♦ Routes messages between post offices in the local domain.
- ♦ Routes messages between domains.
- ♦ Routes messages to and from gateways installed in the local domain.
- ♦ Routes messages between GroupWise systems across the Internet if appropriate DNS lookup capabilities have been set up.
See [“Using Dynamic Internet Links”](#) in [“Connecting to Other GroupWise Systems”](#) in the *GroupWise 2012 Multi-System Administration Guide*.
- ♦ Schedules routing of messages across expensive links.
See [Section 42.3.2, “Scheduling Direct Domain Links,”](#) on page 647.
- ♦ Controls the size of messages that can pass across links.
See [Section 42.2.1, “Restricting Message Size between Domains,”](#) on page 642.
- ♦ Updates the domain database (`wpdomain.db`) whenever GroupWise users, resources, post offices, or other GroupWise objects are added, modified, or deleted.
- ♦ Replicates updates to all domains and post offices throughout your GroupWise system. This keeps the Address Book up-to-date for all GroupWise users.
- ♦ Synchronizes GroupWise user information with Novell eDirectory user information. This handles updates made in ConsoleOne without the GroupWise Administrator snap-in running.
See [Section 42.4.1, “Using eDirectory User Synchronization,”](#) on page 652.
- ♦ Synchronizes GroupWise object information throughout your GroupWise system as needed.
- ♦ Detects and repairs invalid information in the domain database (`wpdomain.db`).
- ♦ Provides logging and statistics about GroupWise message flow.
See [Section 42.4.2, “Enabling MTA Message Logging,”](#) on page 657.

41.5 Link Configuration between Domains and Post Offices

In GroupWise, a link is defined as the information required to route messages between domains, post offices, and gateways in a GroupWise system. Links are created and configured when new domains, post offices, and gateways are created.

For more specific information about how domains are linked to each other, and about how domains and post offices are linked, see [Chapter 10, “Managing the Links between Domains and Post Offices,”](#) on page 155.

41.6 Message Flow between Domains and Post Offices

- ♦ [Section 41.6.1, “Message Flow between Post Offices in the Same Domain,”](#) on page 625
- ♦ [Section 41.6.2, “Message Flow between Different Domains,”](#) on page 625

41.6.1 Message Flow between Post Offices in the Same Domain

To see what happens to message flow within the domain when the domain is closed, view the following message flow diagrams:

- ♦ [“TCP/IP Link Open: Transfer between Post Offices Successful”](#)
- ♦ [“TCP/IP Link Closed: Transfer between Post Offices Delayed”](#)

These diagrams are found in [“Message Delivery to a Different Post Office”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

41.6.2 Message Flow between Different Domains

To see what happens to message flow when the destination domain is closed, view the following message flow diagrams:

- ♦ [“TCP/IP Link Open: Transfer between Domains Successful”](#)
- ♦ [“TCP/IP Link Closed: Transfer between Domains Delayed”](#)

These diagrams are found in [“Message Delivery to a Different Domain”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

42 Configuring the MTA

For MTA system requirements, see “[Agent System Requirements](#)” in the *GroupWise 2012 Installation Guide*. For detailed instructions about installing and starting the MTA for the first time, see “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.

As your GroupWise system grows and evolves, you will probably need to modify MTA configuration to meet changing system needs. The following topics help you configure the MTA:

- ♦ [Section 42.1, “Performing Basic MTA Configuration,” on page 627](#)
 - [Creating an MTA Object in eDirectory](#)
 - [Configuring the MTA in ConsoleOne](#)
 - [Changing the Link Protocol between Domains](#)
 - [Changing the Link Protocol between a Domain and Its Post Offices](#)
 - [Binding the MTA to a Specific IP Address](#)
 - [Moving the MTA to a Different Server](#)
 - [Adjusting the MTA for a New Location of a Domain or Post Office](#)
 - [Adjusting the MTA Logging Level and Other Log Settings](#)
- ♦ [Section 42.2, “Configuring User Access through the Domain,” on page 642](#)
 - [Restricting Message Size between Domains](#)
 - [Securing the Domain with SSL Connections to the MTA](#)
- ♦ [Section 42.3, “Configuring Specialized Routing,” on page 645](#)
 - [Using Routing Domains](#)
 - [Scheduling Direct Domain Links](#)
 - [Using a Transfer Pull Configuration \(Windows Only\)](#)
- ♦ [Section 42.4, “Configuring Domain Maintenance,” on page 652](#)
 - [Using eDirectory User Synchronization](#)
 - [Enabling MTA Message Logging](#)

42.1 Performing Basic MTA Configuration

MTA configuration information is stored as properties of its MTA object in eDirectory. The following topics help you modify the MTA object in ConsoleOne and change MTA configuration to meet changing system configurations:

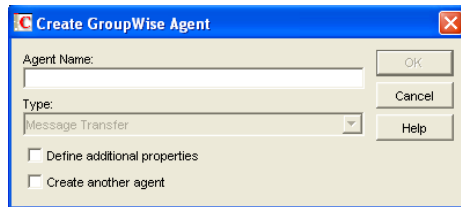
- ♦ [Section 42.1.1, “Creating an MTA Object in eDirectory,” on page 628](#)
- ♦ [Section 42.1.2, “Configuring the MTA in ConsoleOne,” on page 629](#)
- ♦ [Section 42.1.3, “Changing the Link Protocol between Domains,” on page 632](#)
- ♦ [Section 42.1.4, “Changing the Link Protocol between a Domain and Its Post Offices,” on page 636](#)
- ♦ [Section 42.1.5, “Binding the MTA to a Specific IP Address,” on page 639](#)
- ♦ [Section 42.1.6, “Moving the MTA to a Different Server,” on page 640](#)
- ♦ [Section 42.1.7, “Adjusting the MTA for a New Location of a Domain or Post Office,” on page 640](#)
- ♦ [Section 42.1.8, “Adjusting the MTA Logging Level and Other Log Settings,” on page 641](#)

42.1.1 Creating an MTA Object in eDirectory

When you create a new domain, an MTA object is automatically created for it. If the original MTA object for a domain is accidentally deleted, you can create a new one for it. Do not attempt to create more than one MTA object for a domain.

To create a new MTA object in Novell eDirectory:

- 1 In ConsoleOne, browse to and right-click the Domain object for which you need to create an MTA object, then click *New*.
- 2 Double-click GroupWise Agent to display the Create GroupWise Agent dialog box.

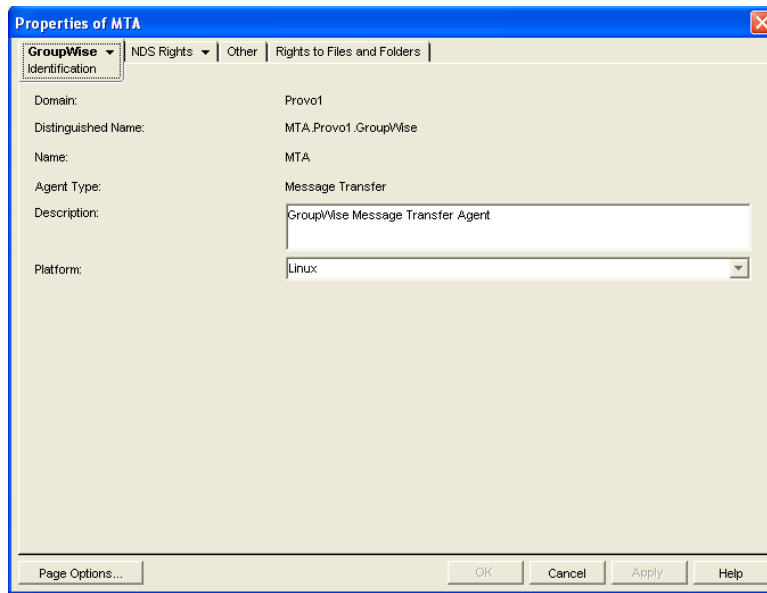


- 3 Type a unique name for the new MTA. The name can include as many as 8 characters. Do not use any of the following invalid characters in the name:

ASCII characters 0-31	Comma ,
Asterisk *	Double quote "
At sign @	Extended ASCII characters that are graphical or typographical symbols; accented characters in the extended range can be used
Backslash \	Parentheses ()
Braces { }	Period .
Colon :	Slash /

The *Type* field is automatically set to *Message Transfer*.

- 4 Select *Define Additional Properties*.
- 5 Click *OK*.
The MTA object is automatically placed within the Domain object.
- 6 Review the information displayed for the first four fields on the Identification page to ensure that you are creating the correct type of Agent object in the correct location.



7 In the *Description* field, type one or more lines of text describing the MTA. This description displays on the MTA server console as the MTA runs.

If multiple administrators work at the server where the MTA will run, the description includes a note about who to contact before stopping the MTA. When running multiple MTAs on the same server, the description should uniquely identify each one. See [Chapter 43, “Monitoring the MTA,”](#) on page 659.

8 In the *Platform* field, select the platform (Linux or Windows) where the MTA will run.

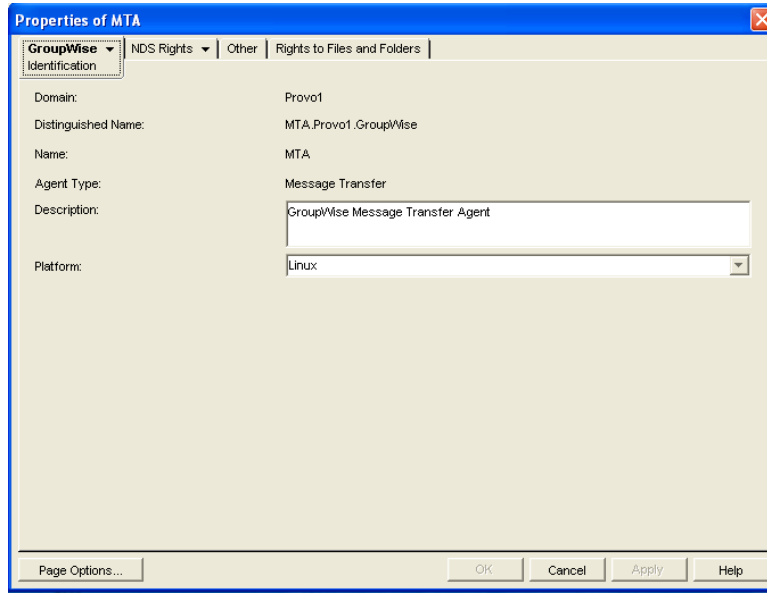
9 Continue with [Section 42.1.2, “Configuring the MTA in ConsoleOne,”](#) on page 629.

42.1.2 Configuring the MTA in ConsoleOne

The advantage to configuring the MTA in ConsoleOne, as opposed to using startup switches in an MTA startup file, is that the MTA configuration settings are stored in eDirectory.

- 1 In ConsoleOne, expand the eDirectory container where the Domain object is located.
- 2 Expand the Domain object.

3 Right-click the MTA object, then click *Properties*.



The table below summarizes the MTA configuration settings in the MTA object properties pages and how they correspond to MTA startup switches (as described in [Chapter 45, “Using MTA Startup Switches,”](#) on page 693):

ConsoleOne Properties Pages and Corresponding Tasks and Startup Switches Settings

Information Page

Domain	See Section 42.1.1, “Creating an MTA Object in eDirectory,” on page 628.
Distinguished Name	
Name	
Agent Type	
Description	
Platform	

Agent Settings Page

Scan Cycle	See Section 44.2.2, “Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways,” on page 686.
Scan High	See also <code>--cyhi</code> and <code>--cylo</code> .
Attach Retry	See Section 44.4, “Adjusting MTA Polling of Closed Locations,” on page 690.
Enable Automatic Database Recovery	See <code>--norecover</code> .
Use 2nd High Priority Scanner	See Section 44.2.3, “Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices,” on page 688.
Use 2nd Mail Priority Scanner	See also <code>--fast0</code> and <code>--fast4</code> .
SNMP Community "Get" String	See Section 43.6, “Using an SNMP Management Console,” on page 679.

ConsoleOne Properties Pages and Settings**Corresponding Tasks and Startup Switches**

HTTP User Name
HTTP Password

See [Section 43.2.1, "Setting Up the MTA Web Console,"](#) on page 669.
See also `--httpuser` and `--httppassword`.

Network Address Page

TCP/IP Address

See ["Using TCP/IP Links between Domains"](#) on page 632 and ["Using TCP/IP Links between a Domain and its Post Offices"](#) on page 637.
See also `--ip` and `--tcpport`.

Bind Exclusively to TCP/IP Address

See [Section 42.1.5, "Binding the MTA to a Specific IP Address,"](#) on page 639.
See also `--ip`.

Message Transfer

See ["Using TCP/IP Links between Domains"](#) on page 632.
See also `--msgtranssl`.

HTTP

See [Section 43.2.1, "Setting Up the MTA Web Console,"](#) on page 669.
See also `--httpsl`.

Log Settings Page

Log File Path
Logging Level
Max Log File Age
Max Log Disk Space

See [Section 43.3, "Using MTA Log Files,"](#) on page 677.
See also `--log`, `--logdays`, `--logdiskoff`, `--loglevel`, and `--logmax`.

Message Log Settings Page

Message Logging Level
Message Log File Path

See [Section 42.4.2, "Enabling MTA Message Logging,"](#) on page 657.
See also `--messagelogsettings`, `--messagelogpath`, `--messagelogdays`, and `--messagelogmaxsize`.

Scheduled Events Page

eDirectory User Synchronization
Event

See [Section 42.4.1, "Using eDirectory User Synchronization,"](#) on page 652.
See also `--nondssync`.

Routing Options Page

Default Routing Domain
Force All Messages to Default Routing
Domain

See [Section 42.3.1, "Using Routing Domains,"](#) on page 645.
See also `--defaultroutingdomain`.

Allow MTA to Send Directly to Other
GroupWise Systems

See ["Using Dynamic Internet Links"](#) in ["Connecting to Other GroupWise Systems"](#) in the *GroupWise 2012 Multi-System Administration Guide*.
See also `--nodns`.

MTA SSL Settings Page

ConsoleOne Properties Pages and Settings**Corresponding Tasks and Startup Switches**

Certificate File
SSL Key File
Password

See [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,”](#) on page 643.

See also `--certfile`, `--keyfile` and `--keypassword`.

After you install the MTA software, you can further configure the MTA using a startup file. To survey the many ways the MTA can be configured, see [Chapter 45, “Using MTA Startup Switches,”](#) on page 693.

42.1.3 Changing the Link Protocol between Domains

How MTAs for different domains communicate with each other is determined by the link protocol in use between the domains. Typically, inbound and outbound links for a domain use the same link protocol, but this is not required. For a review of link protocols, see [Section 10.1.3, “Link Protocols for Direct Links,”](#) on page 159.

If you originally set up an MTA using one link protocol and need to change to a different one, some reconfiguration of the MTA is necessary.

- ♦ [“Using TCP/IP Links between Domains”](#) on page 632
- ♦ [“Using Mapped or UNC Links between Domains”](#) on page 635
- ♦ [“Using Gateway Links between Domains”](#) on page 636

NOTE: The Linux MTA does not support mapped or UNC links between domains. TCP/IP links are required.

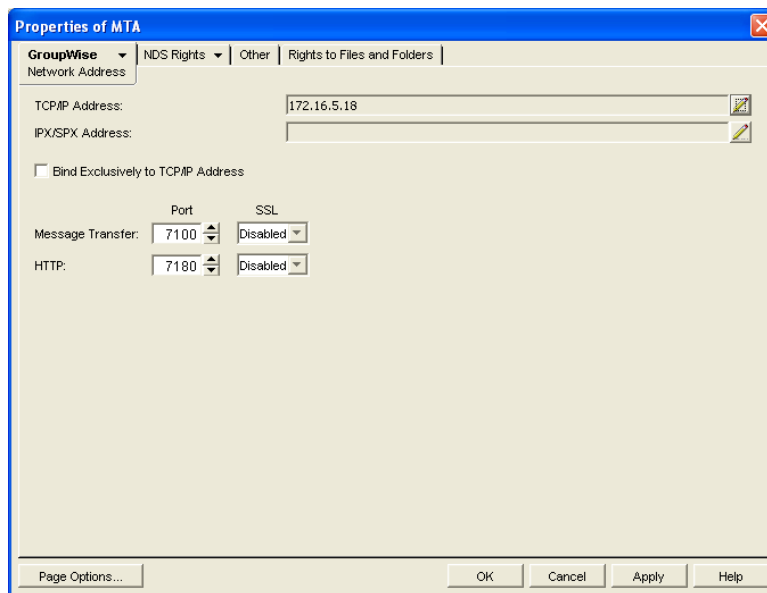
Using TCP/IP Links between Domains

To set up TCP/IP links between domains, you must perform the following two tasks:

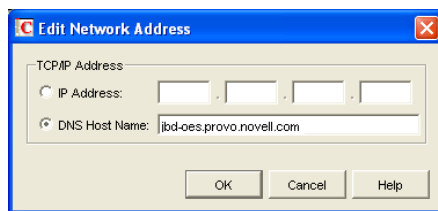
- ♦ [“Configuring the MTA for TCP/IP”](#) on page 632
- ♦ [“Changing the Link Protocol between Domains to TCP/IP”](#) on page 634

Configuring the MTA for TCP/IP

- 1 Make sure TCP/IP is properly set up on the server where the MTA is running.
- 2 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 3 Click *GroupWise > Network Address* to display the Network Address page.



- 4 On the Network Address page, click the pencil icon for the *TCP/IP Address* field to display the *Edit Network Address* dialog box.



- 5 Select *IP Address*, then provide the IP address, in dotted decimal format, of the server where the MTA is running.

or

Select *DNS Host Name*, then provide the DNS hostname of the server where the MTA is running.

IMPORTANT: The MTA must run on a server that has a static IP address. DHCP cannot be used to dynamically assign an IP address for it.

Specifying the DNS hostname rather than the IP address makes it easier to move the MTA from one server to another, should the need arise at a later time. You can assign a new IP address to the hostname in DNS, without changing the MTA configuration information in ConsoleOne.

- 6 Click *OK*.
- 7 To use a TCP port number other than the default port of 7100, type the port number in the *Message Transfer Port* field.
If multiple MTAs will run on the same server, each MTA must have a unique TCP port number.
- 8 For optimum security, select *Enabled* in the *SSL* drop-down list for the message transfer port. For more information, see [Section 42.2.2, "Securing the Domain with SSL Connections to the MTA," on page 643](#).
- 9 Click *OK* to save the network address and return to the main ConsoleOne window.
ConsoleOne then notifies the MTA to restart enabled for TCP/IP.

Corresponding Startup Switches: You can also use the `--ip` and `--tcpport` switches in the MTA startup file to provide the IP address and the message transfer port number.

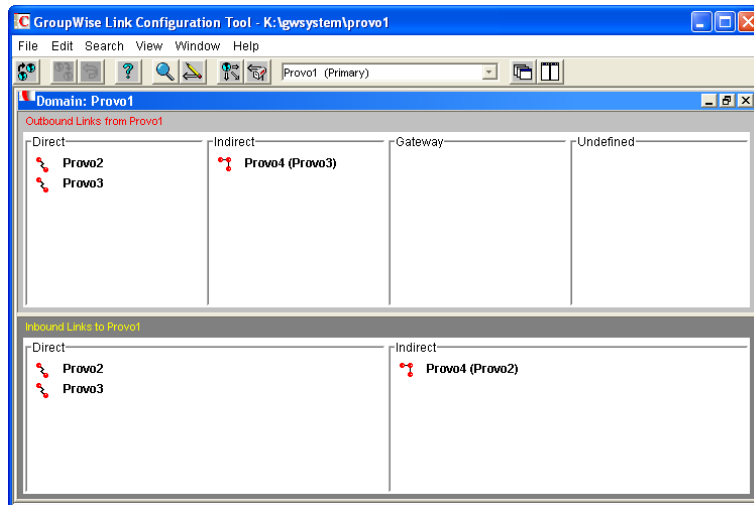
MTA Web Console: You can view the MTA TCP/IP information on the [Configuration](#) page under the *TCP/IP Settings* heading.

Changing the Link Protocol between Domains to TCP/IP

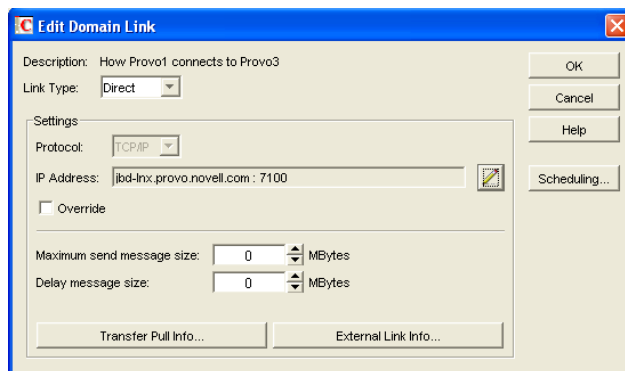
Make sure you have configured the MTA for TCP/IP at both ends of each link.

To change the link between the domains from mapped or UNC to TCP/IP:

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration*.
- 2 Click *View > Domain Links* to display domain links.



- 3 Select the MTA's local domain in the drop-down list.
Outbound and inbound links for the selected domain are listed.
- 4 Double-click a domain in the *Outbound Links* list.



- 5 Set *Link Type* to *Direct*.
- 6 Set *Protocol* to *TCP/IP*.
Make sure the information displayed in the *IP Address* and *MT Port* fields matches the information for the MTA for the domain to which you are linking.
- 7 Click *OK*.

- 8 Repeat [Step 4](#) through [Step 7](#) for each domain in the *Outbound Links* list where you want the MTA to use a TCP/IP link.
Selecting multiple domains is also allowed.
- 9 Double-click a domain in the *Inbound Links* list.
- 10 Set *Link Type* to *Direct*.
- 11 Set *Protocol* to *TCP/IP*.
Make sure the information displayed in the IP Address and MT Port fields matches the information you supplied in [“Configuring the MTA for TCP/IP”](#) on page 632.
- 12 Click *OK*.
- 13 Repeat [Step 9](#) through [Step 12](#) for each domain in the *Inbound Links* list where you want the MTA to use a TCP/IP link.
Selecting multiple domains is also allowed.
- 14 Click *File > Exit > Yes* to save the link changes.
ConsoleOne then notifies the MTA to restart with the new link configuration.

For a sample message flow for this configuration, see [“TCP/IP Link Open: Transfer between Domains Successful”](#) in [“Message Delivery to a Different Domain”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

Using Mapped or UNC Links between Domains

To change to a mapped or UNC link between domains:

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration*.
- 2 Click *View > Domain Links* to display domain links.
- 3 Select the MTA’s local domain in the drop-down list.
Outbound and inbound links for the selected domain are listed.
- 4 Double-click a domain in the *Outbound Links* list.
- 5 Set *Link Type* to *Direct*.
- 6 Set *Protocol* to *Mapped* or *UNC*.
- 7 Enter the full path, in the appropriate format, of the directory where the other domain is located.
- 8 Click *OK*.
- 9 Repeat [Step 4](#) through [Step 8](#) for each domain in the *Outbound Links* list where you want the MTA to use a mapped or UNC link.
Selecting multiple domains is also allowed.
- 10 Double-click a domain in the *Inbound Links* list.
- 11 Set *Link Type* to *Direct*.
- 12 Set *Protocol* to *Mapped* or *UNC*.
- 13 Enter the full path, in the appropriate format, of the directory where the local domain is located.
- 14 Click *OK*.
- 15 Repeat [Step 10](#) through [Step 14](#) for each domain in the *Inbound Links* list where you want the MTA to use a mapped link.
Selecting multiple domains is also allowed.

16 Click *File > Exit > Yes* to save the link changes.

ConsoleOne then notifies the MTA to restart with the new link configuration.

Using Gateway Links between Domains

You can use GroupWise gateways to link domains within your GroupWise system.

- ♦ [“Using the Async Gateway to Link Domains” on page 636](#)
- ♦ [“Using the Internet Agent to Link Domains” on page 636](#)

Using the Async Gateway to Link Domains

You can use the Async Gateway to link a domain into your GroupWise system using a modem. For setup instructions, see the Async Gateway documentation at the [GroupWise Gateway Documentation Web site \(http://www.novell.com/documentation/gwgateways\)](http://www.novell.com/documentation/gwgateways).

NOTE: GroupWise gateways such as the Async Gateway are legacy products that are not supported with the current GroupWise version.

Using the Internet Agent to Link Domains

You can use the Internet Agent (GWIA) to link a domain into your GroupWise system across the Internet. When you use the GWIA as the transport mechanism between domains, it encapsulates GroupWise messages (both email messages and administrative messages) within SMTP messages in order to transport them across the Internet. For setup instructions, see [Section 58.2, “Linking Domains,” on page 848](#)

NOTE: A simpler alternative to a gateway link for spanning the Internet is to use MTA to MTA links, as described for linking separate GroupWise systems in [“Using Dynamic Internet Links”](#) in the [GroupWise 2012 Multi-System Administration Guide](#). The same configuration that can link two separate GroupWise systems can be employed to link a domain within the same GroupWise system.

42.1.4 Changing the Link Protocol between a Domain and Its Post Offices

How messages are transferred between the MTA for the domain and the POA for each post office is determined by the link protocol in use between the domain and each post office. For a review of link protocols, see [Section 10.1.3, “Link Protocols for Direct Links,” on page 159](#).

If you need to change from one link protocol to another, some reconfiguration of the MTA and its link to each post office is necessary.

- ♦ [“Using TCP/IP Links between a Domain and its Post Offices” on page 637](#)
- ♦ [“Using Mapped or UNC Links between a Domain and its Post Offices” on page 639](#)

NOTE: The Linux MTA requires TCP/IP links between a domain and its post offices.

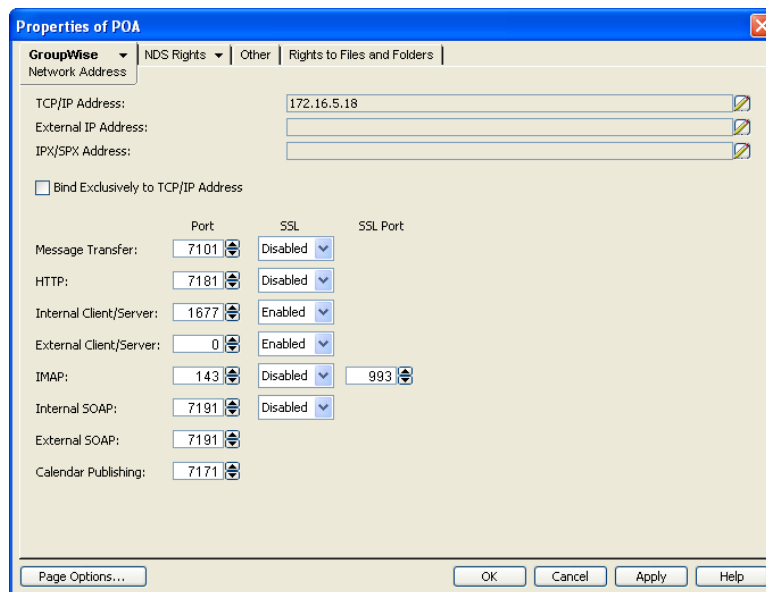
Using TCP/IP Links between a Domain and its Post Offices

To change from mapped or UNC links to TCP/IP links between a domain and its post offices, you must perform the following two tasks:

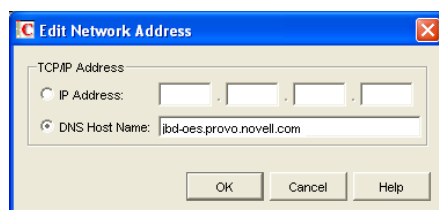
- ♦ “Configuring the Agents for TCP/IP” on page 637
- ♦ “Changing the Link Protocol between a Domain and its Post Offices to TCP/IP” on page 638

Configuring the Agents for TCP/IP

- 1 If the MTA for the domain is not yet set up for TCP/IP communication, see “Configuring the MTA for TCP/IP” on page 632.
- 2 If any post offices do not yet have a POA set up for TCP/IP communication, see Section 36.2.1, “Using Client/Server Access to the Post Office,” on page 494 to set up the initial TCP/IP information.
- 3 In ConsoleOne, expand the Post Office object to display the POA object(s) in the post office.
Only one POA per post office needs to communicate with the MTA. If the post office has multiple POAs, have a POA that performs message file processing communicate with the MTA for best performance. For information about message file processing, see Section 35.5, “Role of the Post Office Agent,” on page 477.
- 4 Right-click the POA object, then click *Properties*.
- 5 Click *GroupWise > Network Address* to display the Network Address page.



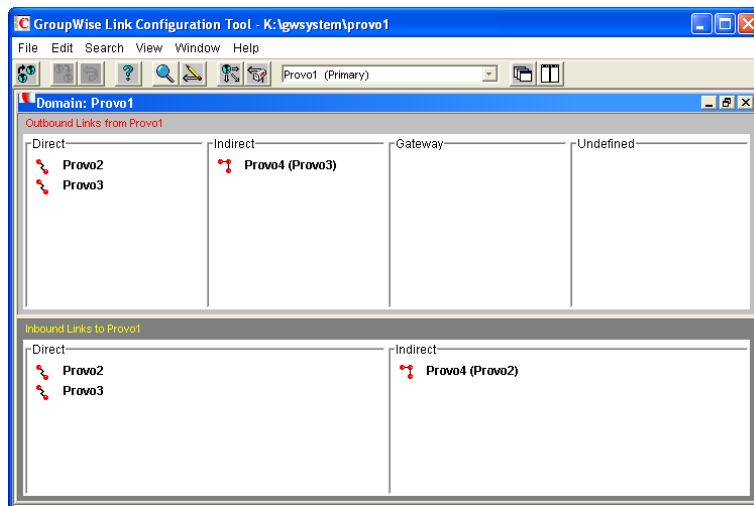
- 6 On the Network Address page, click the pencil icon for the *TCP/IP Address* field to display the *Edit Network Address* dialog box.



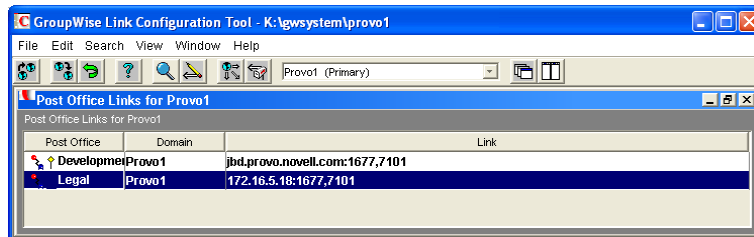
- 7 In the *Message Transfer Port* field, specify a unique TCP port on which the POA will listen for incoming messages from the MTA.
The default is 7101.
- 8 For optimum security, select *Enabled* in the SSL drop-down list for the message transfer port. For more information, see [Section 42.2.2, "Securing the Domain with SSL Connections to the MTA," on page 643.](#)
- 9 Click *OK* to save the TCP/IP information and return to the main ConsoleOne window.
ConsoleOne then notifies the POA to restart with message transfer processing enabled.

Changing the Link Protocol between a Domain and its Post Offices to TCP/IP

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration.*



- 2 In the drop-down list, select the domain where you want TCP/IP links to post offices.
- 3 Click *View > Post Office Links* to display post office links.



- 4 Double-click a Post Office object.
- 5 In the *Protocol* field, select *TCP/IP*.



- 6 Make sure the information displayed in the Edit Post Office Link dialog box matches the information provided in the Edit Network Address dialog box in [“Configuring the Agents for TCP/IP” on page 637](#).
- 7 Click OK.
- 8 Repeat [Step 4](#) through [Step 7](#) for each post office in the domain where you want to use TCP/IP links.
- 9 To exit the Link Configuration tool and save your changes, click *File > Exit > Yes*.
ConsoleOne then notifies the MTA and POAs to restart using the new link protocol.

For a sample message flow for this configuration, see [“TCP/IP Link Open: Transfer between Post Offices Successful”](#) in [“Message Delivery to a Different Post Office”](#) in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

Using Mapped or UNC Links between a Domain and its Post Offices

To change from a TCP/IP link to a mapped or UNC link between a domain and its post offices:

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration*.
- 2 In the drop-down list, select the domain where the post offices reside.
- 3 Click *View Post Office Links* to display post office links.
- 4 Double-click a Post Office object.
- 5 In the *Protocol* field, select *Mapped* or *UNC*.
- 6 Provide the location of the post office in the format appropriate to the selected protocol.
- 7 Click OK.
- 8 Repeat [Step 4](#) through [Step 7](#) for each post office in the domain.
- 9 To exit the Link Configuration tool and save your changes, click *File > Exit > Yes*.
ConsoleOne then notifies the POA and MTA to restart using the new link protocol.

42.1.5 Binding the MTA to a Specific IP Address

If the MTA runs on a server that has multiple IP addresses, you can cause the MTA to bind to a specific IP address. The specified IP address is associated with all ports used by the MTA. Without an exclusive bind, the MTA binds to all IP addresses available on the server.

- 1 In ConsoleOne, expand the Domain object to display the MTA object in the post office.
- 2 Right-click the MTA object, then click *Properties*.
- 3 Click *GroupWise > Network Address* to display the Network Address page.

- 4 If the *TCP/IP Address* field does not yet display the IP address you want the MTA to use:
 - 4a Click the pencil icon for the *TCP/IP Address* field to display the Edit Network Address dialog box.
 - 4b Specify the IP address for the MTA, then click *OK*.
- 5 Select *Bind Exclusively to TCP/IP Address*, then click *OK* to save the IP address setting.

Corresponding Startup Switches: You can also use the `--ip` switch in the MTA startup file to bind the MTA to a specific IP address.

42.1.6 Moving the MTA to a Different Server

As your GroupWise system grows and evolves, you might need to move an MTA from one server to another. For example, you might decide to run the MTA on a different platform, or perhaps you want to move it to a server that has more disk space for the `mslocal` directory.

- 1 Stop the existing MTA.
- 2 Copy the entire `mslocal` subdirectory structure to wherever you want it on the new server. It might contain messages that have not yet been delivered.
- 3 When moving the MTA, pay special attention to the following details:
 - ♦ In the MTA startup file, set the `--work` switch to the location of the `mslocal` directory on the new server.
 - ♦ If the original MTA was configured for TCP/IP links between domains, you must reconfigure the MTA object with the IP address and port number for the MTA on the new server. See [“Using TCP/IP Links between Domains” on page 632](#).
- 4 Install the MTA on the new server. See [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.
- 5 Start the new MTA, as described in the following sections in the *GroupWise 2012 Installation Guide*:
 - ♦ [“Starting the Linux Agents with a User Interface”](#)
 - ♦ [“Starting the Windows GroupWise Agents”](#)
- 6 Observe the new MTA to see that it is running smoothly. See [Chapter 43, “Monitoring the MTA,” on page 659](#).
- 7 If you are no longer using the old server for any GroupWise agents, you can remove the agents to reclaim the disk space, as described in the following sections in the *GroupWise 2012 Installation Guide*:
 - ♦ [“Uninstalling the Linux GroupWise Agents”](#)
 - ♦ [“Uninstalling the Windows GroupWise Agents”](#)

42.1.7 Adjusting the MTA for a New Location of a Domain or Post Office

The MTA configuration must be adjusted if you make the following changes to your GroupWise system configuration:

- ♦ [“New Domain Location” on page 641](#)
- ♦ [“New Post Office Location” on page 641](#)

New Domain Location

If you move a domain from one server to another, you need to edit the MTA startup file to provide the new location of the domain directory.

- 1 Stop the MTA for the old domain location if it is still running.
- 2 Use an ASCII text editor to edit the MTA startup file.

Windows: Only the first 8 characters of the domain name are used in the file name. The startup file is typically located in the directory where the MTA software is installed.

Linux: The full domain name is used in the file name. However, all letters are lowercase and any spaces in the domain name are removed. The startup file is located in the `/opt/novell/groupwise/agents/share` directory.

- 3 Adjust the setting of the `--home` switch to point to the new location of the domain directory.
- 4 Save the MTA startup file.
- 5 Start the MTA for the new domain location, as described in the following sections in the *GroupWise 2012 Installation Guide*:
 - ♦ [“Starting the Linux Agents with a User Interface”](#)
 - ♦ [“Starting the Windows GroupWise Agents”](#)

New Post Office Location

If you move a post office, you need to adjust the link information for that post office.

- 1 Click *Tools > GroupWise Utilities > Link Configuration*.
- 2 In the drop-down list, select the domain where a post office has moved.
- 3 Click *View > Post Office Links* to display post office links.
- 4 Double-click the post office that has been moved.
- 5 Provide its new location in the appropriate format.
- 6 Click *OK*.
- 7 Click *File > Exit > Yes* to save the link changes.

ConsoleOne then notifies the MTA to restart with the new link configuration.

42.1.8 Adjusting the MTA Logging Level and Other Log Settings

When you are installing or troubleshooting the MTA, a logging level of Verbose can be useful. However, when the MTA is running smoothly, you can set the logging level down to Normal to conserve disk space occupied by log files. See [Section 43.3, “Using MTA Log Files,”](#) on page 677.

42.2 Configuring User Access through the Domain

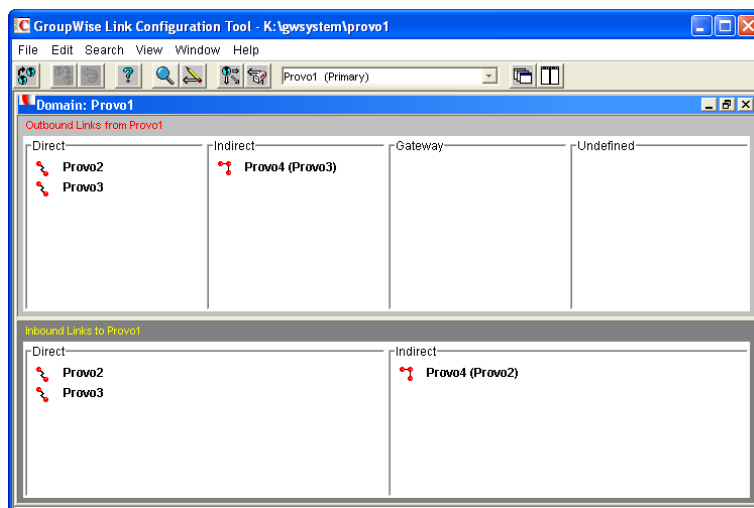
Although users do not access the domain as they use the GroupWise client, their messages often pass through domains while traveling from one post office to another.

- ◆ [Section 42.2.1, “Restricting Message Size between Domains,”](#) on page 642
- ◆ [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,”](#) on page 643
- ◆ [Section 42.2.3, “Enabling Exchange Address Book Synchronization,”](#) on page 645

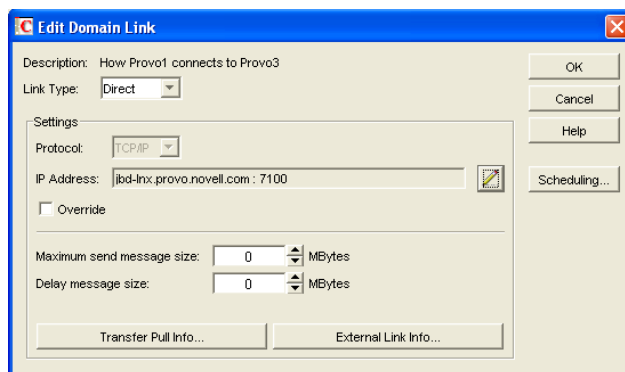
42.2.1 Restricting Message Size between Domains

You can configure the MTA to restrict the size of messages that users are permitted to send outside the domain.

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration*.



- 2 Double-click the domain where you want to restrict message size.



- 3 In the *Maximum Send Message Size* field, specify in megabytes the size of the largest message you want users to be able to send outside the post office.

IMPORTANT: If you have also set a message size limit for your GWIAs, as described in [Section 54.1.2, “Creating a Class of Service,”](#) on page 788, make sure that the MTA message size limit is equal to or greater than the GWIA message size limit.

- 4 (Conditional) If you want to delay large messages, specify the size in megabytes for message files the MTA can process immediately in the *Delay Message Size* field.

If a message file exceeds the delay message size, the message file is moved into the low priority (6) message queue, where only one MTA thread is allocated to process very large messages. This arrangement allows typical messages to be processed promptly, while delaying large messages that exceed the specified size. The result is that large messages do not slow down processing of typical messages. Message size restrictions override message priority, meaning that even high priority messages are delayed if they exceed the size restrictions.

- 5 Click *OK*.
- 6 To exit the Link Configuration Tool and save your changes, click *File > Exit > Yes*.
ConsoleOne then notifies the MTA to restart using the new message size limits.

If a user's message is not sent out of the domain because of this restriction, the user receives an email message providing the following information:

```
Delivery disallowed - Transfer limit is nn MB
```

However, the message is delivered to recipients in the sender's own domain.

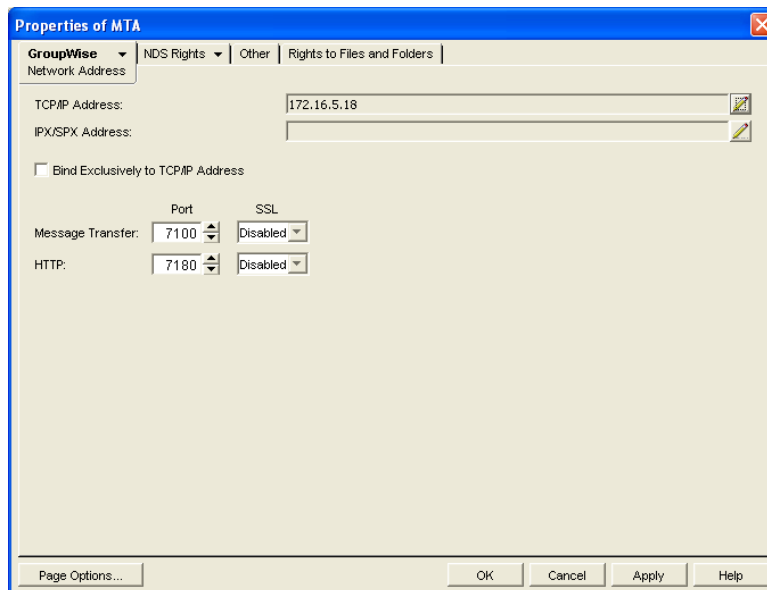
There are additional ways to restrict the size of messages that users can send, as described in [Section 12.3.5, "Restricting the Size of Messages That Users Can Send," on page 201](#).

42.2.2 Securing the Domain with SSL Connections to the MTA

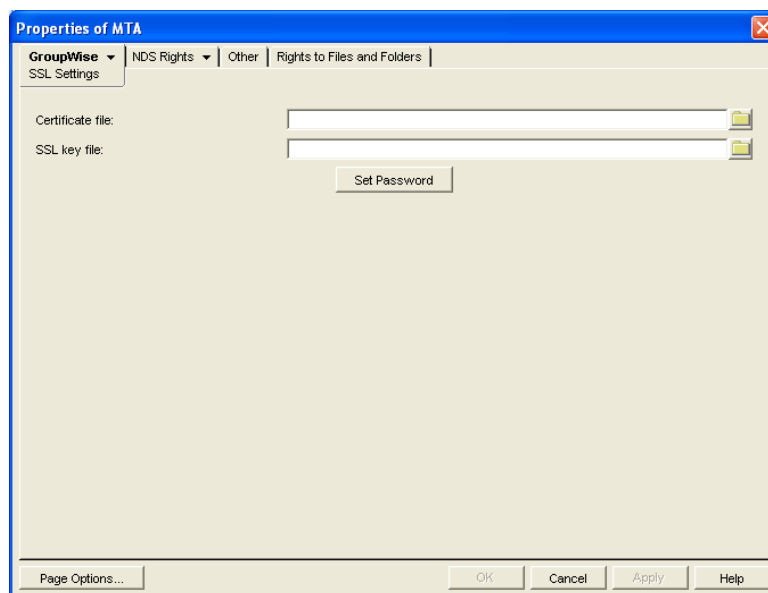
Secure Sockets Layer (SSL) ensures secure communication between the MTA and other programs by encrypting the complete communication flow between the programs. For background information about SSL and how to set it up on your system, see [Section 83.2, "Server Certificates and SSL Encryption," on page 1107](#).

To configure the MTA to use SSL:

- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.



- 3 To use SSL connections between the MTA and the POAs for its post offices, which provides optimum security, select *Enabled* in the *Message Transfer SSL* drop-down list.
The MTA must use a TCP/IP connection to each POA in order to enable SSL for the connection. See [“Using TCP/IP Links between a Domain and its Post Offices”](#) on page 637.
Each POA must also have SSL enabled for the connection to be secure. See [Section 36.3.3, “Securing the Post Office with SSL Connections to the POA,”](#) on page 508.
- 4 To use SSL connections between the MTA and the MTA Web console displayed in your Web browser, which provides optimum security, select *Enabled* in the HTTP SSL drop-down list.
To set up the MTA Web console, see [Section 43.2.1, “Setting Up the MTA Web Console,”](#) on page 669.
- 5 Click *Apply* to save the settings on the Network Address page.
You are prompted to supply the SSL certificate and key files. The key file must be password protected in order for SSL to function correctly.
- 6 Click *Yes* to display the SSL Settings page.



For background information about certificate files and SSL key files, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107.

By default, the MTA looks for the certificate file and SSL key file in the same directory where the MTA executable is located, unless you provide a full path name.

- 7 In the *Certificate File* field, browse to and select the public certificate file provided to you by your CA.
- 8 In the *SSL Key File* field:
 - 8a Browse to and select your private key file.
 - 8b Click *Set Password*.
 - 8c Provide the password that was used to encrypt the private key file when it was created.
 - 8d Click *Set Password*.
- 9 Click *OK* to save the SSL settings.
ConsoleOne then notifies the MTA to restart using the new message size limits.

Corresponding Startup Switches: You can also use the `--certfile`, `--keyfile`, `--keypassword`, `--httpsl`, and `--msgtranssl` switches in the MTA startup file to configure the MTA to use SSL.

MTA Web Console: You can list which connections the MTA is using SSL for from the [Links](#) page. Click *View TCP/IP Connections* to display the list of TCP/IP links.

42.2.3 Enabling Exchange Address Book Synchronization

Starting in GroupWise 2012 SP2, the MTA can perform address book synchronization between GroupWise and Exchange.

Exchange address book synchronization requires its own license. If you enable Exchange address book synchronization, your GroupWise system might be subject to additional licensing fees. We invite you to contact your Novell representative, reseller, or partner to learn more about this feature or for pricing and licensing information.

For setup instructions, see the [GroupWise/Exchange Coexistence Guide](#).

42.3 Configuring Specialized Routing

As you create each new domain in your GroupWise system, you link it to another domain. You can view and modify the links between domains using the Link Configuration Tool. See [Chapter 10, “Managing the Links between Domains and Post Offices,”](#) on page 155. The following topics help you configure the MTA to customize routing through your GroupWise system:

- ♦ [Section 42.3.1, “Using Routing Domains,”](#) on page 645
- ♦ [Section 42.3.2, “Scheduling Direct Domain Links,”](#) on page 647
- ♦ [Section 42.3.3, “Using a Transfer Pull Configuration \(Windows Only\),”](#) on page 650

42.3.1 Using Routing Domains

As an alternative to configuring individual links between individual domains throughout your GroupWise system, you can establish a system of one or more routing domains under the following circumstances.

- ♦ Domains must connect to the routing domains with TCP/IP links.
- ♦ GroupWise 5.5 and later domains can be part of the routing domain system. Domains and MTAs that are still at a 5.2 or earlier version cannot participate and must use links as provided in the Link Configuration Tool.

A routing domain can serve as a hub in the following situations:

- ♦ Messages that are otherwise undeliverable can be automatically sent to a single routing domain. This routing domain can be set up to perform DNS lookups and route messages out across the Internet. See [“Using Dynamic Internet Links”](#) in [“Connecting to Other GroupWise Systems”](#) in the [GroupWise 2012 Multi-System Administration Guide](#).
- ♦ All messages from a domain can be automatically routed through another domain, regardless of the final destination of the messages. This provides additional control of message flow through your GroupWise system.

You can set up routing domains on two levels:

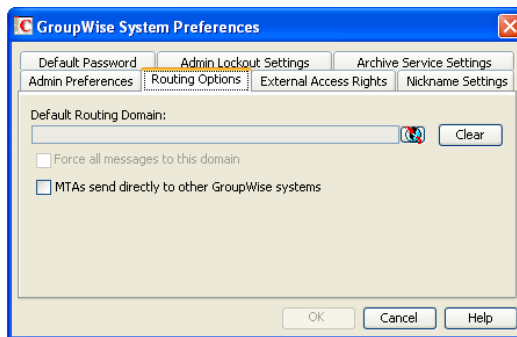
- ♦ “Selecting a System Default Routing Domain” on page 646
- ♦ “Selecting a Specific Routing Domain for an Individual Domain” on page 646

Selecting a System Default Routing Domain

You can establish a single default routing domain for your entire GroupWise system. This provides a centralized routing point for all messages. It takes precedence over specific links established when domains were created or links modified with the Link Configuration Tool.

To set up a system default routing domain:

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > System Preferences > Routing Options* to display the *Routing Options* tab.



- 2 In the *Default Routing Domain* field, browse to and select the domain you want to serve as the default routing domain for your entire GroupWise system.
- 3 If you want all GroupWise messages to pass through the default routing domain regardless of the destination of the message, select *Force All Messages to This Domain*.

or

If you want only undeliverable GroupWise messages to be routed to the default routing domain, deselect *Force All Messages to This Domain*.

If you do not force all messages to the system default routing domain, then you have the option of allowing selected MTAs to provide routing domain services in addition to the system default routing domain.

- 4 Select *MTAs Send Directly to Other GroupWise Systems* if you want all MTAs in your GroupWise system to perform DNS lookups and route messages out across the Internet.

or

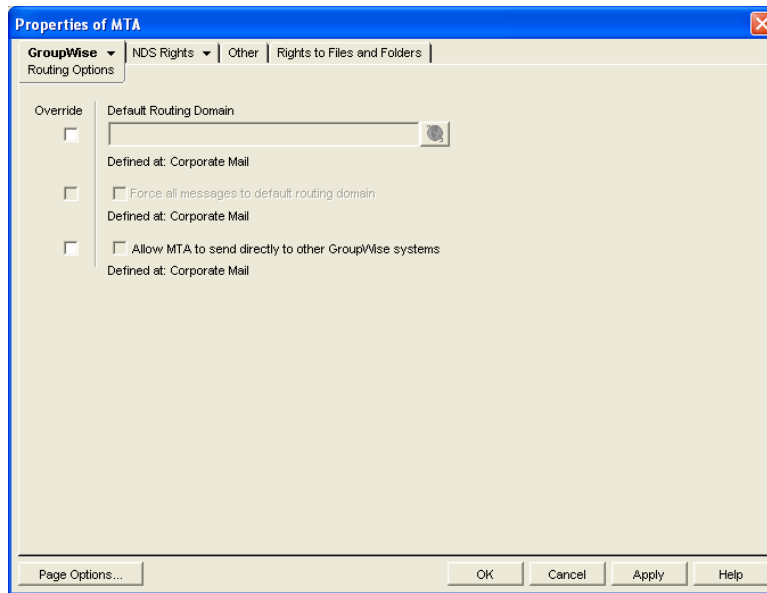
Deselect *MTAs Send Directly to Other GroupWise Systems* if you want to individually designate which MTAs should perform eDirectory lookups and route messages out across the Internet.

- 5 Click *OK* to save the routing options you have specified for the system default routing domain.

Selecting a Specific Routing Domain for an Individual Domain

As long as you are not forcing all messages to the system default routing domain, you can override the system default routing information for an individual domain.

- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Routing Options* to display the *Routing Options* page.



System default routing information displays if it has been set up. See [“Selecting a System Default Routing Domain”](#) on page 646.

- 3 Select *Override* next to the default information you want to change for the selected domain.
- 4 Set the routing options as needed for the selected domain.
- 5 Click *OK* to save the specialized routing information for the selected domain.

ConsoleOne then notifies the MTA to restart so the routing information can be put into effect.

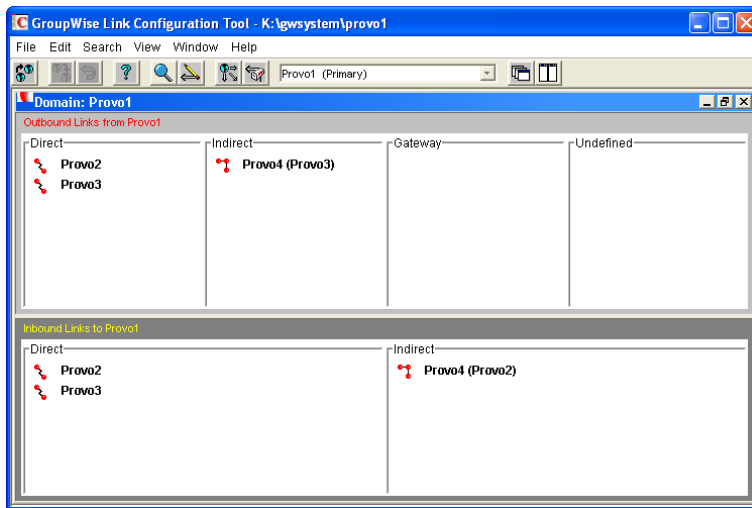
MTA Web Console: You can check routing information on the [Configuration](#) page under the *General Settings* heading.

42.3.2 Scheduling Direct Domain Links

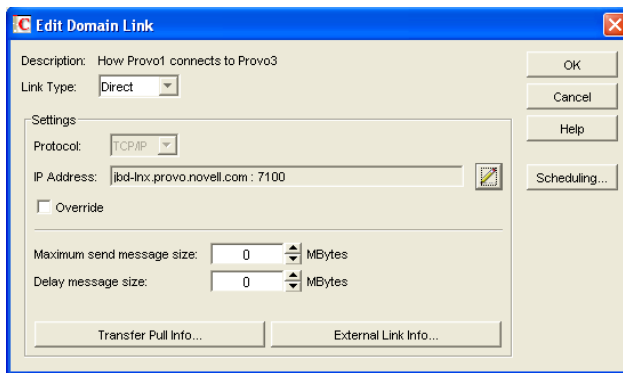
When domains link across an expensive medium such as long-distance phone lines, you can reduce the cost of the link by controlling when it is open. You can choose to have some types of messages wait in the message queues for the lowest phone rate. You can collect messages in the message queues until a specified time or size limit is reached, then open the link, rather than opening the link for each message as it arrives in the queue. You can design as many link profiles as you need, to schedule the transfer of various types of GroupWise messages in the most efficient and cost-effective manner.

To create a schedule for a link between domains:

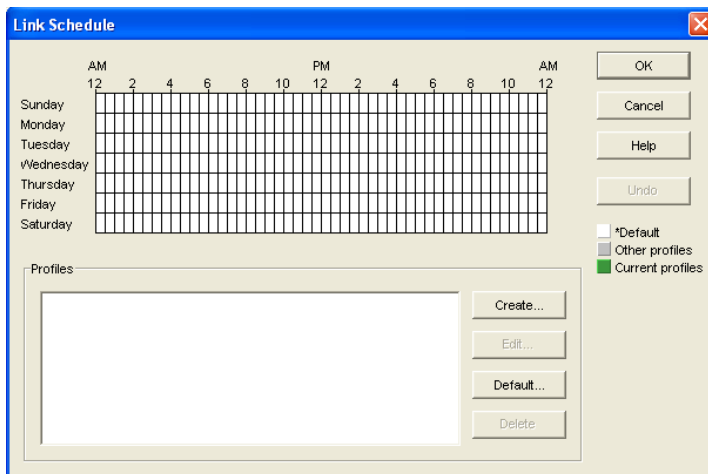
- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration*.
- 2 In the drop-down list, select the domain to schedule a link for.
- 3 Click *View > Domain Links* to display domain links.



- 4 Double-click the domain you want to create a link schedule for. Only direct links can be scheduled.



- 5 Click *Scheduling*.



The link schedule grid displays the current schedule for the selected direct link. The grid consists of half-hour time slots showing the link profile assigned to each time slot. Available link profiles are listed below the link schedule grid.

Each link profile defines the following values to set the conditions under which the link opens:

- ◆ Which message queues to monitor
- ◆ Maximum wait time for any message in any monitored queue
- ◆ Maximum number of waiting messages allowed in all monitored queues
- ◆ Maximum total size of waiting messages allowed in all monitored queues

The default profile shows as white in the link schedule grid. The default profile is in effect at all times when no other profile has been selected. Any other defined profiles show as gray. The currently selected link profile shows as green.

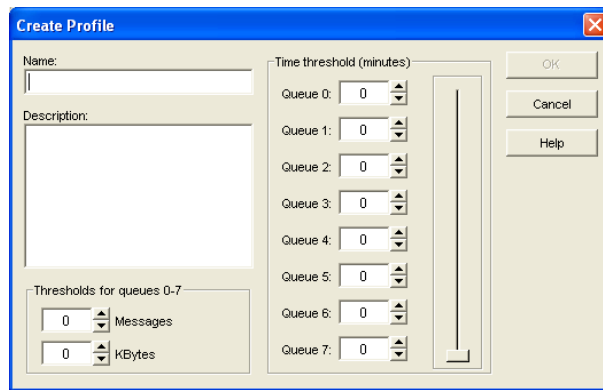
6 To create a new link profile, click *Create*.

or

To edit an existing link profile, select it in the profile list, then click *Edit*.

or

To edit the default link profile, click *Default*.



7 If you are creating a new link profile, provide a unique name for the link profile in the *Name* field.

If you are editing an existing link profile, you cannot change the name.

8 In the *Description* field, provide whatever additional information is necessary to describe the purpose of the link profile.

9 Use the scroll bar in the *Time Threshold* box to select which queues to monitor and process when this link profile is in effect.

Queue	Purpose
0	Busy Search requests
1	Requests from GroupWise Remote users
2	High priority user messages; administrative messages
3	High priority status messages
4	Normal priority user messages
5	Normal priority status messages
6	Low priority user messages
7	Low priority status messages

The contents of deselected queues are not monitored but are processed when the link opens.

- 10 For each selected queue, specify the maximum number of minutes a message must wait in each queue before the link opens.

If you want the link to open immediately when a message arrives in the queue, specify 0 (zero).

- 11 In the *Messages* field, specify the total number of messages waiting in all selected queues that will trigger the link to open.
- 12 In the *KBytes* field, specify the total size in kilobytes of all messages waiting in all selected queues that will trigger the link to open.
- 13 Click *OK* to save the link profile and return to the Link Scheduling dialog box.
- 14 Select the new or modified link profile in the profile list.
- 15 Click a time slot or drag to select a range of time slots.

Time slots assigned to the selected link profile display as green.

- 16 Select all the time slots you want governed by the selected link profile.
- 17 Select a different link profile to assign to time slots.

or

Create or edit another link profile.

or

Click *OK* to save the schedule for the current link.

- 18 When the schedule is saved, click *OK* to close the Edit Domain Link dialog box.
- 19 To exit the Link Configuration Tool, click *File > Exit > Yes*.

ConsoleOne then notifies the MTA to restart using the new link schedule.

42.3.3 Using a Transfer Pull Configuration (Windows Only)

Typically for a mapped or UNC link, the MTA for the sending domain writes (or “pushes”) message files into the input queue subdirectories of the receiving domain. However, it is possible to change this configuration so the MTA for the receiving domain picks up (or “pulls”) message files from the sending domain.

The transfer pull directory is a location in the sending domain where the MTA for the receiving domain can pick up message files (that is, “pull” them from the sending domain). It represents the only configuration where an MTA processes messages outside its own domain directory structure.

NOTE: The transfer pull configuration does not apply to the Linux MTA because the Linux MTA does not use mapped or UNC links.

To set up a transfer pull configuration between domains:

- 1 Manually create a transfer directory with input queue subdirectories from which outgoing message files are pulled.

The transfer directory must contain a *wpcsin* subdirectory, with standard priority 0 through 7 subdirectories beneath. The transfer directory must be placed where both the sending and receiving MTAs have rights.

- 2 In ConsoleOne, modify the outgoing link from the sending domain so the MTA for the sending domain writes message files to the transfer directory, rather than directly to the receiving domain. See [“Modifying the Outgoing Transfer Pull Link” on page 651](#).

- 3 In ConsoleOne, modify the incoming link to the receiving domain so the MTA for the receiving domain actively pulls message files from the transfer directory, rather than waiting for them to be delivered. See [“Modifying the Incoming Transfer Pull Link” on page 651](#).
- 4 Stop and restart the MTAs for both domains.

Modifying the Outgoing Transfer Pull Link

- 1 In ConsoleOne, connect to the sending domain.
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,” on page 69](#).
- 2 Click *Tools > GroupWise Utilities > Link Configuration*.
- 3 In the drop-down list, select the sending domain.
- 4 Click *View > Domain Links* to view outbound and inbound links for the sending domain.
- 5 In the *Outbound Links from sending_domain_name* list box, double-click the receiving domain.
- 6 If you are using a UNC path, click *Override* to display the *Path* field.
- 7 In the *Path* or *UNC Override* field (depending on the selected protocol), specify the full path to the transfer directory you created.
You can use a UNC path or a mapped drive path for the Windows MTA.
- 8 Click *OK*.
- 9 Click *File > Exit > Yes* to save the link changes for the sending domain and return to the main ConsoleOne window.
- 10 Continue with [“Modifying the Incoming Transfer Pull Link” on page 651](#).

Modifying the Incoming Transfer Pull Link

- 1 In ConsoleOne, connect to the receiving domain.
If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, “Select Domain,” on page 69](#).
- 2 Click *Tools > GroupWise Utilities > Link Configuration*.
- 3 In the drop-down list, select the receiving domain.
- 4 Click *View Domain Links* to view outbound and inbound links for the receiving domain.
- 5 In the *Outbound Links from receiving_domain_name* list box, double-click the sending domain.
- 6 Verify that the information displayed in the Edit Domain Link dialog box is correct.
- 7 Click *Transfer Pull Info*.
- 8 Specify the full path to the transfer directory you created.
You can use a UNC path or a mapped drive path for the Windows MTA.
- 9 Specify the number of seconds after which the MTA checks the transfer directory for message files to pull.
- 10 Specify the command needed to reestablish the connection with the transfer directory, if that connection should be broken for any reason.
- 11 Click *OK* until you return to the Link Configuration dialog box.
- 12 Click *File > Exit > Yes* to save the link changes for the receiving domain and return to the main ConsoleOne window.
- 13 Stop and restart the MTAs for both domains.

42.4 Configuring Domain Maintenance

You can configure the MTA to synchronize user information in the GroupWise Address Book with user information in eDirectory. You can also configure it to gather information about all messages that pass through the domain for tracking purposes.

- ♦ [Section 42.4.1, “Using eDirectory User Synchronization,” on page 652](#)
- ♦ [Section 42.4.2, “Enabling MTA Message Logging,” on page 657](#)

42.4.1 Using eDirectory User Synchronization

As long as GroupWise administration is performed with the GroupWise Administrator snap-in to ConsoleOne running, user information is automatically synchronized between GroupWise and eDirectory. However, three situations can cause this automatic synchronization to be insufficient:

- ♦ An administrator modifies user information in ConsoleOne without having the GroupWise Administrator snap-in running.
- ♦ The user information was changed using Novell iManager.
- ♦ The user information was changed using Novell eGuide and the GroupWise Identity Manager driver is not in use

In these situations, user information in eDirectory no longer matches corresponding user information in GroupWise. (User objects are the only GroupWise objects that can be modified without the GroupWise Administrator snap-in running. Modification of all other GroupWise objects requires the presence of the GroupWise Administrator snap-in.)

This section covers the following aspects of eDirectory user synchronization:

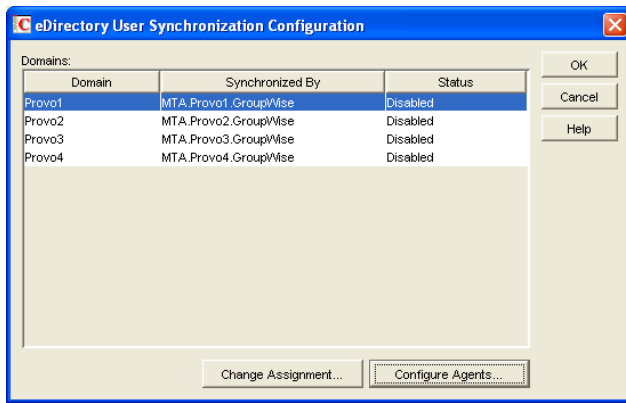
- ♦ [“Enabling eDirectory User Synchronization” on page 652](#)
- ♦ [“Assigning an eDirectory-Enabled MTA to Synchronize Other Domains” on page 655](#)
- ♦ [“Scheduling eDirectory User Synchronization” on page 656](#)

Enabling eDirectory User Synchronization

By default, eDirectory user synchronization is disabled. The MTA still performs all its other functions, but any changes made to user information in eDirectory without the GroupWise Administrator snap-in running do not appear in GroupWise until eDirectory user synchronization has been performed.

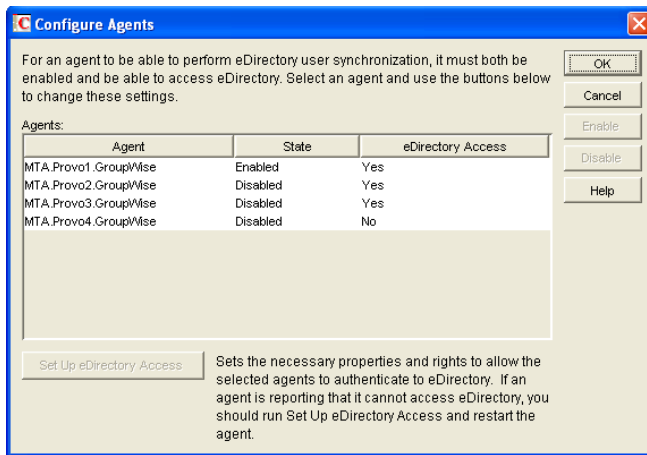
Although all MTAs can be enabled to perform eDirectory user synchronization, the minimum requirement is that at least one MTA be configured that way. If your GroupWise system spans multiple trees, at least one MTA in each tree must be configured to perform eDirectory user synchronization. The MTA server should have a local eDirectory replica for the MTA to access.

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > eDirectory User Synchronization* to display the eDirectory User Synchronization Configuration dialog box.



The eDirectory User Synchronization Configuration dialog box lists all domains in your GroupWise system, the MTA currently assigned to provide eDirectory user synchronization for each domain, and the current status of that agent's ability to perform eDirectory user synchronization.

2 Click *Configure Agents*.



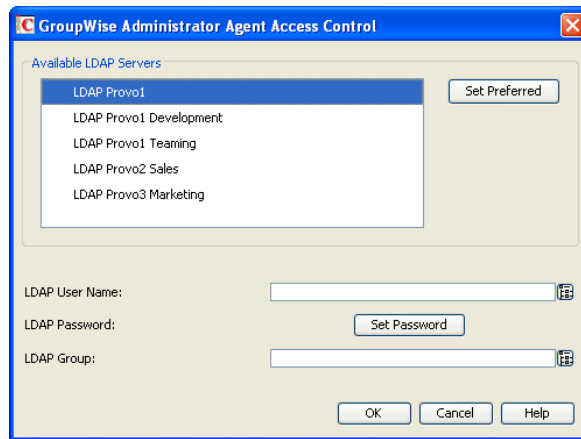
3 Select an MTA that you want to perform eDirectory user synchronization.

4 If the *eDirectory Access* column for the MTA displays *Yes*, click *Enable*.

or

If the *eDirectory Access* column for the MTA displays *No*:

4a Click *Set Up eDirectory Access*.



4b Fill in the following fields:

Available LDAP Servers: Select the LDAP server that you want the MTA to log into in order to gain access to eDirectory, then click *Set Preferred*.

LDAP User Name: Browse to and select the user that the MTA can use to log in as. The selected user must have rights to browse properties of User objects.

Click *Set Password*, provide the password associated with the user selected above, then click *Set Password*.

LDAP Group: Browse to and select the LDAP Group object for the server where the MTA runs. The LDAP Group object provides a table of attribute mappings between eDirectory and LDAP that the MTA needs in order to perform eDirectory user synchronization.

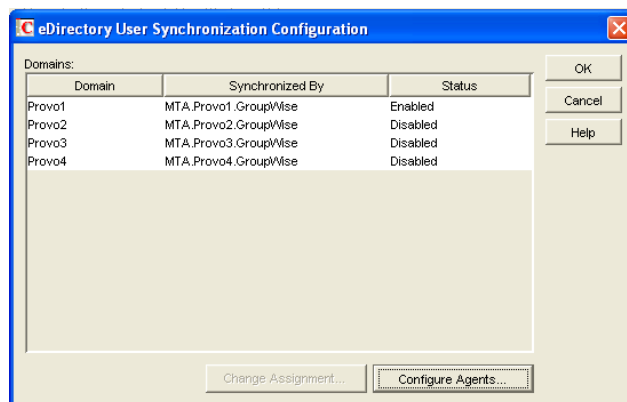
4c Click *OK* to save the LDAP information.

The *eDirectory Access* column for that MTA should now display *Yes* so that you can enable it.

5 If your GroupWise system spans multiple trees, repeat [Step 3](#) through [Step 4](#) as needed to enable eDirectory user synchronization for at least one MTA in each tree.

6 Click *OK* to return to the eDirectory User Synchronization Configuration dialog box.

Each domain for which you have configured the MTA for eDirectory user synchronization should now display *Enabled* in the *Status* column.



7 If all domains are now enabled, click *OK* to return to main ConsoleOne window, then continue with [“Scheduling eDirectory User Synchronization”](#) on page 656.

or

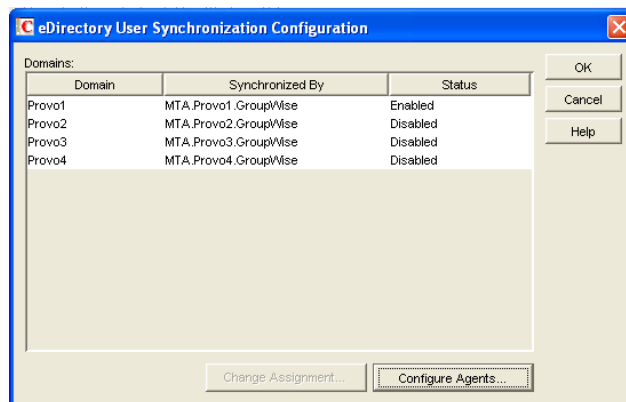
If some domains are still disabled, continue with [“Assigning an eDirectory-Enabled MTA to Synchronize Other Domains”](#) on page 655.

Assigning an eDirectory-Enabled MTA to Synchronize Other Domains

After at least one MTA is performing eDirectory user synchronization, other MTAs not performing eDirectory user synchronization themselves can have an eDirectory-enabled MTA gather the eDirectory information for them.

In the eDirectory User Synchronization Configuration dialog box,

- 1 Click a domain that still displays *Disabled* in the *Status* column.



- 2 Select an MTA, then click *Change Assignment*.



- 3 Select the MTA you want to perform eDirectory user synchronization for the selected domain, then click *OK*.

The domain should now display *Enabled* in the *Status* column of the eDirectory User Synchronization Configuration dialog box.

- 4 Repeat [Step 1](#) through [Step 3](#) until all domains in your GroupWise system are enabled for eDirectory user synchronization.
- 5 Click *OK* to return to the main ConsoleOne window.

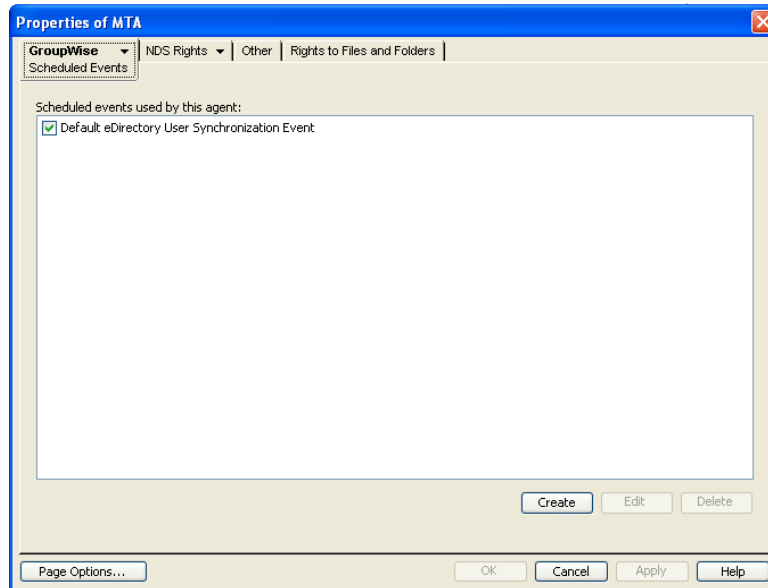
Scheduling eDirectory User Synchronization

By default, one eDirectory user synchronization event is scheduled at 1:00 a.m. daily for each MTA where eDirectory user synchronization is enabled.

You can edit the default event, or you can create one or more additional eDirectory user synchronization events to perform eDirectory user synchronization more frequently.

To schedule an eDirectory user synchronization event:

- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Scheduled Events* to display the Scheduled Events page.

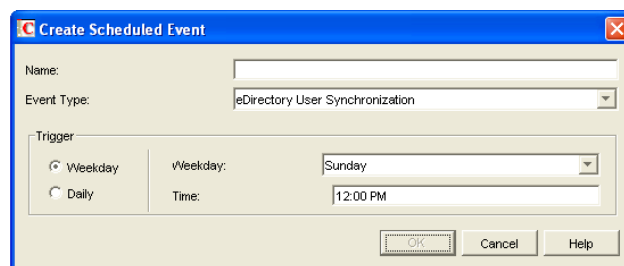


The Scheduled Events page lists a pool of MTA events available to all MTAs in your GroupWise system if any events have already been created.

- 3 Select the default event, then click *Edit*.

or

Click *Create*, then type a name for the event.



The name can include as many as 128 characters.

- 4 Set *Type* to *eDirectory User Synchronization*.
- 5 In the *Trigger* box, specify when you want the eDirectory user synchronization event to take place.

You can have the synchronization event take place once a week, once a day, or at any other regular interval, at whatever time you choose.

- 6 Specify the time of day when you want eDirectory user synchronization to take place.
- 7 Click *OK* twice to close the scheduled event dialog boxes and save the eDirectory user synchronization event.

ConsoleOne then notifies the MTA to restart so the eDirectory user synchronization event can be put into effect.

42.4.2 Enabling MTA Message Logging

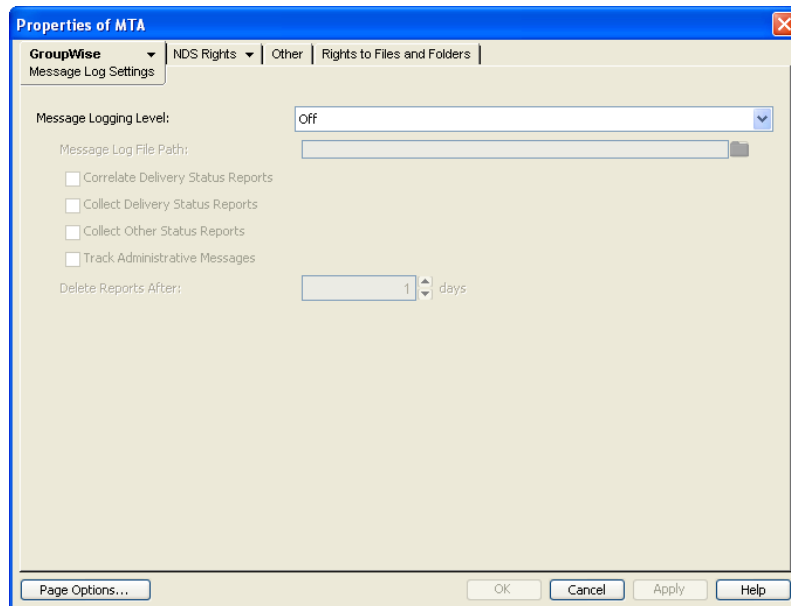
Message logging is turned off by default, because it causes the MTA to use additional CPU and disk resources. However, gathering information about message traffic on your GroupWise system lets you perform many valuable tasks, including:

- ♦ Tracking messages
- ♦ Gathering statistics to help optimize your GroupWise system
- ♦ Billing customers for messages delivered
- ♦ Tracking messages from the MTA Web console and from GroupWise Monitor

When you enable MTA message logging, the MTA stores data about GroupWise message traffic as it processes messages. The stored data is then available for use by the MTA Web console Message Tracking feature and by the GroupWise Monitor Message Tracking Report option. In addition, third-party programs can produce customized billing, tracking, and statistical reports based on the information stored in the database.

To enable MTA message logging:

- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Message Log Settings*.



- 3 In the *Message Logging* field, select a logging level to turn message logging on.
- 4 In the *Message Log Path* field, specify the full path of the file where the MTA will record the logging information.

- 5 Select the types of information you want to track:

Correlate Delivery Status Reports: Select this option to maintain the relationship between user messages and their corresponding delivery status reports in the logged information.

Collect Delivery Status Reports: Select this option to log delivery status reports as well as user messages.

Collect Other Status Reports: Select this option to log user-requested information about messages sent, such as indicating that messages have been opened or deleted by the recipients.

Track Administrative Messages: Select this option to log administrative messages such as database updates.

- 6 In the *Delete Reports After* field, specify the number of days to retain reports on disk. Reports are automatically deleted after the specified time has passed.

- 7 Click *OK* to save the MTA message log settings.

ConsoleOne then notifies the MTA to restart so the new settings can be put into effect.

- 8 For instructions about using the data that the MTA collects, see [“Tracking Messages” on page 675](#) and [Section 71.3.7, “Message Tracking Report,” on page 987](#).

Corresponding Startup Switches: You can also use the `--messagelogsettings`, `--messagelogpath`, `--messagelogdays`, and `--messagelogmaxsize` switches in the MTA startup file to configure MTA message logging.

43 Monitoring the MTA

By monitoring the MTA, you can determine whether or not its current configuration is meeting the needs of your GroupWise system. You have a variety of resources to help you monitor the operation of the MTA:

- ♦ [Section 43.1, “Using the MTA Server Console,” on page 659](#)
- ♦ [Section 43.2, “Using the MTA Web Console,” on page 669](#)
- ♦ [Section 43.3, “Using MTA Log Files,” on page 677](#)
- ♦ [Section 43.4, “Using GroupWise Monitor,” on page 678](#)
- ♦ [Section 43.5, “Using Novell Remote Manager,” on page 679](#)
- ♦ [Section 43.6, “Using an SNMP Management Console,” on page 679](#)
- ♦ [Section 43.7, “Notifying the Domain Administrator,” on page 682](#)
- ♦ [Section 43.8, “Using the MTA Error Message Documentation,” on page 683](#)
- ♦ [Section 43.9, “Employing MTA Troubleshooting Techniques,” on page 683](#)
- ♦ [Section 43.10, “Using Platform-Specific MTA Monitoring Tools,” on page 683](#)
- ♦ [Section 43.11, “Using MTA Message Logging,” on page 683](#)

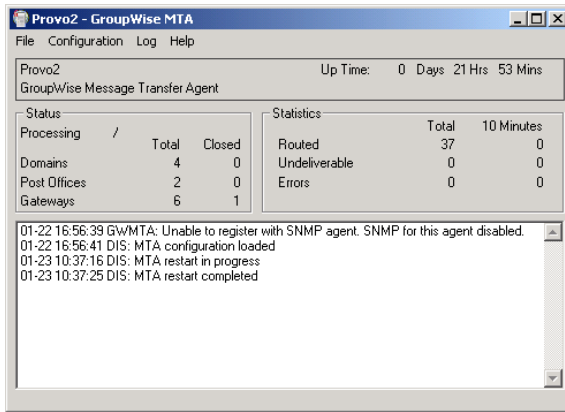
43.1 Using the MTA Server Console

The following topics help you monitor and control the MTA from the MTA server console:

- ♦ [Section 43.1.1, “Monitoring the MTA from the MTA Server Console,” on page 659](#)
- ♦ [Section 43.1.2, “Controlling the MTA from the MTA Server Console,” on page 662](#)

43.1.1 Monitoring the MTA from the MTA Server Console

The MTA server console provides information, status, and message statistics about the MTA to help you assess its current functioning.



Linux: You must use the `--show` startup switch in order to display the Linux MTA server console. See “Starting the Linux Agents with a User Interface” in “Installing GroupWise Agents” in the *GroupWise 2012 Installation Guide*.

Windows: You can suppress the Windows MTA server console by running the Windows MTA as a service. See “Starting the Windows GroupWise Agents” in “Installing GroupWise Agents” in the *GroupWise 2012 Installation Guide*.

The MTA server console consists of several components:

- ◆ “MTA Information Box” on page 660
- ◆ “MTA Status Box” on page 660
- ◆ “MTA Statistics Box” on page 661
- ◆ “MTA Alert Box” on page 661
- ◆ “MTA Admin Thread Status Box” on page 662

Do not exit the MTA server console unless you want to stop the MTA. You can minimize the MTA server console, but do not close it unless you want to stop the MTA.

MTA Information Box

The *MTA Information* box identifies the MTA whose MTA server console you are viewing, which is especially helpful when multiple MTAs are running on the same server.

Domain: Displays the name of the domain serviced by this MTA.

Description: Displays the description provided in the Description field in the MTA Information page in ConsoleOne. If multiple administrators work at the server where the MTA runs, the description can include a note about who to contact before stopping the MTA.

Up Time: Displays the length of time the MTA has been running.

MTA Web Console: The [Status](#) page also displays this information.

MTA Status Box

The *MTA Status* box displays the current status of the MTA and its backlog.

Processing: Displays a rotating bar when the MTA is running. If the bar is not rotating, the MTA has stopped. For assistance, see [“Message Transfer Agent Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

Domains: Displays the total number of domains the MTA links to and the number that are currently closed.

Post Offices: Displays the total number of post offices in the domain and the number that are currently closed.

Gateways: Displays the total number of gateways in the domain and the number that are currently closed.

If you have closed domains, post offices, or gateways, see [“MTA Status Box Shows a Closed Location”](#) in [“Message Transfer Agent Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems* for assistance.

MTA Web Console: The [Status](#) page also displays this information. In addition, you can display detailed information about specific queue contents.

MTA Statistics Box

The *MTA Statistics* box displays the total statistics for the current up time, and 10-minute statistics for all messages the MTA has routed.

Routed: Displays the number of messages successfully routed to the domains, post offices, and gateways serviced by the MTA.

Undeliverable: Displays the number of messages that could not be delivered to a domain, post office, or gateway. For assistance, see [“MTA Statistics Box Shows Undeliverable Messages”](#) in [“Message Transfer Agent Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

Errors: Displays the number of errors the MTA encounters while processing messages in its input queues. For assistance, see [“MTA Statistics Box Shows Errors”](#) in [“Message Transfer Agent Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

MTA Web Console: The [Status](#) page also displays this information.

MTA Alert Box

The *MTA Alert* box displays important messages that could require an administrator’s attention.

Informational Status Messages

When you first start the MTA, you typically see a message informing you that the MTA configuration has been loaded.

Error Messages

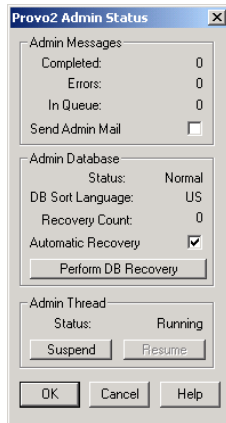
If the MTA encounters a problem that disrupts the flow of GroupWise messages, it displays an error message in the alert box. For assistance, see [“Message Transfer Agent Error Messages”](#) in *GroupWise 2012 Troubleshooting 1: Error Messages*.

MTA Web Console: The [Status](#) page also displays this information. In addition, you can view and search MTA log files on the [Log Files](#) page.

MTA Admin Thread Status Box

The MTA admin thread updates the domain database (`wpdomain.db`) when domains, post offices, users, and other types of object information are added, modified, or removed, and repairs it when damage is detected.

To display the *MTA Admin Thread Status* box from the MTA server console, click *Configuration > Admin Status*.



The following tasks pertain specifically to the MTA admin thread:

- ♦ [“Suspending/Resuming the MTA Admin Thread” on page 665](#)
- ♦ [“Displaying MTA Admin Thread Status” on page 666](#)
- ♦ [“Recovering the Domain Database Automatically or Immediately” on page 667](#)

MTA Web Console: You can display MTA admin thread status on the [Configuration](#) page. Under the *General Settings* heading, click *Admin Task Processing*. If the MTA Web console is password protected, as described in [Section 43.2.1, “Setting Up the MTA Web Console,” on page 669](#), you can change the admin settings for the current MTA session.

43.1.2 Controlling the MTA from the MTA Server Console

You can perform the following tasks to monitor and control the MTA from the MTA server console at the server where the MTA is running:

- ♦ [“Stopping the MTA” on page 663](#)
- ♦ [“Restarting the MTA” on page 664](#)
- ♦ [“Suspending/Resuming MTA Processing for a Location” on page 664](#)
- ♦ [“Suspending/Resuming the MTA Admin Thread” on page 665](#)
- ♦ [“Displaying the MTA Software Date” on page 665](#)
- ♦ [“Displaying the Current MTA Settings” on page 665](#)
- ♦ [“Displaying MTA Status Information” on page 665](#)
- ♦ [“Displaying MTA Admin Thread Status” on page 666](#)
- ♦ [“Recovering the Domain Database Automatically or Immediately” on page 667](#)
- ♦ [“Browsing the Current MTA Log File” on page 668](#)
- ♦ [“Viewing a Selected MTA Log File” on page 668](#)

- ♦ [“Cycling the MTA Log File”](#) on page 668
- ♦ [“Adjusting MTA Log Settings”](#) on page 669
- ♦ [“Editing the MTA Startup File”](#) on page 669
- ♦ [“Accessing Online Help for the MTA”](#) on page 669

Stopping the MTA

You might need to stop and restart the MTA for the following reasons:

- ♦ Updating the agent software
- ♦ Troubleshooting message flow problems
- ♦ Backing up the domain database
- ♦ Rebuilding the domain database

To stop the MTA from the MTA server console:

- 1 Click *File > Exit > Yes*.

Linux: If the Linux MTA does not respond to *Exit*, follow the instructions in [“Stopping the Linux MTA When It Is Running as a Daemon”](#) on page 663.

Windows: If the Windows MTA does not respond to *Exit*, you can close the MTA server console to stop the MTA or use the Task Manager to terminate the MTA task.

- 2 Restart the MTA, as described in the following sections in the [GroupWise 2012 Installation Guide](#):
 - ♦ [“Starting the Linux Agents as Daemons”](#)
 - ♦ [“Starting the Windows GroupWise Agents”](#)

Stopping the Linux MTA When It Is Running as a Daemon

To stop the Linux MTA when it is running in the background as a daemon and you started it using the `grpwise` script:

- 1 Make sure you are logged in as `root`.
- 2 Enter the following command:


```
rcgrpwise stop
```
- 3 Use the following command to verify that the MTA has stopped:


```
rcgrpwise status
```

To stop the Linux MTA when it is running in the background as a daemon and you started it manually (not using the `grpwise` script):

- 1 Make sure you are logged in as `root`.
- 2 Determine the process IDs (PIDs) of the MTA:

```
ps -eaf | grep gwmta
```

The PIDs for all `gwmta` processes are listed.

You can also obtain this information from the [Environment](#) page of the MTA Web console.

- 3 Kill the first MTA process listed:

Syntax: `kill PID`

Example: `kill 1483`

It might take a few seconds for all MTA processes to terminate.

- 4 Use the `ps` command to verify that the MTA has stopped:

```
ps -eaf | grep gwmnta
```

- 5 (Conditional) If the `kill` command does not stop the MTA, use the following command:

Syntax: `kill -9 PID`

Example: `kill -9 1483`

Restarting the MTA

Restarting the MTA from the MTA server console causes it to reread the configuration information provided in ConsoleOne. However, the MTA does not reread its startup file when you restart it from the MTA server console.

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *File > Restart > Yes* to restart the MTA.

If you want the MTA to reread its startup file, you must stop it, then restart it.

MTA Web Console: If the MTA Web console is password protected, as described in [Section 43.2.1, "Setting Up the MTA Web Console," on page 669](#), you can restart the MTA from the [Status](#) page. Click *Restart MTA* in the upper right corner of the page.

Suspending/Resuming MTA Processing for a Location

You can cause the MTA to stop processing messages for a location without stopping the MTA completely. For example, you could suspend message processing for a post office while backing up the post office.

To suspend the MTA for a location:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Status*.
- 3 Click the location (or multiple locations) to suspend, then click *Suspend*.

Routing of all messages to and from the location remains suspended until you resume processing.

To resume the MTA for a location:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Status*.
- 3 Click the location (or multiple locations) to resume, then click *Resume*.

MTA Web Console: If the MTA Web console is password protected, as described in [Section 43.2.1, "Setting Up the MTA Web Console," on page 669](#), you can suspend and resume processing for a specific location on the [Links](#) page. Select one or more locations, then click *Suspend* or *Resume* as needed.

Suspending/Resuming the MTA Admin Thread

You can cause the MTA to stop updating the domain database (`wpdomain.db`) without stopping the MTA completely. For example, you could suspend the MTA admin thread while backing up the domain database.

To suspend the MTA admin thread:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Admin Status > Suspend*.

The MTA admin thread no longer accesses the domain database until you resume processing.

To resume the MTA admin thread:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Admin Status > Resume*.

MTA Web Console: If the MTA Web console is password protected, as described in [Section 43.2.1, “Setting Up the MTA Web Console,” on page 669](#), you can suspend and resume the MTA admin thread from the [Configuration](#) page. Under the General Settings heading, click *Admin Task Processing > Suspend or Resume > Submit*.

Displaying the MTA Software Date

It is important to keep the MTA software up-to-date. You can display the date of the MTA software from the MTA server console.

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Help > About MTA*.

MTA Web Console: You also check the MTA software date on the [Environment](#) page.

Displaying the Current MTA Settings

You can list the current configuration settings of the MTA at the MTA server console.

To display the current MTA settings:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Agent Settings*.

For information about the MTA settings, see [Chapter 45, “Using MTA Startup Switches,” on page 693](#).

MTA Web Console: You check the current MTA settings on the [Configuration](#) page.

Displaying MTA Status Information

The MTA server console displays essential information about the functioning of the MTA. More detailed information is also available.

To display detailed MTA configuration information:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Status* to display a list of the locations to which the MTA is connected.

The following information is provided:

Location Name: Displays the name of the location serviced by the MTA.

Location Type: Indicates whether the location is a domain, post office, or gateway.

Connection Status: Indicates whether the MTA has been successful in locating and opening the database in the location.

- ♦ **Open:** The MTA can access the database or communicate with the agent at the location.
- ♦ **Closed:** The MTA cannot access the database or communicate with the agent at the location. For assistance, see “[MTA Configuration Status Isn’t Open](#)” in “[Message Transfer Agent Problems](#)” in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.
- ♦ **Suspended:** The MTA is not processing messages for the location because it has been suspended. See “[Suspending/Resuming MTA Processing for a Location](#)” on page 664.
- ♦ **Open Pending:** Post offices in the domain are in the process of opening and the MTA is clearing its holding queues. After this is accomplished, the MTA begins processing current messages and the status changes to Open.

Home: Displays the full path to the database that the MTA services in the listed location. For a TCP/IP connection, it displays the IP address of the server that the MTA connects to in order to service the database.

- 3 Select a location, then click *Details* to display the above information plus the following additional details:

Hold: Displays the full path to the location of the `mslocal` directory structure used by the MTA to hold messages for closed locations.

Pull: Displays the transfer pull directory, if any. See [Section 42.3.3, “Using a Transfer Pull Configuration \(Windows Only\),”](#) on page 650.

Version: Provides the version (2012, 8.0/7.0/6.x/5.x/4.x) of the database at the location.

Last Closed/Opened: Provides the date and time when the location was last closed and opened.

Last Closure Reason: Indicates why a closed location is closed. To look up last closure reasons, see “[Message Transfer Agent Error Messages](#)” in *GroupWise 2012 Troubleshooting 1: Error Messages*.

Messages Written/Read: Provides statistics about throughput since the MTA was last started.

Applications: Displays the programs the MTA can deliver messages to. Depending on the configuration of your GroupWise system, you might see GroupWise agents or GroupWise 4.1 servers listed.

TCP/IP: Lists the IP port the MTA listens on.

MTA Web Console: You can check the current MTA status on the [Links](#) page at the MTA Web console. Click a direct link to view its message queues.

Displaying MTA Admin Thread Status

Status information for the MTA admin thread is displayed in a separate dialog box, rather than on the main MTA server console.

To display MTA admin thread status information:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Admin Status*.

The following status information is displayed:

Admin Message Box

The Admin Message box provides the following information about the workload of the MTA admin thread:

Completed: Number of administrative message successfully processed.

Errors: Number of administrative messages not processed because of errors.

In Queue: Number of administrative messages waiting in the queue to be processed.

Send Admin Mail: Select this option to send a message to the administrator whenever a critical error occurs. See [Section 43.7, “Notifying the Domain Administrator,”](#) on page 682.

Admin Database Box

The *Admin Database* box provides the following information about the domain database:

Status: Displays one of the following statuses:

- ◆ **Normal:** The MTA admin thread is able to access the domain database normally.
- ◆ **Recovering:** The MTA admin thread is recovering the domain database.
- ◆ **DB Error:** The MTA admin thread has detected a critical database error. The domain database (`wppdomain.db`) cannot be recovered. Rebuild the domain database in ConsoleOne. See [Section 26.3, “Rebuilding Domain or Post Office Databases,”](#) on page 405.

The MTA admin thread does not process any more administrative messages until the database status has returned to Normal.

- ◆ **Unknown:** The MTA admin thread cannot determine the status of the domain database. Exit the MTA, then restart it, checking for errors on startup.

DB Sort Language: Displays the language code for the language that determines the sort order of lists displayed in ConsoleOne and the GroupWise Address Book.

Recovery Count: Displays the number of recoveries performed on the domain database for the current MTA session.

Admin Thread Box

The *Admin Thread* box provides the following information about the MTA admin thread:

Status: Displays one of the following statuses:

- ◆ **Running:** The MTA admin thread is active.
- ◆ **Suspended:** The MTA admin thread is not processing administrative messages.
- ◆ **Starting:** The MTA admin thread is initializing.
- ◆ **Terminated:** The MTA admin thread is not running.

MTA Web Console: You can display MTA admin thread status from the [Configuration](#) page. Under the *General Settings* heading, click *Admin Task Processing*.

Recovering the Domain Database Automatically or Immediately

The MTA admin thread can recover the domain database (`wppdomain.db`) when it detects a problem.

To enable/disable automatic domain database recovery:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Admin Status > Automatic Recovery* to toggle this feature on or off for the current MTA session.

To recover the domain database immediately:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Admin Status > Perform DB Recovery*.

For additional database repair procedures, see [Chapter 26, “Maintaining Domain and Post Office Databases,”](#) on page 401.

MTA Web Console: If the MTA Web console is password protected, as described in [Section 43.2.1, “Setting Up the MTA Web Console,”](#) on page 669, you can recover the post office database from the [Configuration](#) page. Under the *General Settings* heading, click *Admin Task Processing*. Select *Automatic Recovery* or *Perform DB Recovery* as needed.

Browsing the Current MTA Log File

The MTA displays only the most urgent messages in the alert box. Additional information is written to the MTA log file. The amount of information depends on the current log settings for the MTA. See [Section 43.3, “Using MTA Log Files,”](#) on page 677.

The information automatically scrolls up the screen as additional information is written. You can stop the automatic scrolling so you can manually scroll back through earlier information.

To browse the current MTA log file and control scrolling:

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Log > Active Log*.
- 3 Deselect *Automatic Scrolling* to manually scroll back through parts of the log that have already scrolled out of the box.
- 4 Click *Freeze* to stop the MTA from logging information to the active log box.
- 5 Click *Thaw* when you want the MTA to resume logging information to the active log box.

For explanations of messages in the MTA log file, see [“Message Transfer Agent Error Messages”](#) in [GroupWise 2012 Troubleshooting 1: Error Messages](#).

MTA Web Console: You can browse and search MTA log files on the [Log Files](#) page.

Viewing a Selected MTA Log File

Reviewing log files is an important way to monitor the functioning of the MTA.

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Log > View Log Files*.
- 3 Select a log file, then click *View*.

For explanations of messages in the MTA log file, see [“Message Transfer Agent Error Messages”](#) in [GroupWise 2012 Troubleshooting 1: Error Messages](#).

MTA Web Console: You can view and search MTA log files on the [Log Files](#) page.

Cycling the MTA Log File

You can have the MTA start a new log file as needed.

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Log > Cycle Log*.

Adjusting MTA Log Settings

Default log settings are established when you start the MTA. However, they can be adjusted for the current MTA session from the MTA server console.

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Log > Log Settings*.
- 3 Adjust the values as needed for the current MTA session.

See [Section 43.3, “Using MTA Log Files,” on page 677](#).

MTA Web Console: If the MTA Web console is password protected, as described in [Section 43.2.1, “Setting Up the MTA Web Console,” on page 669](#), you can adjust MTA log settings from the [Configuration](#) page. Click the *Event Log Settings* heading.

Editing the MTA Startup File

You can change the configuration of the MTA by editing the MTA startup file from the MTA server console.

- 1 At the server where the MTA is running, display the MTA server console.
- 2 Click *Configuration > Edit Startup File*.
- 3 Make the necessary changes, then save and exit the startup file.
- 4 Stop and restart the MTA.

Accessing Online Help for the MTA

Click *Help* on the menu bar for information about the MTA server console. Click the *Help* button in any dialog box for additional information.

43.2 Using the MTA Web Console

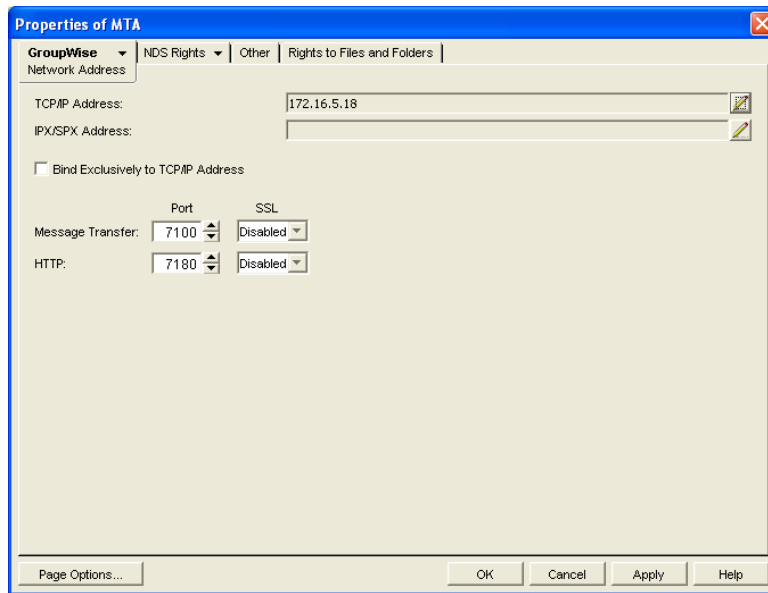
The MTA Web console enables you to monitor the MTA from any location where you have access to a Web browser and the Internet. This provides substantially more flexible access than the MTA server console, which can only be accessed from the server where the MTA is running.

- ♦ [Section 43.2.1, “Setting Up the MTA Web Console,” on page 669](#)
- ♦ [Section 43.2.2, “Accessing the MTA Web Console,” on page 671](#)
- ♦ [Section 43.2.3, “Monitoring the MTA from the MTA Web Console,” on page 672](#)
- ♦ [Section 43.2.4, “Controlling the MTA from the MTA Web Console,” on page 675](#)

43.2.1 Setting Up the MTA Web Console

The default HTTP port for the MTA Web console is established during MTA installation. You can change the port number and increase security after installation.

- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.



If you configured the MTA for TCP/IP links during installation, the *TCP/IP Address* field should display the MTA server's network address. If it does not, follow the instructions in ["Using TCP/IP Links between Domains"](#) on page 632. The MTA must be configured for TCP/IP in order to provide the MTA Web console.

- 3 Make a note of the IP address or DNS hostname in the *TCP/IP Address* field. You need this information to access the MTA Web console.

The *HTTP Port* field displays the default port number of 7180.

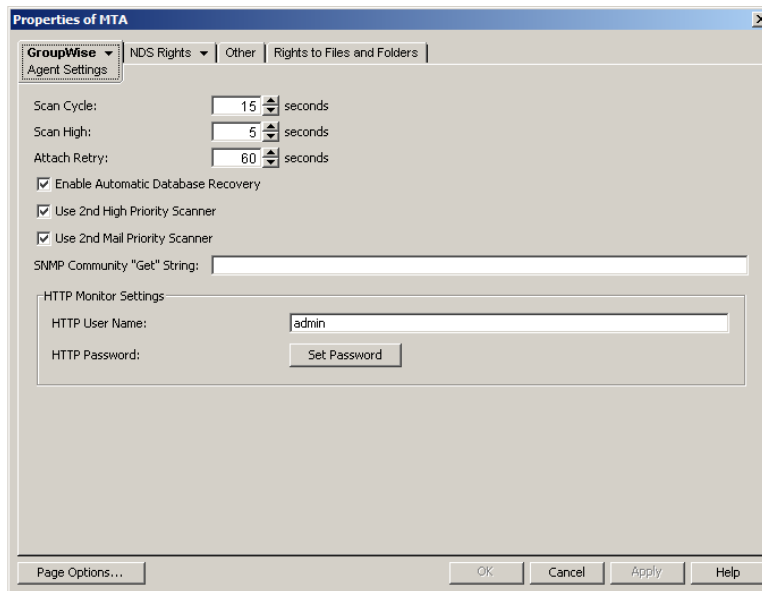
- 4 If the default HTTP port number is already in use on the MTA server, specify a unique port number.
- 5 Make a note of the HTTP port number. You will need this information to access the MTA Web console.
- 6 If you want to use an SSL connection for the MTA Web console, which provides optimum security, select *Enabled* in the *HTTP SSL* drop-down list.

For additional instructions about using SSL connections, see [Section 83.2, "Server Certificates and SSL Encryption,"](#) on page 1107.

- 7 Click *Apply* to save your changes on the Network Address page.

If you want to limit access to the MTA Web console, you can provide a user name and password.

- 8 Click *GroupWise > Agent Settings* to display the Agent Settings page.



9 In the *HTTP Settings* box:

9a In the *HTTP User Name* field, specify a unique user name.

9b Click *Set Password*.

9c Type the password twice for verification.

9d Click *Set Password*.

Unless you are using an SSL connection, do not use an eDirectory user name and password because the information passes over the non-secure connection between your Web browser and the MTA.

For convenience, use the same user name and password for all agents that you plan to monitor from GroupWise Monitor. This saves you from having to provide the user name and password information as Monitor accesses each agent.

10 Click *OK* to save the MTA Web console settings.

ConsoleOne then notifies the MTA to restart so the new settings can be put into effect.

Corresponding Startup Switches: You can also use the `--httpport`, `--httpuser`, and `--httppassword` startup switches in the MTA startup file to enable the MTA Web console. In addition, you can use the `--httprefresh` switch to control how often the MTA refreshes the information provided to your Web browser.

43.2.2 Accessing the MTA Web Console

To monitor the MTA from your Web browser, view the URL where the MTA is located by supplying the network address and port number as provided in ConsoleOne. For example:

```
http://172.16.5.18:7100
http://172.16.5.18:7180
http://server1:7100
https://server2:7180
```

When viewing the MTA Web console, you can specify either the message transfer port or the HTTP port.

GroupWise 2012 MTA - Provo1		
Status Configuration Environment Log Files Links Message Tracking Help		
Restart MTA		
Up Time: 0 Days 4 Hrs 11 Mins		
	Total	Closed
Domains	3	0
Post Offices	1	0
Gateways	1	0
Messages Processed		
	Total	Last 10 minutes
Routed	31	23
Undeliverable	0	0
Errors	0	0
Queue Information		
Router		0
Closed Links		
Alerts		
<12/05/11 14:11:35> DIS: MTA configuration loaded		

43.2.3 Monitoring the MTA from the MTA Web Console

The MTA Web console provides several pages of information to help you monitor the performance of the MTA. The title bar at the top of the MTA Web console displays the name of the MTA and its domain. Below the title bar appears the MTA Web console menu that lists the pages of information available in the MTA Web console. Online help throughout the MTA Web console helps you interpret the information being displayed and use the links provided.

- ◆ [“Monitoring MTA Status” on page 672](#)
- ◆ [“Checking the MTA Operating System Environment” on page 673](#)
- ◆ [“Viewing and Searching MTA Log Files” on page 673](#)
- ◆ [“Monitoring the Routing Queue” on page 674](#)
- ◆ [“Monitoring Links” on page 674](#)
- ◆ [“Tracking Messages” on page 675](#)

Monitoring MTA Status

When you first access the MTA Web console, the Status page is displayed. Online help throughout the MTA Web console helps you interpret the information being displayed and use the links provided.

GroupWise 2012 MTA - Provo1		
Status Configuration Environment Log Files Links Message Tracking Help		
Restart MTA		
Up Time: 0 Days 4 Hrs 11 Mins		
	Total	Closed
Domains	3	0
Post Offices	1	0
Gateways	1	0
Messages Processed		
	Total	Last 10 minutes
Routed	31	23
Undeliverable	0	0
Errors	0	0
Queue Information		
Router		0
Closed Links		
Alerts		
<12/05/11 14:11:35> DIS: MTA configuration loaded		

Click the *Router* link to display details about the MTA routing queue ([gwinprog](#)). You can quickly determine how many messages are awaiting processing, how large they are, and how long they have been waiting in the routing queue.

Click a closed location to display its holding queue to see how many messages are waiting for transfer.

Checking the MTA Operating System Environment

On the MTA Web console menu, click *Environment* to display information about the operating system where the MTA is running.

On a Linux server, the following information is displayed:

GroupWise 2012 MTA - Provo1	
Status Configuration Environment Log Files Links Message Tracking Help	
Server Configuration	
Server	jbd-oes
OS Revision	Linux Release 2.6.16.60-0.54.5-default
OES Version	Novell Open Enterprise Server 2.0.3 (x86_64)
Main Thread Process ID	22764
Build Dates	
GroupWise Agent Build Version	12.0.0-98273
GroupWise Agent Build Date	12-03-11
GroupWise Resource Build Date	11-11-11

On a Windows server, the following information is displayed:

GroupWise 2012 POA - Sales.Provo2	
Status Configuration Environment Log Files Scheduled Events MTP Status Help	
OS Data	
Windows Version	6.1 (Build 7601)Service Pack 1
Process ID	4840
Build Dates	
GroupWise Agent Build Version	12.0.0-98273
GroupWise Agent Build Date	12-03-11
GroupWise Engine Build Date	12-03-11
GroupWise Resource Build Date	12-03-11

Viewing and Searching MTA Log Files

On the MTA Web console menu, click *Log Files* to display and search MTA log files.

GroupWise 2012 MTA - Provo1																																														
Status Configuration Environment Log Files Links Message Tracking Help																																														
View Event Log Settings																																														
Event Log Filter																																														
Events containing <input type="text"/>																																														
Message type																																														
<input type="checkbox"/> Message logging	<input type="checkbox"/> Routing																																													
<input type="checkbox"/> Event logging	<input type="checkbox"/> Admin																																													
<input type="checkbox"/> Dispatcher	<input type="checkbox"/> Scanner																																													
<input type="checkbox"/> Message transfer																																														
Event logs: <input type="checkbox"/> Select all																																														
<table><tbody><tr><td>1123mta.001</td><td>11-24-11 00:00:00</td><td>0697147</td></tr><tr><td>1124mta.001</td><td>11-25-11 00:00:00</td><td>052669</td></tr><tr><td>1125mta.001</td><td>11-26-11 00:00:00</td><td>0711007</td></tr><tr><td>1126mta.001</td><td>11-27-11 00:00:00</td><td>0652837</td></tr><tr><td>1127mta.001</td><td>11-28-11 00:00:00</td><td>0656071</td></tr><tr><td>1128mta.001</td><td>11-28-11 18:34:47</td><td>0372541</td></tr><tr><td>1128mta.002</td><td>11-29-11 00:00:00</td><td>0202557</td></tr><tr><td>1129mta.001</td><td>11-30-11 00:00:00</td><td>0962658</td></tr><tr><td>1130mta.001</td><td>12-01-11 00:00:00</td><td>0595249</td></tr><tr><td>1201mta.001</td><td>12-02-11 00:00:00</td><td>0346861</td></tr><tr><td>1202mta.001</td><td>12-03-11 00:00:00</td><td>0345811</td></tr><tr><td>1203mta.001</td><td>12-04-11 00:00:00</td><td>0346990</td></tr><tr><td>1204mta.001</td><td>12-05-11 00:00:00</td><td>0346051</td></tr><tr><td>1205mta.001</td><td>12-05-11 13:54:34</td><td>0201250</td></tr><tr><td>• 1205mta.002</td><td>12-05-11 18:04:53</td><td>0098679</td></tr></tbody></table>		1123mta.001	11-24-11 00:00:00	0697147	1124mta.001	11-25-11 00:00:00	052669	1125mta.001	11-26-11 00:00:00	0711007	1126mta.001	11-27-11 00:00:00	0652837	1127mta.001	11-28-11 00:00:00	0656071	1128mta.001	11-28-11 18:34:47	0372541	1128mta.002	11-29-11 00:00:00	0202557	1129mta.001	11-30-11 00:00:00	0962658	1130mta.001	12-01-11 00:00:00	0595249	1201mta.001	12-02-11 00:00:00	0346861	1202mta.001	12-03-11 00:00:00	0345811	1203mta.001	12-04-11 00:00:00	0346990	1204mta.001	12-05-11 00:00:00	0346051	1205mta.001	12-05-11 13:54:34	0201250	• 1205mta.002	12-05-11 18:04:53	0098679
1123mta.001	11-24-11 00:00:00	0697147																																												
1124mta.001	11-25-11 00:00:00	052669																																												
1125mta.001	11-26-11 00:00:00	0711007																																												
1126mta.001	11-27-11 00:00:00	0652837																																												
1127mta.001	11-28-11 00:00:00	0656071																																												
1128mta.001	11-28-11 18:34:47	0372541																																												
1128mta.002	11-29-11 00:00:00	0202557																																												
1129mta.001	11-30-11 00:00:00	0962658																																												
1130mta.001	12-01-11 00:00:00	0595249																																												
1201mta.001	12-02-11 00:00:00	0346861																																												
1202mta.001	12-03-11 00:00:00	0345811																																												
1203mta.001	12-04-11 00:00:00	0346990																																												
1204mta.001	12-05-11 00:00:00	0346051																																												
1205mta.001	12-05-11 13:54:34	0201250																																												
• 1205mta.002	12-05-11 18:04:53	0098679																																												
<input type="button" value="View Events"/> <input type="button" value="Cycle Log"/>																																														

To view a particular log file, select the log file, then click *View Events*.

To search all log files for a particular string, type the string in the *Events Containing* field, select *Select All*, then click *View Events*. You can also manually select multiple log files to search.

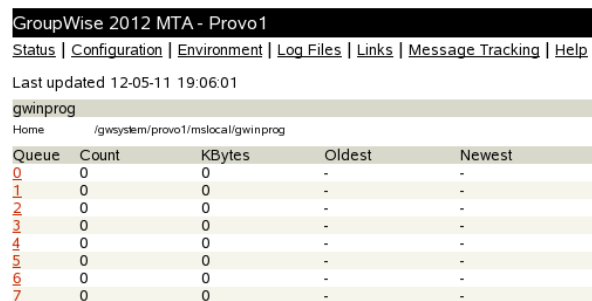
In the *Message Type* list, you can select one or more types of MTA processing to search for:

- ♦ **Message Logging (MLG):** The message logging threads write information into the message log file if message logging has been turned on. See [Section 42.4.2, “Enabling MTA Message Logging,”](#) on page 657.
- ♦ **Event Logging (LOG):** The event logging thread writes information into the event log files that you can search on this page. See [Section 43.3, “Using MTA Log Files,”](#) on page 677.
- ♦ **Dispatcher (DIS):** The dispatcher thread starts other MTA threads as needed to meet the demands being put on the MTA at any given time.
- ♦ **Message Transfer (MTP):** The message transfer threads communicate with other MTAs and with POAs in the local domain to transfer messages to domains and post offices to which the local MTA is linked by way of TCP/IP. See [“Using TCP/IP Links between Domains”](#) on page 632 and [“Using TCP/IP Links between a Domain and its Post Offices”](#) on page 637.
- ♦ **Routing (RTR):** The router threads process messages in the routing queue and prepare them for transfer to the next hop in the link path to their destinations. See [Section 44.3, “Optimizing the Routing Queue,”](#) on page 689.
- ♦ **Admin (ADM):** The admin thread updates the domain database (`wpdomain.db`) whenever administrative information changes. See [“MTA Admin Thread Status Box”](#) on page 662.
- ♦ **Scanner (SCA):** The scanner threads check for incoming messages when UNC or mapped links are in use. See [Section 44.2.3, “Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices,”](#) on page 688.

The results of the search are displayed on a separate page that can be printed.

Monitoring the Routing Queue

On the MTA Web console menu, click *Status*, then click *Router* to display the contents of the routing queue. Typically, no message files are waiting unless the MTA is down or backlogged.



Queue	Count	KBytes	Oldest	Newest
0	0	0	-	-
1	0	0	-	-
2	0	0	-	-
3	0	0	-	-
4	0	0	-	-
5	0	0	-	-
6	0	0	-	-
7	0	0	-	-

You can click any queue to view the message files it contains.

Monitoring Links

On the MTA Web console menu, click *Links* to monitor the direct links between the MTA and other locations.

GroupWise 2012 MTA - Provo1

Status | [Configuration](#) | [Environment](#) | [Log Files](#) | [Links](#) | [Message Tracking](#) | [Help](#)

Last updated 12-05-11 19:08:28 View [Link Configuration](#)
View [TCP/IP Connections](#)
View [Gateways](#)

Direct Link	Type	Status	Messages Queued	Oldest
<input type="checkbox"/> Provo1	Domain	Open	0	-
<input type="checkbox"/> Development	Post Office	Open	0	-
<input type="checkbox"/> GWIA	Gateway	Open	0	-
<input type="checkbox"/> Provo2	Domain	Open	0	-
<input type="checkbox"/> Provo3	Domain	Open	0	-

Click a location to view its holding queue. Click *View Link Configuration* to determine the address of each location and access the agent Web consoles of other domains and of post offices that belong to the local domain. Click *View TCP/IP Connections* to view incoming and outgoing TCP/IP links. Click *View Gateways* to restrict the list to just gateways.

Tracking Messages

Before you can track messages at the MTA Web console, you must enable message logging for MTAs throughout your system. See [Section 42.4.2, “Enabling MTA Message Logging,” on page 657](#). When you enable MTA message logging, the MTA stores data about GroupWise message traffic as it processes messages. The stored data is then available for use from the MTA Web console.

To track a specific message, have the sender check the Sent Item Properties for the message in the GroupWise client. The *Mail Envelope Properties* field displays the message ID of the message; for example, 3AD5EDEB.31D : 3 : 12763. To track all messages sent by a particular user, make a note of the user’s GroupWise user ID.

On the MTA Web console menu, click *Message Tracking*.

GroupWise 2012 MTA - Provo1

Status | [Configuration](#) | [Environment](#) | [Log Files](#) | [Links](#) | [Message Tracking](#) | [Help](#)

View [Message Log Settings](#)
View [Log Files](#)

Message Tracking

Filename

Message ID

Originabr

Fill in *one* of the fields, depending on what you want to track, then click *Submit*. The results of the search are displayed on a separate page which can be printed.

43.2.4 Controlling the MTA from the MTA Web Console

At the MTA Web console, you can change some MTA log settings for the current MTA session. You can also stop and start some specific MTA threads.

IMPORTANT: In order to control the MTA from the MTA Web console, you must set up authentication for the MTA Web console, as described in [Section 43.2.1, “Setting Up the MTA Web Console,”](#) on page 669.

- ◆ [“Changing MTA Configuration Settings”](#) on page 676
- ◆ [“Controlling the MTA Admin Thread”](#) on page 676
- ◆ [“Controlling Links to Other Locations”](#) on page 677

Changing MTA Configuration Settings

On the MTA Web console menu, click *Configuration*. Online help on the Configuration page helps you interpret the configuration information being displayed.

GroupWise 2012 MTA - Provo1	
Status Configuration Environment Log Files Links Message Tracking Help	
GroupWise MTA Configuration Settings	
General Settings:	
Domain Directory:	/gwsystem/provo1
Work Directory:	/gwsystem/provo1/mslocal
Database Version:	12
Preferred GWIA:	Provo1.GWIA
Default Route:	
Force Route:	No
Known IDomains:	*yourcompanyname.com
Allow Direct Send to Other Systems:	No
Error Mail to Administrator:	No
Display the Active Log Window Initially:	No
eDirectory Authenticated:	Yes
eDirectory User Synchronization:	Yes
Admin Task Processing :	Yes
Database Recovery:	Yes
Simple Network Management Protocol (SNMP):	Disabled
IPv6 Protocol:	Enabled
Startup File :	
TCP/IP Settings:	
Maximum Inbound TCP/IP Connections:	40
TCP/IP Address:	172.15.7.17
TCP Port for Incoming Connections:	7100
Message Transfer over SSL:	Disabled
TCP Port for HTTP Connections:	7180
HTTP Refresh Rate:	60 secs
HTTP over SSL:	Disabled
TCP/IP Connection Timeout:	40
TCP/IP Data Timeout:	40
Event Log Settings :	
Log Level:	Normal
Disk Logging:	Yes

Click the *Event Log Settings* heading to change the MTA log settings for the current MTA session.

Controlling the MTA Admin Thread

On the Configuration page, click *Admin Task Processing*.

GroupWise 2012 MTA - Provo1	
Status Configuration Environment Log Files Links Message Tracking Help	
Provo1	
Admin Messages	
Completed:	8
Errors:	0
Send Admin Mail:	<input type="checkbox"/>
Admin Database	
Status:	Normal
DB Sort Language:	EN
Recovery Count:	0
Automatic Recovery:	<input checked="" type="checkbox"/>
Perform DB Recovery:	<input type="checkbox"/>
Admin Thread	
Status:	Running
Suspend:	<input type="radio"/>
Resume:	<input type="radio"/>
<input type="button" value="Submit"/>	

Modify the functioning of the MTA admin thread as needed, then click *Submit*. The changes remain in effect for the current MTA session.

Controlling Links to Other Locations

On the MTA Web console menu, click *Links*.

Direct Link	Type	Status	Messages Queued	Oldest
<input type="checkbox"/> Provo1	Domain	Open	0	-
<input type="checkbox"/> Development	Post Office	Open	0	-
<input type="checkbox"/> GWA	Gateway	Open	0	-
<input type="checkbox"/> Provo2	Domain	Open	0	-
<input type="checkbox"/> Provo3	Domain	Open	0	-

Select one or more locations, then click *Suspend* or *Resume* as needed.

43.3 Using MTA Log Files

Error messages and other information about MTA functioning are written to log files as well as displaying on the MTA server console. Log files can provide a wealth of information for resolving problems with MTA functioning or message flow. This section covers the following subjects to help you get the most from MTA log files:

- ♦ [Section 43.3.1, “Locating MTA Log Files,”](#) on page 677
- ♦ [Section 43.3.2, “Configuring MTA Log Settings and Switches,”](#) on page 677
- ♦ [Section 43.3.3, “Viewing MTA Log Files,”](#) on page 678
- ♦ [Section 43.3.4, “Interpreting MTA Log File Information,”](#) on page 678

43.3.1 Locating MTA Log Files

The default location of the MTA log files varies by platform:

Linux: `/var/log/novell/groupwise/domain_name.mta`

Windows: `mslocal` subdirectory in the directory specified by the `--work` switch

You can change the location where the MTA creates its log files, as described in [Configuring MTA Log Settings and Switches](#).

43.3.2 Configuring MTA Log Settings and Switches

The following aspects of logging are configurable:

- ♦ Log File Path (`--log`)
- ♦ Disk Logging (`--logdiskoff`)
- ♦ Logging Level (`--loglevel`)

- ♦ Maximum Log File Age ([--logdays](#))
- ♦ Maximum Log File Size ([--logmax](#))

You can configure the log settings in the following ways:

- ♦ Using ConsoleOne to establish defaults ([Section 42.1.8, “Adjusting the MTA Logging Level and Other Log Settings,”](#) on page 641)
- ♦ Using startup switches to override ConsoleOne settings ([Section 45, “Using MTA Startup Switches,”](#) on page 693)
- ♦ Using the MTA server console to override log MTA settings for the current session ([“Adjusting MTA Log Settings”](#) on page 669)
- ♦ Using the MTA Web console to override other MTA settings for the current MTA session ([Section 43.2.4, “Controlling the MTA from the MTA Web Console,”](#) on page 675)

43.3.3 Viewing MTA Log Files

You can view the contents of the MTA log file from the MTA server console and Web console. See the following tasks:

- ♦ [“Browsing the Current MTA Log File”](#) on page 668
- ♦ [“Viewing a Selected MTA Log File”](#) on page 668
- ♦ [“Cycling the MTA Log File”](#) on page 668
- ♦ [“Viewing and Searching MTA Log Files”](#) on page 673

43.3.4 Interpreting MTA Log File Information

On startup, the MTA records the MTA settings currently in effect. Thereafter, it logs events that take place, including errors. To look up error messages that appear in MTA log files, see [“Message Transfer Agent Error Messages”](#) in *GroupWise 2012 Troubleshooting 1: Error Messages*.

Because the MTA consists of multiple threads, you might find it useful to retrieve the log file into an editor and sort it on the thread ID that follows the date and time information. Sorting groups all messages together for the same MTA thread. At the MTA Web console, you can search through multiple log files. See [“Viewing and Searching MTA Log Files”](#) on page 673. You can also use the search capability of the MTA Web console to gather information about a specific MTA thread. See [“Viewing and Searching MTA Log Files”](#) on page 673.

43.4 Using GroupWise Monitor

GroupWise Monitor is a monitoring and management tool that allows you to monitor GroupWise agents and gateways from any location where you are connected to the Internet and have access to a Web browser. The MTA Web console can be accessed from GroupWise Monitor, enabling you to monitor all MTAs in your GroupWise system from one convenient location. In addition, GroupWise Monitor can notify you when agent problems arise.



For installation and setup instructions, see “[Installing GroupWise Monitor](#)” in the *GroupWise 2012 Installation Guide*. For usage instructions, see [Part XV, “Monitor,”](#) on page 939.

43.5 Using Novell Remote Manager

If the MTA is running on Novell Open Enterprise Server (OES), you can use Novell Remote Manager to monitor the MTA. For more information, see the *Novell Remote Manager for Linux Administration Guide* for your version of OES Linux (<http://www.novell.com/documentation/oes.html>).

43.6 Using an SNMP Management Console

You can monitor the MTA from the Management and Monitoring component of Novell ZENworks for Servers or another SNMP management and monitoring program. When properly configured, the MTA sends SNMP traps to network management consoles for display along with other SNMP monitored programs.

Although the MTA is SNMP-enabled by default, the server where the MTA is installed must be properly configured to support SNMP, and the MTA object in eDirectory must be properly configured as well. To set up SNMP services for your server, complete the following tasks:

- [Section 43.6.1, “Setting Up SNMP Services for the MTA,”](#) on page 679
- [Section 43.6.2, “Copying and Compiling the MTA MIB File,”](#) on page 681
- [Section 43.6.3, “Configuring the MTA for SNMP Monitoring,”](#) on page 682

43.6.1 Setting Up SNMP Services for the MTA

Select the instructions for the platform where the MTA runs:

- [“Linux: Setting Up SNMP Services for the MTA”](#) on page 680
- [“Windows: Setting Up SNMP Services for the MTA”](#) on page 680

Linux: Setting Up SNMP Services for the MTA

The Linux MTA is compatible with NET-SNMP. An older version of SNMP called UCD-SNMP cannot be used with the Linux MTA. NET-SNMP comes standard with OES Linux, but it does not come standard with SLES 9. If you are using SLES 9, you must update to NET-SNMP in order to use SNMP to monitor the Linux MTA.

- 1 Make sure you are logged in as root.
- 2 If NET-SNMP is not already set up on your Linux server, use the following command to configure SNMP:

```
snmpconf -g basic_setup
```

The `snmpconf` command creates the `snmpd.conf` file in one of the following directories, depending on your version of Linux:

```
/usr/share/snmp  
/usr/local/share/snmp  
~/ .snmp
```

- 3 Locate the `snmpd.conf` file on your Linux server.
- 4 In a text editor, open the `snmpd.conf` file and add the following line:

```
dlmod Gwsnmp /opt/novell/groupwise/agents/lib/libgwsnmp.so
```
- 5 Save the `snmpd.conf` file and exit the text editor.
- 6 Restart the SNMP daemon (`snmpd`) to put the changes into effect.

IMPORTANT: Make sure that the SNMP daemon always starts before the MTA starts.

- 7 Skip to [Section 43.6.2, “Copying and Compiling the MTA MIB File,”](#) on page 681.

Windows: Setting Up SNMP Services for the MTA

For Windows, the SNMP Service is usually not included during the initial operating system installation. The SNMP Service can be easily added at any time. To add or configure the SNMP Service, you must be logged in as a member of the Administrator group.

To set up SNMP services for the Windows MTA, complete the following tasks:

- ♦ [“Installing SNMP Support on Windows Server 2008”](#) on page 680
- ♦ [“Installing SNMP Support on Windows Server 2003”](#) on page 681
- ♦ [“Installing GroupWise Agent SNMP Support”](#) on page 681

Installing SNMP Support on Windows Server 2008

- 1 On the Control Panel, click *Programs and Features*.
- 2 Click *Turn Windows features on or off* to open the Server Manager.
- 3 Click *Features > Add Features*.
- 4 In the *Features* list, expand *SNMP Services*, then select *SNMP Service*.
- 5 Click *Next*, then click *Install*.
- 6 When the installation is finished, click *Close*, then exit the Server Manager.
- 7 Skip to [Installing GroupWise Agent SNMP Support](#).

Installing SNMP Support on Windows Server 2003

- 1 Click *Start > Control Panel > Add or Remove Programs*.
- 2 Click *Add/Remove Windows Components*.
- 3 Select *Management and Monitoring Tools*.
- 4 Click *Details*, then select *Simple Network Management Protocol*.
- 5 Follow the on-screen instructions to install the SNMP Trap Service.
- 6 Continue with [Installing GroupWise Agent SNMP Support](#).

Installing GroupWise Agent SNMP Support

The GroupWise Agent Installation program includes an option for installing SNMP support. However, if the server where you installed the agents did not yet have SNMP set up, that installation option was not available. Now that you have set up SNMP, you can install GroupWise agent SNMP support.

At the Windows server where you want to install the GroupWise agent SNMP support:

- 1 Run `setup.exe` at the root of the downloaded *GroupWise 2012* software image.
- 2 Click *Install GroupWise System*, click *Yes* to accept the License Agreement, then click *Next* to perform a standard installation.
- 3 Select *Install individual components*, deselect *GroupWise Administration*, then click *Next*.
- 4 On the Installation Path page, browse to and select the path where the agent software is installed, then select *Install and Configure SNMP for GroupWise Agents*.
- 5 Continue through the rest of the installation process as prompted by the Agent Installation program.
The Agent Installation program copies the SNMP support files to the agent installation directory, makes the appropriate Windows registry entries, and restarts the Windows SNMP service.
- 6 Continue with [Section 43.6.2, "Copying and Compiling the MTA MIB File,"](#) on page 681.

43.6.2 Copying and Compiling the MTA MIB File

An SNMP-enabled MTA returns information contained in a Management Information Base (MIB). The MIB is an ASCII data structure that defines the information gathered. It also defines the properties that can be monitored and managed on the SNMP-enabled MTA.

Before you can monitor an SNMP-enabled MTA, you must compile the `gwmta.mib` file using your SNMP management program. GroupWise agent MIB files are located in the `/agents/snmpmibs` directory of your GroupWise software distribution directory or the downloaded *GroupWise 2012* software image.

The MIB file contains all the Trap, Set, and Get variables used for communication between the MTA and management console. The Trap variables provide warnings that point to current and potential problems. The Set variables allow you to configure portions of the application while it is still running. The Get variables display the current status of different processes of the application.

- 1 Copy the `gwmta.mib` file from the `\agents\snmp` directory to the location required by your SNMP management program.
- 2 Compile or import the `gwmta.mib` file as required by your SNMP management program.
- 3 Continue with [Configuring the MTA for SNMP Monitoring](#).

43.6.3 Configuring the MTA for SNMP Monitoring

In order for SNMP monitoring programs to monitor the MTA, the MTA must be configured with a network address and SNMP community string.

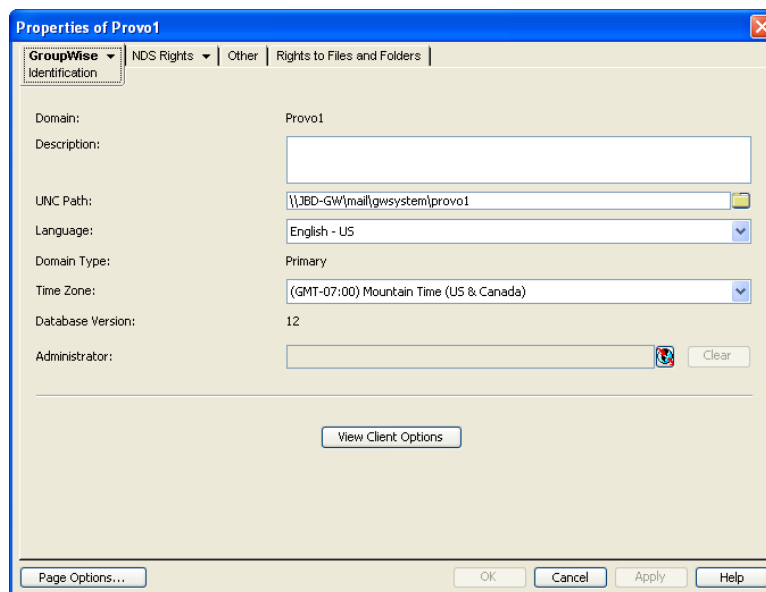
- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.
- 3 Click the pencil icon to provide the TCP/IP address of the server where the MTA runs, then click *Apply*.
- 4 Click *GroupWise > Agent Settings*.
- 5 Provide your system SNMP community GET string, then click *OK*.
- 6 Configure the SNMP Service with the same community GET string:
 - 6a On the Windows desktop, click *Start > Administrator Tools > Services*.
 - 6b Right-click *SNMP Service*, then click *Properties*.
 - 6c Click *Security*, then click *Add* in the *Accepted community names* list.
 - 6d In the *Community Name* field, specify your system SNMP community GET string.
 - 6e In the *Community Rights* drop down list, select *READ WRITE*.
 - 6f Click *Add* to add the community string to the list, then click *OK* to close the SNMP Properties
- 7 Restart the MTA.

The MTA should now be visible to your SNMP monitoring program.

43.7 Notifying the Domain Administrator

If you want to be notified with an email message whenever the MTA encounters a critical error, you can designate yourself as an administrator of the domain for which the MTA is running.

- 1 In ConsoleOne, browse to and right-click the Domain object, then click *Properties* to display the Identification page.



- 2 In the *Administrator* field, browse to and select your GroupWise user ID.

A domain can have a single administrator, or you can create a group to function as administrators.

- 3 Click *OK* to save the administrator information.

The selected user or group then begins receiving email messages whenever the MTA for the domain encounters a critical error.

Corresponding Startup Switches: By default, the MTA generates error mail if an administrator has been assigned for the domain. Error mail can be turned off using the `--noerrormail` switch.

MTA Web Console: Another way to receive email notification of MTA problems is to use GroupWise Monitor to access the MTA Web console. See [Section 69.5.1, “Configuring Email Notification,”](#) on page 957.

43.8 Using the MTA Error Message Documentation

MTA error messages are documented with the source and explanation of the error, possible causes of the error, and actions to take to resolve the error. See “[Message Transfer Agent Error Messages](#)” in *GroupWise 2012 Troubleshooting 1: Error Messages*.

43.9 Employing MTA Troubleshooting Techniques

If you are having a problem with the MTA but not receiving a specific error message, or if the suggested actions for the specific error did not resolve the problem, you can review more general troubleshooting strategies for dealing with MTA problems. See “[Message Transfer Agent Problems](#)” in “[Strategies for Agent Problems](#)” in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

You can also use GroupWise Monitor to troubleshoot message transfer problems. See [Part XV, “Monitor,”](#) on page 939.

43.10 Using Platform-Specific MTA Monitoring Tools

Each operating system where the MTA runs provides tools for monitoring programs.

Linux: You can use SNMP tools like `snmpget` and `snmpwalk` that allow you to retrieve the data about all the services registered with the SNMP service. These tools are part of the NET-SNMP package. See your Linux documentation for additional monitoring suggestions.

Windows: You can use the Performance Monitor in Windows Administrator Tools to gather similar information. See your Windows documentation for additional monitoring suggestions.

43.11 Using MTA Message Logging

For extremely detailed monitoring of message flow, you can configure the MTA to gather a variety of statistics. See [Section 42.4.2, “Enabling MTA Message Logging,”](#) on page 657.

44 Optimizing the MTA

You can adjust how the MTA functions to optimize its performance. Before attempting optimization, you should run the MTA long enough to observe its efficiency and its impact on other network applications running on the same server. See [Chapter 43, “Monitoring the MTA,”](#) on page 659.

Also, remember that optimizing your network hardware and operating system can make a difference in MTA performance.

The following topics help you optimize the MTA:

- ♦ [Section 44.1, “Optimizing TCP/IP Links,”](#) on page 685
- ♦ [Section 44.2, “Optimizing Mapped/UNC Links,”](#) on page 686
- ♦ [Section 44.3, “Optimizing the Routing Queue,”](#) on page 689
- ♦ [Section 44.4, “Adjusting MTA Polling of Closed Locations,”](#) on page 690

44.1 Optimizing TCP/IP Links

Using startup switches in the MTA startup file, you can fine-tune the performance of TCP/IP links.

- ♦ [Section 44.1.1, “Adjusting the Number of MTA TCP/IP Connections,”](#) on page 685
- ♦ [Section 44.1.2, “Adjusting the MTA Wait Intervals for Slow TCP/IP Connections,”](#) on page 686

44.1.1 Adjusting the Number of MTA TCP/IP Connections

When using TCP/IP links between domains, you can control the number of inbound connections the MTA can establish for receiving messages from POAs and GWIAs in the same domain and from MTAs and GWIAs in other domains in your GroupWise system.

Use the `--tcpinbound` switch in the MTA startup file to increase the maximum number of inbound connections the MTA can establish from the default of 40 to whatever setting meets the needs of your system. There is no maximum setting.

If the MTA is receiving more requests than it can accept, the sending MTAs must wait until a connection becomes available, which slows down message transfer. Each connection requires only about 20 KB. For example, if you configure the MTA to accept 600 connections, it would require approximately 12 MB of RAM. Although there is no maximum setting for inbound connections, this setting is adequate to handle very heavy usage. Use lower settings to conserve RAM or for lighter usage.

MTA Web Console: You can check the maximum number of TCP/IP connections that the MTA can start on the [Configuration](#) page under the *TCP/IP Settings* heading.

44.1.2 Adjusting the MTA Wait Intervals for Slow TCP/IP Connections

When using TCP/IP links, you can control how long the MTA waits for responses.

By default, the MTA waits 5 seconds for a response when trying to contact another MTA or a POA across a TCP/IP link. If no response is received from the other MTA or the POA, the sending MTA tries again three more times. If all four attempts fail, the MTA reports an error, then waits 10 minutes before it tries again.

When the MTA attempts to send messages to another MTA or a POA across a TCP/IP link, the sending MTA tries for 20 seconds before reporting an error.

On some networks, these wait intervals might not be sufficient, and the MTA might report an error when, by waiting longer, the needed connection or data transfer could take place.

Use the `--tcpwaitconnect` switch in the MTA startup file to increase the number of seconds the MTA waits for a response from another MTA or a POA across a TCP/IP link.

Use the `--tcpwaitdata` switch in the MTA startup file to increase the number of seconds the MTA attempts to send messages to another MTA or a POA across a TCP/IP link.

MTA Web Console: You can check the current wait intervals on the [Configuration](#) page under the *TCP/IP Settings* heading.

44.2 Optimizing Mapped/UNC Links

If you must use mapped or UNC links, you can fine-tune how the MTA polls its input queues.

- ♦ [Section 44.2.1, “Using TCP/IP Links between Locations,” on page 686](#)
- ♦ [Section 44.2.2, “Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways,” on page 686](#)
- ♦ [Section 44.2.3, “Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices,” on page 688](#)

NOTE: The Linux MTA does not use mapped or UNC links.

44.2.1 Using TCP/IP Links between Locations

TCP/IP links between domains or between a domain and its post offices are faster than mapped or UNC links because the MTA is immediately notified whenever a new message arrives. This eliminates the latency involved in scanning input directories for messages to process. To change from mapped or UNC links to TCP/IP links, see [“Using TCP/IP Links between Domains” on page 632](#) and [“Using TCP/IP Links between a Domain and its Post Offices” on page 637](#)

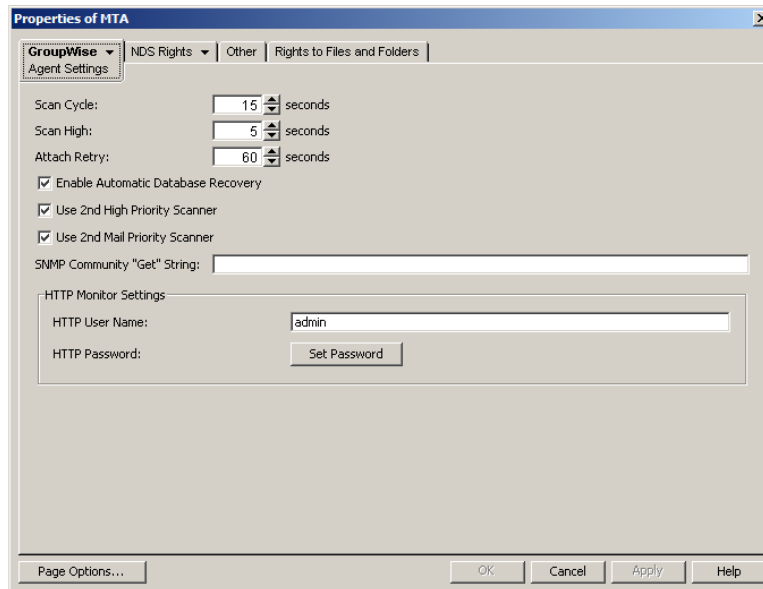
44.2.2 Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways

When using mapped or UNC links between the local domain and its post offices and other domains, the MTA can create a lot of network traffic just scanning its input queues, especially if the message load is light. This can be minimized by setting the scan cycle to a higher number. On the other hand,

if the scan cycle is set too high, important messages might need to wait in the input queues to be picked up by the MTA. The MTA's scan cycle settings also control how often it communicates with gateways installed in the domain.

By default, when using mapped or UNC links, the MTA scans its high priority queues every 5 seconds and its regular and low priority queues every 15 seconds. You can adjust the scan cycle settings to meet the needs of your GroupWise system.

- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 3 Decrease the number of seconds in the *Scan Cycle* field if you want the MTA to scan the regular and low priority queues (2-7) more often.

or

Increase the number of seconds in *Scan Cycle* field if you want the MTA to scan the regular and low priority queues (2-7) less often.

- 4 Decrease the number of seconds in the *Scan High* field if you want the MTA to scan the high priority queues (0-1) more often.

or

Increase the number of seconds in the *Scan High* field if you want the MTA to scan high priority queues (0-1) less often.

For the locations and specific uses of the MTA input queues, see "[Message Transfer/Storage Directories](#)" in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

- 5 Click *OK* to save the new scan cycle settings.

ConsoleOne then notifies the MTA to restart so the new settings can be put into effect.

Corresponding Startup Switches: You can also use the `--cylo` and `--cyhi` switches in the MTA startup file to adjust the MTA scan cycle.

MTA Web Console: You can check the current MTA scan cycle on the [Configuration](#) page under the *Performance Settings* heading.

44.2.3 Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices

When using mapped or UNC links, the MTA automatically starts four scanner threads, one for each of the following subdirectories of its input queues:

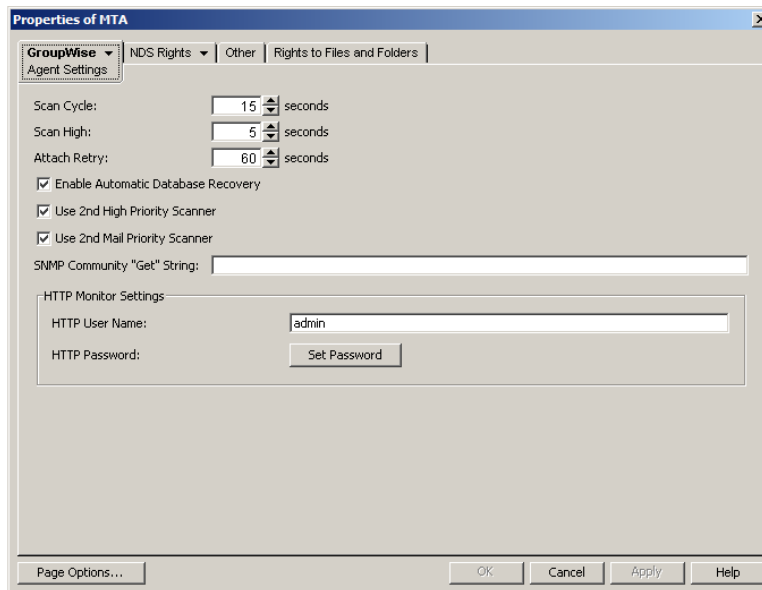
Priority Subdirectory	Used For
0	Busy Search requests from GroupWise client users
1	GroupWise Remote user requests
2	Administrative messages and high priority user messages
3-7	Regular and low priority messages and status messages

For the locations of the MTA input queues, see “[Message Transfer/Storage Directories](#)” in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

To conserve server resources, you can reduce the number of scanner threads that the POA starts, but this is not recommended.

IMPORTANT: Do not try to run more than one MTA for the same domain.

- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Agent Settings page.



Use 2nd High Priority Scanner is selected by default to provide separate MTA scanner threads for Busy Searches and GroupWise Remote users.

Use 2nd Mail Priority Scanner is selected by default to provide separate MTA scanner threads for administrative messages and high priority user messages vs. regular and low priority messages.

With these default settings, the MTA always starts four scanner threads. You can deselect either option so that the MTA starts fewer scanner threads

- 3 Deselect scanner thread options to allocate threads to priority subdirectories as shown in the table below.

Primary Use	Priority Directory	Two Scanner Threads	Two High Priority Scanners	Two Mail Priority Scanners	Default Operation
Busy searches	wpcsin\0	High priority scanner thread	High priority scanner thread one	High priority scanner thread	High priority scanner thread one
GroupWise Remote user requests	wpcsin\1		High priority scanner thread two		High priority scanner thread two
Administrative requests and high priority messages	wpcsin\2	Mail priority scanner thread	Mail priority scanner thread	Mail priority scanner thread one	Mail priority scanner thread one
High priority statuses	wpcsin\3				
Normal priority messages	wpcsin\4			Mail priority scanner thread two	Mail priority scanner thread two
Normal priority statuses	wpcsin\5				
Low priority messages	wpcsin\6				
Low priority statuses	wpcsin\7				
Total Scanner Threads in Use:		2	3	3	4

- 4 Click *OK* to save the new scanner thread settings.

ConsoleOne then notifies the MTA to restart so the new setting can be put into effect.

Corresponding Startup Switches: You can also use the `--fast0` and `--fast4` switches in the MTA startup file to adjust the allocation of MTA scanner threads.

MTA Web Console: You can check the current MTA scan cycle on the [Configuration](#) page under the *Performance Settings* heading.

44.3 Optimizing the Routing Queue

Using startup switches in the MTA startup file, you can fine-tune MTA processing in of the routing queue. When the MTA starts, it starts one or more router threads to process its routing queue ([gwinprog](#)). As messages arrive in the routing queue, it starts additional routers as needed, within parameters you can set.

- ♦ [Section 44.3.1, “Adjusting the Maximum Number of Active Router Threads,”](#) on page 690
- ♦ [Section 44.3.2, “Adjusting the Maximum Number of Idle Router Threads,”](#) on page 690

MTA Web Console: You can view the current contents of the routing queue from the [Status](#) page. Click *Router* under the *Queue Information* heading.

44.3.1 Adjusting the Maximum Number of Active Router Threads

By default, the MTA continues to start additional router threads to process messages in the routing queue as long as message traffic demands it, until as many as 16 router threads are running. Use the `--maxrouters` switch in the MTA startup file to control the number of router threads the MTA can start.

Set `--maxrouters` to a lower number to conserve resources and keep the MTA from starting more than the specified maximum number of router threads.

44.3.2 Adjusting the Maximum Number of Idle Router Threads

By default, after the MTA starts a router thread, it keeps it running, up to the maximum number specified by the `--maxrouters` switch. In a system where short bursts of heavy message traffic are followed by extended lulls, idle router threads could be consuming resources that would be better used by other processes. Use the `--maxidlerouters` switch in the MTA startup file to determine how many idle router threads are allowed to remain running. The default is 16 idle router threads.

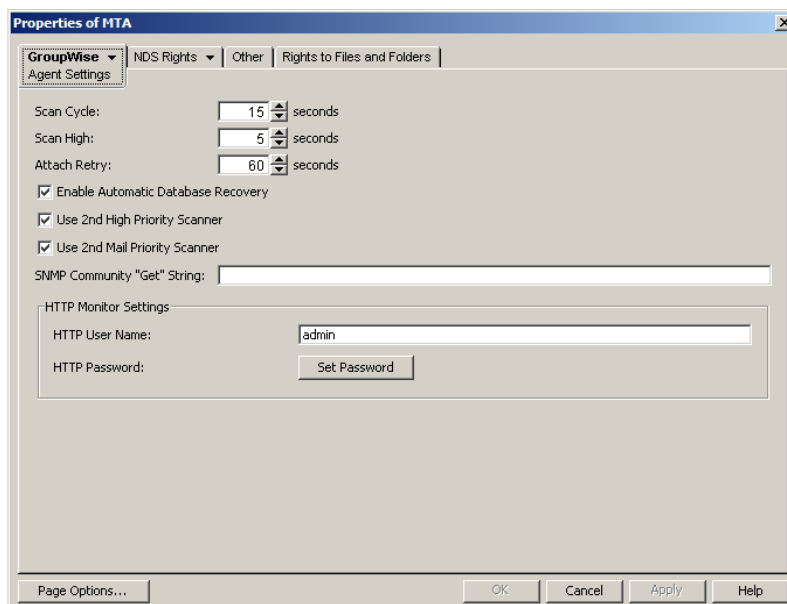
Set `--maxidlerouters` to a lower number if you want the MTA to terminate idle router threads more quickly. Set `--maxidlerouters` to a higher number if you want the MTA to keep more idle router threads ready to process incoming message traffic.

44.4 Adjusting MTA Polling of Closed Locations

When a location becomes closed (unavailable), the MTA waits before attempting to recontact that location. If the MTA waits only a short period of time, the MTA can waste time and create network traffic by trying to reestablish a connection with a closed location. On the other hand, you do not want the MTA to ignore an available location by waiting too long.

By default, the MTA waits 600 seconds (10 minutes) between its attempts to contact a closed location. You can adjust the time interval the MTA waits to meet the needs of your GroupWise system.

- 1 In ConsoleOne, browse to and right-click the MTA object, then click *Properties*.
- 2 Click *GroupWise > Agent Settings* to display the Agent Settings page.



- 3 Decrease the number of seconds in the *Attach Retry* field if you want the MTA to try to contact closed locations more often.

or

Increase the number of seconds in the *Attach Retry* field if you want the MTA to try to contact closed locations less often.

- 4 Click *OK* to save the new *Attach Retry* setting.

ConsoleOne then notifies the MTA to restart so the new setting can be put into effect.

For a TCP/IP link, a location is considered open if the MTA receives a response from the receiving agent within the currently configured wait intervals. See [Section 44.1.2, "Adjusting the MTA Wait Intervals for Slow TCP/IP Connections," on page 686](#). Otherwise, the location is considered closed.

For a mapped or UNC link, a location is considered open if the MTA can perform the following actions:

- ♦ Create a temporary directory in the MTA input queue (*domain\wpcsin* and *post_office\wpcsin* directories)
- ♦ Create a temporary file in that new directory
- ♦ Delete the temporary file
- ♦ Delete the temporary directory

For more information about the MTA input queues, see "[Message Transfer/Storage Directories](#)" in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*.

45 Using MTA Startup Switches

You can override settings provided in ConsoleOne by using startup switches in the MTA startup file. The default location for the startup file varies by platform.

Linux: `/opt/novell/groupwise/agents/share`

Windows: `c:\Program Files\Novell\GroupWise Server\Agents`

When you run the Agent Installation program, an initial MTA startup file is created. It is named using the first 8 characters of the domain name with a `.mta` extension. This initial startup file includes the `--home` startup switch set to the location of the domain directory.

When you update the MTA software, the existing MTA startup file can be retained or overwritten as needed.

Linux: When you use both the *Install* and *Configure* options in the Agent Installation program, the existing MTA startup file is backed up and then overwritten. When you use only the *Install* option, the existing MTA startup file is retained.

Windows: When you select *Install the software files, but do not configure the agents* in the Agent Installation program, the existing MTA startup file is retained. When you do not select this option, the existing MTA startup file is backed up and then overwritten.

Startup switches specified on the command line override those in the startup file. Startup switches in the startup file override corresponding settings in ConsoleOne. You can view the MTA startup file from the Configuration page of the MTA Web console.

The table below summarizes MTA startup switches for all platforms and how they correspond to configuration settings in ConsoleOne.

Switch starts with: `a b c d e f g h i j k l m n o p q r s t u v w x y z`

Linux MTA	Windows MTA	ConsoleOne Settings
<code>@file_name</code>	<code>@file_name</code>	N/A
<code>--activelog</code>	<code>/activelog</code>	N/A
<code>--certfile</code>	<code>/certfile</code>	<i>Certificate File</i>
<code>--cluster</code>	<code>/cluster</code>	N/A
<code>--cyhi</code>	<code>/cyhi</code>	<i>Scan High</i>
<code>--cylo</code>	<code>/cylo</code>	<i>Scan Cycle</i>
<code>--defaultroutingdomain</code>	<code>/defaultroutingdomain</code>	<i>Default Routing Domain</i>
<code>--fast0</code>	<code>/fast0</code>	<i>Use 2nd High Priority Scanner</i>

Linux MTA	Windows MTA	ConsoleOne Settings
--fast4	/fast4	<i>Use 2nd Mail Priority Scanner</i>
--help	/help	N/A
--home	/home	N/A
--httppassword	/httppassword	<i>HTTP Password</i>
--httpport	/httpport	<i>HTTP Port</i>
--httprefresh	/httprefresh	N/A
--httpssl	/httpssl	<i>HTTP</i>
--httpuser	/httpuser	<i>HTTP User Name</i>
--ip	/ip	<i>TCP/IP Address</i>
--keyfile	/keyfile	<i>SSL Key File</i>
--keypassword	/keypassword	<i>SSL Key File Password</i>
--language	/language	N/A
--log	/log	<i>Log File Path</i>
--logdays	/logdays	<i>Max Log File Age</i>
--logdiskoff	/logdiskoff	<i>Logging Level</i>
--loglevel	/loglevel	<i>Logging Level</i>
--logmax	/logmax	<i>Max Log Disk Space</i>
--maxidlerouters	/maxidlerouters	N/A
--maxrouters	/maxrouters	N/A
--messagelogdays	/messagelogdays	<i>Delete Reports After</i>
--messagelogmaxsize	/messagelogmaxsize	N/A
--messagelogpath	/messagelogpath	<i>Message Log File Path</i>
--messagelogsettings	/messagelogsettings	<i>Message Logging Level</i>
--msgtranssl	/msgtranssl	<i>Message Transfer SSL</i>
--noada	/noada	N/A
--nodns	/nodns	N/A
--noerrormail	/noerrormail	N/A
--nondssync	/nondssync	N/A
--norecover	/norecover	N/A
--nosnmp	/nosnmp	N/A
--show	N/A	N/A
--tcpinbound	/tcpinbound	N/A
--tcpport	/tcpport	<i>Network Address</i>

Linux MTA	Windows MTA	ConsoleOne Settings
<code>--tcpwaitconnect</code>	<code>/tcpwaitconnect</code>	N/A
<code>--tcpwaitdata</code>	<code>/tcpwaitdata</code>	N/A
<code>--vsnoadm</code>	<code>/vsnoadm</code>	N/A
<code>--work</code>	<code>/work</code>	N/A

45.1 @file_name

Specifies the location of the MTA startup file. On Linux, the startup file always resides in the `/opt/novell/groupwise/agents/share` directory. On Windows, the full path must be included if the file does not reside in the same directory with the MTA program. The startup file must reside on the same server where the MTA is installed.

Linux MTA	Windows MTA
Syntax: <code>@[/dir]file</code>	<code>@[drive:][\dir\]file</code>
Example: <code>./gwmata @../share/lnxdom.mta</code>	<code>gwmata.exe @provo2.mta</code> <code>gwmata.exe @d:\agt\provo2.mta</code>

45.2 --activelog

Displays the active log window rather than the alert box when the MTA starts. See [Section 43.1.1, “Monitoring the MTA from the MTA Server Console,”](#) on page 659.

Linux MTA	Windows MTA
Syntax: <code>--activelog</code>	<code>/activelog</code>

45.3 --certfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the MTA and other programs. See [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,”](#) on page 643.

Linux MTA	Windows MTA
Syntax: <code>--certfile-/dir/file</code>	<code>/certfile-[drive:]\dir\file</code> <code>/certfile-\\svr\sharename\dir\file</code>
Example: <code>--certfile /certs/gw.crt</code>	<code>/certfile-\\ssl\gw.crt</code> <code>/certfile-m:ssl\gw.crt</code> <code>/certfile-\\server2\c\ssl\gw.crt</code>

See also `--keyfile` and `--keypassword`.

45.4 --cluster

Informs the MTA that it is running in a cluster. A clustered MTA automatically binds to the IP address configured for the MTA object even if the *Bind Exclusively to TCP/IP Address* option is not selected on the MTA Network Address page in ConsoleOne. This prevents unintended connections to other IP addresses, such as the loopback address or the node's physical IP address. For information about clustering the MTA, see the [GroupWise 2012 Interoperability Guide](#).

	Linux MTA	Windows MTA
Syntax:	--cluster	/cluster

See also [/ip](#).

45.5 --cyhi

Sets the number of seconds in the scan cycle that the MTA uses to scan its priority 0-1 input queues. The default is 5 seconds. See [Section 44.2.2, "Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways,"](#) on page 686.

	Linux MTA	Windows MTA
Syntax:	--cyhi-seconds	/cyhi-seconds
Example:	--cyhi 3	/cyhi-3

See also [--cylo](#).

45.6 --cylo

Sets the number of seconds in the scan cycle that the MTA uses to scan its priority 2-7 input queues. The default is 15 seconds. See [Section 44.2.2, "Adjusting MTA Polling of Input Queues in the Domain, Post Offices, and Gateways,"](#) on page 686.

	Linux MTA	Windows MTA
Syntax:	--cylo-seconds	/cylo-seconds
Example:	--cylo 10	/cylo-10

See also [--cyhi](#).

45.7 --defaultroutingdomain

Identifies the domain name in your GroupWise system to which all MTAs should send messages when they cannot resolve the available routing information to a specific *user.post_office.domain* GroupWise address. See [Section 42.3.1, “Using Routing Domains,”](#) on page 645.

	Linux MTA	Windows MTA
Syntax:	--defaultroutingdomain <i>domain</i>	/defaultroutingdomain- <i>domain</i>
Example:	--defaultroutingdomain inethub	/defaultroutingdomain-inethub

45.8 --fast0

Causes the MTA to monitor and process the priority 0 and 1 subdirectories independently with separate scanner threads, rather than in sequence with the same scanner thread. See [Section 44.2.3, “Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices,”](#) on page 688.

	Linux MTA	Windows MTA
Syntax:	--fast0	/fast0

See also [--fast4](#).

45.9 --fast4

Causes the MTA to monitor and process the priority 2 and 3 subdirectories with a separate scanner thread from the priority 4 through 7 subdirectories. See [Section 44.2.3, “Adjusting the Number of MTA Scanner Threads for the Domain and Post Offices,”](#) on page 688.

	Linux MTA	Windows MTA
Syntax:	--fast4	/fast4

See also [--fast0](#).

45.10 --help

Displays the MTA startup switch Help information. When this switch is used, the MTA does not start.

	Linux MTA	Windows MTA
Syntax:	--help or --?	/help or /?
Example:	./gwmta --help	gwmta.exe /help

45.11 --home

Specifies the domain directory, where the MTA can access the domain database ([wpsdomain.db](#)). There is no default location. You must use this switch in order to start the MTA

	Linux MTA	Windows MTA
Syntax:	<code>--home /dir</code>	<code>/home-[drive:]\dir</code> <code>/home-\\svl\sharename\dir</code>
Example:	<code>--home /gwsystem/provo2</code>	<code>/home-\provo2</code> <code>/home-m:\provo2</code> <code>home-\\server2\c\mail\provo2</code>

If you specify a UNC path with the `--home` switch when you run the MTA as a Windows service, you must configure the MTA service to run under a specific Windows user account. If you specify a local directory or a mapped drive, you can configure the MTA service to run under the local system account. However, running under the Administrator account is highly recommended.

45.12 --httppassword

Specifies the password for the MTA to prompt for before allowing MTA status information to be displayed in your Web browser. Do not use an existing eDirectory password because the information passes over the non-secure connection between your Web browser and the MTA. See [Section 43.2, "Using the MTA Web Console,"](#) on page 669.

	Linux MTA	Windows MTA
Syntax:	<code>--httppassword <i>unique_password</i></code>	<code>/httppassword-<i>unique_password</i></code>
Example:	<code>--httppassword AgentWatch</code>	<code>/httppassword-AgentWatch</code>

See also [/httpuser](#), [/httpport](#), [/httprefresh](#), and [/httpsl](#).

45.13 --httpport

Sets the HTTP port number used for the MTA to communicate with your Web browser. The default is 7180; the setting must be unique. See [Section 43.2, "Using the MTA Web Console,"](#) on page 669.

	Linux MTA	Windows MTA
Syntax:	<code>--httpport <i>port_number</i></code>	<code>/httpport-<i>port_number</i></code>
Example:	<code>--httpport 3802</code>	<code>/httpport-3803</code>

See also `--httpuser`, `--httppassword`, `--httprefresh`, and `--httpsl`.

45.14 --httprefresh

Specifies the rate at which the MTA refreshes the status information in your Web browser. The default is 60 seconds. See [Section 43.2, “Using the MTA Web Console,”](#) on page 669.

	Linux MTA	Windows MTA
Syntax:	--httprefresh <i>seconds</i>	/httprefresh- <i>seconds</i>
Example:	--httprefresh 90	/httprefresh-120

See also [--httpuser](#), [--httppassword](#), [--httpport](#), and [--https](#).

45.15 --https

Enables secure SSL communication between the MTA and the MTA Web console displayed in your Web browser. See [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,”](#) on page 643.

	Linux MTA	Windows MTA
Syntax:	--https	/https

See also [--certfile](#), [--keyfile](#), and [--keypassword](#).

45.16 --httpuser

Specifies the user name for the MTA to prompt for before allowing MTA status information to be displayed in your Web browser. Providing a user name is optional. Do not use an existing eDirectory user name because the information passes over the non-secure connection between your Web browser and the MTA. See [Section 43.2, “Using the MTA Web Console,”](#) on page 669.

	Linux MTA	Windows MTA
Syntax:	--httpuser <i>unique_name</i>	/httpuser- <i>unique_name</i>
Example:	--httpuser GWWebCon	/httpuser-GWWebCon

See also [--httppassword](#), [--httpport](#), and [--httprefresh](#).

45.17 --ip

Binds the MTA to a specific IP address when the server where it runs uses multiple IP addresses. The specified IP address is associated with both ports used by the MTA (message transfer and HTTP). Without the `--ip` switch, the MTA binds to all available IP addresses. See [Section 42.1.5, “Binding the MTA to a Specific IP Address,” on page 639](#).

	Linux MTA	Windows MTA
Syntax:	<code>--ip IP_address</code> <code>--ip "full_DNS_name"</code>	<code>/ip-IP_address</code> <code>/ip-"full_DNS_name"</code>
Example:	<code>--ip 172.16.5.18</code> <code>--ip "mtasvr.provo.novell.com"</code>	<code>/ip-172.16.5.18</code> <code>/ip-"mtasvr.provo.novell.com"</code>

45.18 --keyfile

Specifies the full path to the private file used to provide secure SSL communication between the MTA and other programs. See [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,” on page 643](#).

	Linux MTA	Windows MTA
Syntax:	<code>--keyfile /dir/file</code>	<code>/keyfile-[drive:]\dir\file</code> <code>/keyfile-\\svr\sharename\dir\file</code>
Example:	<code>--keyfile /ssl/gw.key</code>	<code>/keyfile-ssl\gw.key</code> <code>/keyfile-m:\ssl\gw.key</code> <code>/keyfile-\\server2\c\ssl\gw.key</code>

See also [--certfile](#) and [--keypassword](#).

45.19 --keypassword

Specifies the password used to encrypt the private SSL key file when it was created. See [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,” on page 643](#).

	Linux MTA	Windows MTA
Syntax:	<code>--keypassword password</code>	<code>/keypassword-password</code>
Example:	<code>--keypassword gwssl</code>	<code>/keypassword-gwssl</code>

See also [--certfile](#) and [--keyfile](#).

45.20 --language

Specifies the language to run the MTA in, using a two-letter language code as listed below. You must install the MTA in the selected language in order for the MTA to display in the selected language.

The initial default is the language used in the domain. If that language has not been installed, the next default is the language used by the operating system. If that language has not been installed, the final default is English. You only need to use this switch if you need to override these defaults.

	Linux MTA	Windows MTA
Syntax:	<code>--language code</code>	<code>/language-code</code>
Example:	<code>--language de</code>	<code>/language-fr</code>

Contact your local Novell sales office for information about language availability.

See [Chapter 7, “Multilingual GroupWise Systems,”](#) on page 123 for a list of language codes.

45.21 --log

Specifies the directory where the MTA will store its log files. The default location varies by platform.

Linux: `/var/log/novell/groupwise/domain_name.mta`

Windows: `mslocal` subdirectory in the directory specified by the `--work` switch

For more information, see [Section 43.3, “Using MTA Log Files,”](#) on page 677.

	Linux MTA	Windows MTA
Syntax:	<code>--log /dir</code>	<code>/log-[drive:]\dir</code> <code>/log-\\sv\sharename\dir</code>
Example:	<code>--log /gwsystem/logs</code>	<code>/log-\agt\log</code> <code>/log-m:\agt\log</code> <code>/log-\\server2\c\mail\agt\log</code>

You typically find multiple log files in the specified directory. The first four characters represent the date. The next three characters identify the agent. A three-digit extension allows for multiple log files created on the same day. For example, a log file named `0518mta.001` indicates that it is an MTA log file, created on May 18. If you restarted the MTA on the same day, a new log file is started, named `0518mta.002`.

See also `--loglevel`, `--logdiskoff`, `--logdays`, and `--logmax`.

45.22 --logdays

Sets the number of days you want MTA log files to remain on disk before being automatically deleted. The default log file age is 30 days. See [Section 43.3, “Using MTA Log Files,” on page 677](#).

	Linux MTA	Windows MTA
Syntax:	--logdays <i>days</i>	/logdays- <i>days</i>
Example:	--logdays 45	/logdays-60

See also [--log](#), [--loglevel](#), [--logdiskoff](#), and [--logmax](#).

45.23 --logdiskoff

Turns off disk logging for the MTA so no information about the functioning of the MTA is stored on disk. The default is for logging to be turned on. See [Section 43.3, “Using MTA Log Files,” on page 677](#).

	Linux MTA	Windows MTA
Syntax:	--logdiskoff	/logdiskoff

See also [--loglevel](#).

45.24 --loglevel

Controls the amount of information logged by the MTA. Logged information is displayed in the log message box and written to the MTA log file during the current agent session. The default is Normal, which displays only the essential information suitable for a smoothly running MTA. Use Verbose to display the essential information, plus additional information helpful for troubleshooting. Verbose logging does not degrade MTA performance, but log files saved to disk consume more disk space when verbose logging is in use. See [Section 43.3, “Using MTA Log Files,” on page 677](#).

	Linux MTA	Windows MTA
Syntax:	--loglevel <i>level</i>	/loglevel- <i>level</i>
Example:	--loglevel verbose	/loglevel-verbose

See also [--log](#), [--logdiskoff](#), [--logdays](#), and [--logmax](#).

45.25 --logmax

Sets the maximum amount of disk space for all MTA log files. When the specified disk space is consumed, the MTA deletes existing log files, starting with the oldest. The default is 102400 KB (100 MB) of disk space for all MTA log files. The maximum allowable setting is 102400000 (1 GB). Specify 0 (zero) for unlimited disk space. See [Section 43.3, “Using MTA Log Files,”](#) on page 677.

	Linux MTA	Windows MTA
Syntax:	--logmax <i>kilobytes</i>	/logmax- <i>kilobytes</i>
Example:	--logmax 130000	/logmax-160000

See also [--log](#), [--loglevel](#), [--logdiskoff](#), and [--logdays](#).

45.26 --maxidlerouters

Specifies the maximum number of idle router threads the MTA can keep running. The default is 16; valid values range from 1 to 16. See [Section 44.3, “Optimizing the Routing Queue,”](#) on page 689.

	Linux MTA	Windows MTA
Syntax:	--maxidlerouters <i>threads</i>	/maxidlerouters- <i>threads</i>
Example:	--maxidlerouters 10	/maxidlerouters-12

See also [--maxrouters](#).

45.27 --maxrouters

Specifies the maximum number of router threads the MTA can start. The default is 16; valid values range from 1 to 16. See [Section 44.3, “Optimizing the Routing Queue,”](#) on page 689.

	Linux MTA	Windows MTA
Syntax:	--maxrouters <i>threads</i>	/maxrouters- <i>threads</i>
Example:	--maxrouters 12	/maxrouters-14

See also [--maxidlerouters](#).

45.28 --messagelogdays

Sets the number of days you want MTA message log files to remain on disk before being automatically deleted. The default is 30 days. See [Section 42.4.2, “Enabling MTA Message Logging,”](#) on page 657.

	Linux MTA	Windows MTA
Syntax:	--messagelogdays <i>days</i>	/messagelogdays- <i>days</i>

Linux MTA	Windows MTA
Example: --messagelogdays 45	/messagelogdays-60

See also [--messagelogsettings](#), [--messagelogpath](#), and [--messagelogmaxsize](#).

45.29 --messagelogmaxsize

Sets the maximum size for MTA message log files. The default is 102400 KB (100 MB). The maximum allowable setting is 102400000 (1 GB). See [Section 42.4.2, “Enabling MTA Message Logging,” on page 657](#).

Linux MTA	Windows MTA
Syntax: --messagelogmaxsize <i>kilobytes</i>	/messagelogmaxsize- <i>kilobytes</i>
Example: --messagelogmaxsize 130000	/messagelogmaxsize-160000

See also [--messagelogsettings](#), [--messagelogpath](#), and [--messagelogdays](#).

45.30 --messagelogpath

Specifies the directory for the MTA message log. The default location is `mlocal\msglog`. See [Section 42.4.2, “Enabling MTA Message Logging,” on page 657](#).

Linux MTA	Windows MTA
Syntax: --messagelogpath <i>/dir</i>	/messagelogpath- <i>[drive:]dir</i> /messagelogpath- <i>\\svr\sharename\dir</i>
Example: --messagelogpath /gwsys/logs	/messagelogpath-mta\log /messagelogpath-m:\mta\log /messagelogpath-\\svr2\c\mail\mta\log

See also [--messagelogsettings](#), [--messagelogdays](#), and [--messagelogmaxsize](#).

45.31 --messagelogsettings

Enables MTA message logging. See [Section 42.4.2, “Enabling MTA Message Logging,” on page 657](#).

Linux MTA	Windows MTA
Syntax: --messagelogsettings <i>codes</i>	/messagelogsettings- <i>codes</i>
Example: --messagelogsettings e	/messagelogsettings-e

See also [--messagelogpath](#), [--messagelogdays](#), and [--messagelogmaxsize](#).

45.32 --msgtranssl

Enables secure SSL communication between the MTA and the POAs in its domain. See [Section 42.2.2, “Securing the Domain with SSL Connections to the MTA,”](#) on page 643.

	Linux MTA	Windows MTA
Syntax:	--msgtranssl	/msgtranssl

See also [--certfile](#), [--keyfile](#), and [--keypassword](#).

45.33 --noada

Disables the MTA admin thread. For an explanation of the MTA admin thread, see [“MTA Admin Thread Status Box”](#) on page 662.

	Linux MTA	Windows MTA
Syntax:	--noada	/noada

Historical Note: In GroupWise 5.2 and earlier, a separate agent, the Administration Agent (ADA), handled the functions now consolidated into the MTA admin thread. Hence the switch name, --noada.

45.34 --nodns

Disables DNS lookups for the MTA. See [“Using Dynamic Internet Links”](#) in [“Connecting to Other GroupWise Systems”](#) in the *GroupWise 2012 Multi-System Administration Guide*.

	Linux MTA	Windows MTA
Syntax:	--nodns	/nodns

45.35 --noerrormail

Prevents error files from being sent to the GroupWise administrator. The default is for error mail to be sent to the administrator. See [Section 43.7, “Notifying the Domain Administrator,”](#) on page 682.

	Linux MTA	Windows MTA
Syntax:	--noerrormail	/noerrormail

45.36 --nondssync

Disables eDirectory user synchronization. See [Section 42.4.1, “Using eDirectory User Synchronization,”](#) on page 652.

	Linux MTA	Windows MTA
Syntax:	--nondssync	N/A

45.37 --norecover

Disables automatic database recovery. The default is for automatic database recovery to be turned on. If the MTA detects a problem with the domain database (`wppdomain.db`) when automatic database recovery has been turned off, the MTA notifies the administrator, but it does not recover the problem database. See [Chapter 26, “Maintaining Domain and Post Office Databases,”](#) on page 401.

	Linux MTA	Windows MTA
Syntax:	--norecover	/norecover

45.38 --nosnmp

Disables SNMP for the MTA. The default is to have SNMP enabled. See [Section 43.6, “Using an SNMP Management Console,”](#) on page 679.

	Linux MTA	Windows MTA
Syntax:	--nosnmp	/nosnmp

45.39 --show

Starts the Linux MTA with a server console interface similar to that provided for the Windows MTAs. This user interface requires that the X Window System and Open Motif are running on the Linux server.

	Linux MTA	Windows MTA
Syntax:	--show	N/A

The `--show` switch cannot be used in the MTA startup file. However, if you want the MTA to start with a user interface when you run the `grpwise` script or when the server reboots, you can configure the GroupWise High Availability service (`gwaha`) to accomplish this, as described in [“Configuring the GroupWise High Availability Service in the gwaha.conf File”](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.

45.40 --tcpinbound

Sets the maximum number of inbound TCP/IP connections for the MTA from POAs and GWIAs belonging to the domain and from MTAs and GWIAs in other domains in your GroupWise system. The default is 40. There is no maximum number of outbound connections. The only limit on the MTA for outbound connections is available resources. See [Section 44.1.1, “Adjusting the Number of MTA TCP/IP Connections,”](#) on page 685.

	Linux MTA	Windows MTA
Syntax:	--tcpinbound <i>number</i>	/tcpinbound- <i>number</i>
Example:	--tcpinbound 60	/tcpinbound-70

45.41 --tcpport

Sets the TCP port number on which the MTA listens for incoming messages from other MTAs, POAs, and GWIAs. The default is 7100. See [“Using TCP/IP Links between Domains”](#) on page 632.

	Linux MTA	Windows MTA
Syntax:	--tcpport <i>port_number</i>	/tcpport- <i>port_number</i>
Example:	--tcpport 7200	/tcpport-7200

45.42 --tcpwaitconnect

Sets the maximum number of seconds the MTA waits for a connection to another MTA. The default is 5. See [Section 44.1.2, “Adjusting the MTA Wait Intervals for Slow TCP/IP Connections,”](#) on page 686.

	Linux MTA	Windows MTA
Syntax:	--tcpwaitconnect <i>seconds</i>	/tcpwaitconnect- <i>seconds</i>
Example:	--tcpwaitconnect 10	/tcpwaitconnect-10

See also [--tcpwaitdata](#).

45.43 --tcpwaitdata

Sets the maximum number of seconds the MTA attempts to send data over a TCP/IP connection to another MTA. The default is 20. See [Section 44.1.2, “Adjusting the MTA Wait Intervals for Slow TCP/IP Connections,”](#) on page 686.

	Linux MTA	Windows MTA
Syntax:	--tcpwaitdata <i>seconds</i>	/tcpwaitdata- <i>seconds</i>
Example:	--tcpwaitdata 30	/tcpwaitdata-30

See also [--tcpwaitconnect](#).

45.44 --vsnoadm

Prevents GroupWise administration messages from being processed by an integrated virus scanner. Because administration messages are created within your GroupWise system, they are not likely to contain viruses. In a GroupWise system with a large amount of administrative activity (adding users, deleting users, etc.), skipping the virus scanning of administrative messages can speed up processing of users' email messages.

	Linux MTA	Windows MTA
Syntax:	--vsnoadm	/vsnoadm

45.45 --work

Specifies the directory where the MTA creates its local working directory (`mslocal`). The default is the domain directory. However, if the domain is located on a different server from where the MTA will run, use a local directory so the MTA cannot lose its connection to its `mslocal` directory.

	Linux MTA	Windows MTA
Syntax:	--work <i>/dir</i>	<i>/work-[drive:]\dir</i> <i>/work-\\sv\sharename\dir</i>
Example:	--work /gwmata	<i>/work-gwmata</i> <i>/work-m:\gwmata</i> <i>/work-\\server2\c\mail\gwmata</i>

XI Document Viewer Agent

- ♦ Chapter 46, “Understanding Document Conversion,” on page 711
- ♦ Chapter 47, “Scaling Your DVA Installation,” on page 713
- ♦ Chapter 48, “Configuring the DVA,” on page 719
- ♦ Chapter 49, “Monitoring the DVA,” on page 725
- ♦ Chapter 50, “Optimizing the DVA,” on page 729
- ♦ Chapter 51, “Using Document Viewer Agent Startup Switches,” on page 731

For port number information, see [Section A.5, “Document Viewer Agent Port Numbers,”](#) on page 1170.

For detailed Linux-specific DVA information, see [Appendix C, “Linux Commands, Directories, and Files for GroupWise Administration,”](#) on page 1179.

For additional assistance in managing the DVA, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

46 Understanding Document Conversion

The document files that users attach to email messages are as varied as the combinations of document formats, tools, and users throughout the world. The Document Viewer Agent (DVA), which is automatically installed along with the POA and the MTA, accommodates multiple attachment formats by converting GroupWise attachments into HTML format. For a list of the file types that the DVA can convert, see *Oracle Outside In Technology Supported Formats* (<http://www.oracle.com/technetwork/middleware/content-management/ds-oitfiles-133032.pdf>).

Two GroupWise components rely on document conversion for their functionality:

- ♦ **GroupWise WebAccess:** When GroupWise users access their mailboxes through GroupWise WebAccess, they expect to view attached documents in their Web browser, regardless of the file format of the attached file. For WebAccess users, the DVA converts attached document files into HTML so that the attachments can be viewed along with the email messages or other GroupWise items to which the documents are attached.
- ♦ **Post Office Agent:** When GroupWise users access their mailboxes in any manner and use the Find feature to search for text, they expect to locate the text in attached documents as well as in email messages and other GroupWise items. For all GroupWise users, the DVA converts attached document files into HTML, so that attachments can be indexed by the POA.

IMPORTANT: By default, the POA uses the Document Converter Agent (DCA) to convert documents into HTML format for indexing. The DCA is an internal POA process and is not as scalable as the DVA. You must manually configure the POA to use the DVA instead of the default DCA, as described in [Section 39.3, “Enabling the Document Viewer Agent \(DVA\) for Indexing,”](#) on page 576.

The DVA can simultaneously convert multiple document files into HTML format.

Because some document files contain unexpected data, they cannot be successfully converted into HTML format for viewing in GroupWise WebAccess and for indexing by the POA. The DVA isolates the document conversion task from other GroupWise activities. If the DVA encounters a problem converting a particular document file, the problem does not affect conversion of other document files, nor does it affect the user experience in GroupWise, except that the problem document cannot be viewed in WebAccess and cannot be located using the Find feature.

47 Scaling Your DVA Installation

If your GroupWise system is relatively small (one domain and a few post offices), a basic installation of one DVA along with each POA might meet your needs. However, if your GroupWise system is large or requires failover support, you can scale your DVA installation to better meet the reliability, performance, and availability needs of your GroupWise users.

- ♦ [Section 47.1, “DVA Configurations,” on page 713](#)
- ♦ [Section 47.2, “DVA Installation on Additional Servers,” on page 715](#)

47.1 DVA Configurations

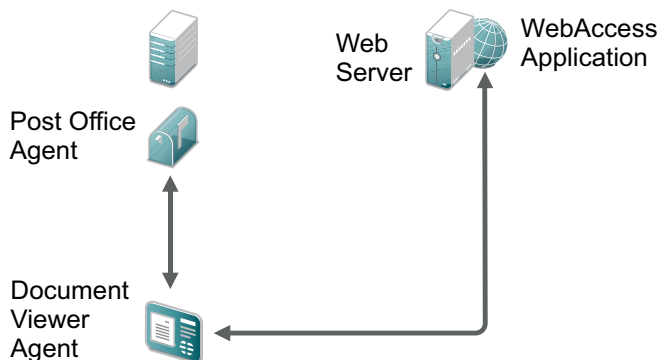
Depending on the needs of your GroupWise system, it might be necessary for you to have multiple DVAs running to service WebAccess Applications and POAs.

- ♦ [Section 47.1.1, “Basic DVA Installation,” on page 713](#)
- ♦ [Section 47.1.2, “Multiple DVAs for WebAccess,” on page 714](#)
- ♦ [Section 47.1.3, “Multiple DVAs for a Post Office,” on page 714](#)
- ♦ [Section 47.1.4, “Multiple Shared DVAs,” on page 715](#)

47.1.1 Basic DVA Installation

By default, the DVA is installed along with each POA that you install and is configured to communicate with that specific POA.

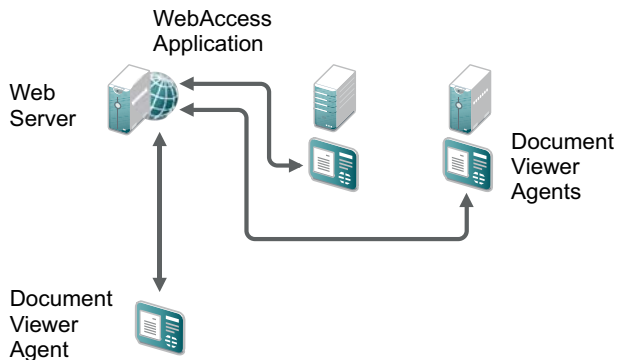
When you install WebAccess on a Web server, you configure the WebAccess Application to communicate with one DVA.



Depending on the needs for attachment viewing in GroupWise WebAccess and for attachment indexing for all users, it might be necessary for you to add additional DVAs to your system. Although the DVA software is installed along with the POA and MTA software, you can install the agent software on any server and run the DVA without running the other agents on that server. For instructions, see [Section 47.2, “DVA Installation on Additional Servers,”](#) on page 715.

47.1.2 Multiple DVAs for WebAccess

If GroupWise WebAccess users display a large number of attached documents, you can install and configure multiple DVA to service the WebAccess Application so that attached documents can be displayed more promptly.

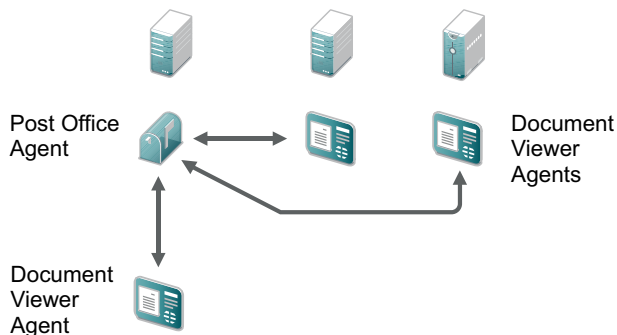


For more information about this configuration, see [Section 62.1.3, “Configuring Multiple DVAs for the WebAccess Application,”](#) on page 905.

47.1.3 Multiple DVAs for a Post Office

One DVA might provide sufficient indexing performance for the POA, but you might want to protect against downtime that would occur if the DVA became unavailable because of server failure or some other reason. Installing more than one DVA enables you to set up failover support to make document conversion and indexing more reliable.

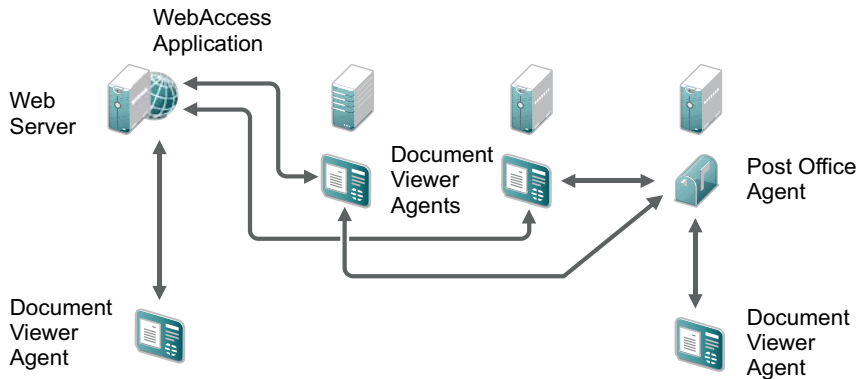
If you have a post office with a heavy load of attachment indexing, you can install and configure multiple DVAs to service the POA for that post office.



For more information about this configuration, see [Section 39.3, “Enabling the Document Viewer Agent \(DVA\) for Indexing,”](#) on page 576.

47.1.4 Multiple Shared DVAs

When you install multiple DVAs, they can be accessed by both WebAccess Applications and POAs if that works well for your GroupWise system configuration.



47.2 DVA Installation on Additional Servers

The following sections assume that you are already running the DVA that was installed along with the POA for a post office, and that you want to install additional DVAs to run independently on other servers for use by the WebAccess Application and /or the POA. When the WebAccess Application needs additional DVAs, you might want to install one on the Web server itself.

IMPORTANT: Make sure that the servers where you install the DVA meet the system requirements listed in [“Agent System Requirements”](#).

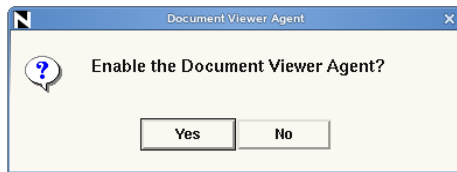
- [Section 47.2.1, “Linux: Installing Additional DVAs,” on page 715](#)
- [Section 47.2.2, “Windows: Installing Additional DVAs,” on page 716](#)

47.2.1 Linux: Installing Additional DVAs

- 1 In a terminal window on the server where you want to install the DVA, log in as `root`, then provide the `root` password.
- 2 Change to the root directory of the downloaded *GroupWise 2012* software image.
or
If you have already copied the agent software to a software distribution directory, change to `/opt/novell/groupwise/software`.
- 3 Run `./install`.
- 4 Select the language in which you want to run the GroupWise Installation program, then click *OK*.
- 5 On the main GroupWise System Installation page, click *Install Products > GroupWise Agents > Install Agents* to install the GroupWise agent software, including the DVA
- 6 When the installation is complete, click *OK*.
The GroupWise agent software, including the DVA, is installed to the following directory:
`/opt/novell/groupwise/agents`
- 7 Click *Configure GroupWise Agents*, then click *Next*.

- 8 Accept the License Agreement, then click *Next*.
- 9 On the Domains/Post Offices page, click *Next*.

By not specifying any domains or post offices, you keep the MTA and the POA from being configured to run on this server.



- 10 In the Document Viewer Agent dialog box, click *Yes* to configure the DVA for high availability. For more information, see [“Enabling the GroupWise High Availability Service for the Linux GroupWise Agents”](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.
or
Click *No* if you do not want to configure the DVA for high availability.
- 11 (Conditional) If you do not want the DVA to start automatically when the server restarts, deselect *Launch GroupWise Agents on System Startup*.
- 12 Click *Exit* to exit the GroupWise Agent Installation program.
- 13 Exit the GroupWise Installation program.
- 14 Use the following commands to manually manage the DVA on the Linux server:

```
rcgrpwise start gwdva
rcgrpwise stop gwdva
rcgrpwise status gwdva
rcgrpwise print gwdva
```

or

Use the following command to start the Linux DVA:

```
/opt/novell/groupwise/agents/bin/gwdva @gwdva.dva
```

When you use this command to start the DVA, you must use the `kill` command to stop it, as described in [Stopping the Linux GroupWise Agents as Daemons](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.

NOTE: Currently, the DVA must run as `root`. It cannot be configured to run as a non-root user as the other GroupWise agents can.

- 15 To configure the DVA, see [Chapter 48, “Configuring the DVA,”](#) on page 719.
- 16 To monitor the DVA, see [Chapter 49, “Monitoring the DVA,”](#) on page 725.

47.2.2 Windows: Installing Additional DVAs

- 1 Change to the root directory of the downloaded *GroupWise 2012* software image.
or
(Conditional) If you have already copied the agent software to a software distribution directory, change to that location
- 2 Run `setup.exe`.
- 3 (Conditional) If prompted, select the interface language for the Installation program, then click *OK*.

- 4 On the main GroupWise System Installation page, click *Install GroupWise System*, then click *Yes* to accept the License Agreement and display the Installation Type page.

When you install the agents, you are performing a Standard installation.

- 5 Click *Next* to accept the default of *Standard*.
- 6 Select *Install Individual Components*, deselect *GroupWise Administration*, then click *Next*.
- 7 On the Installation Path page, select *Install the software files, but do not configure the agents*, then click *Next*.

When you install the DVA along with the MTA and the POA, the agents are installed as Windows services by default. When you install the DVA independently, you must select *Install the software files, but do not configure the agents* in order to skip the Domains/Post Offices page where the MTA and POA are configured. This deselects *Install as Windows services*, so when you install the DVA independently, you must install it as a Windows application.

- 8 On the Summary and Modification page, click *Install*.

The GroupWise agents are installed to the following directory:

`c:\Program Files\Novell\GroupWise Server\Agents`

Because you did not configure the MTA and the POA, they do not run on the server, even though the agent software was installed.

- 9 Click *Finish* to exit the Agent Installation program.
- 10 Click the Windows *Start* menu > *All Programs* > *Novell GroupWise Agents* > *GWDVA*.
The DVA server console opens on the Windows desktop.
- 11 To monitor the DVA in your Web browser, see [Section 49.2, "Using the DVA Web Console," on page 725](#).
- 12 To configure the DVA, see [Chapter 48, "Configuring the DVA," on page 719](#).

48 Configuring the DVA

The DVA is automatically installed along with the POA and the MTA. The default configuration of the DVA is sufficient to provide basic document conversion functionality. The DVA is configured by editing its startup file (`gwdva.dva`).

- ◆ [Section 48.1, “Editing the `gwdva.dva` File,” on page 719](#)
- ◆ [Section 48.2, “Performing Basic DVA Configuration,” on page 719](#)
- ◆ [Section 48.3, “Enabling the DVA Document Quarantine,” on page 722](#)
- ◆ [Section 48.4, “Putting DVA Configuration Changes into Effect,” on page 722](#)

48.1 Editing the `gwdva.dva` File

The location of the `gwdva.dva` file varies by platform:

Linux: `/opt/novell/groupwise/agents/share`

Windows: `c:\Program Files\Novell\GroupWise Server\Agents`

You can use any ASCII text editor that you prefer to edit the `gwdva.dva` file.

IMPORTANT: When you update the DVA software, a new `gwdva.dva` file is installed. The existing `gwdva.dva` file is retained as `gwdva.nnn`, where `nnn` increments each time you update the DVA software.

48.2 Performing Basic DVA Configuration

- ◆ [Section 48.2.1, “Setting the DVA Home Directory,” on page 719](#)
- ◆ [Section 48.2.2, “Changing the DVA IP Address or Port Number,” on page 720](#)
- ◆ [Section 48.2.3, “Securing Document Conversion with SSL Connections,” on page 721](#)

48.2.1 Setting the DVA Home Directory

By default, the DVA creates its working directory named `gwdva.dir` under the directory where the DVA is installed. The location varies by platform:

Linux: `/opt/novell/groupwise/agents/bin/gwdva.dir`

Windows: `c:\Program Files\Novell\GroupWise Server\Agents\gwdva.dir`

The DVA working directory has four subdirectories (log, quarantine, temp, and template). If this directory consumes more disk space than you want consumed in a software subdirectory, you can move it to a different location on the local server or to a location on a remote server.

- 1 Open the [gwdva.dva file](#) in a text editor.
- 2 Search to find the following switch:

/home
- 3 Remove the semicolon (;) to activate the setting.
- 4 Specify the full path name for the DVA working directory., for example:

```
Linux:      /opt/novell/groupwise/gwdva
Windows:   c:\Program Files\Novell\GroupWise Server\gwdva
           m:\gwsystem\gwdva
           \\gwserver5\c\gwsystem\gwdva
```

On Windows, if you are running the DVA as a Windows service rather than as an application, the format you use for the path name influences the Windows user account that the DVA service can run under. If you specify a home directory on the local server or on a mapped drive, the DVA service can run under the local system account. If you specify a home directory as a UNC path to a remote server, the DVA service must run as a Windows user that has rights to access the remote home directory.

IMPORTANT: For simplicity of DVA administration, running the DVA as the Windows Administrator user is highly recommended.

- 5 (Optional) Use the `--log`, `--temp`, and `--template` switches to move these subdirectories out from under the DVA working directory. The quarantine directory cannot be moved.
- 6 Save the `gwdva.dva` file.
- 7 Skip to [Section 48.4, "Putting DVA Configuration Changes into Effect,"](#) on page 722.

48.2.2 Changing the DVA IP Address or Port Number

The DVA communicates with the other programs (the WebAccess Application, the POA, and the DVA Web console) by way of HTTP. By default, the DVA uses the first IP address it finds on the server and listens on port 8301.

- 1 Open the [gwdva.dva file](#) in a text editor.
- 2 Change the IP address:
 - 2a Search to find the following switch:

/ip
 - 2b Remove the semicolon (;) to activate the setting.
 - 2c Specify the IP address that you want the DVA to use.
- 3 Change the port number:
 - 3a Search to find the following switch:

/httpport
 - 3b Remove the semicolon (;) to activate the setting.

- 3c Specify the port number that you want the DVA to use.

Worker threads are assigned port numbers ascending above the main port number. For example, if you decide to use a main port number of 8500, the 5 default worker threads would be assigned ports 8501 through 8505. You must make sure that none of these incremental port numbers are already in use on the server, up to the largest possible number of DVA threads that could be started. For more information, see [Section 50.1, “Controlling Thread Usage,”](#) on page 729.

- 4 Save the `gwdva.dva` file.
- 5 Skip to [Section 48.4, “Putting DVA Configuration Changes into Effect,”](#) on page 722.

For information about how the DVA interacts with other programs, see:

- ♦ [“Configuring Multiple DVAs for the WebAccess Application”](#) on page 905
- ♦ [“Enabling the Document Viewer Agent \(DVA\) for Indexing”](#) on page 576
- ♦ [“Configuring the DVA Web Console”](#) on page 726

48.2.3 Securing Document Conversion with SSL Connections

Secure Sockets Layer (SSL) ensures secure communication between the DVA and other programs (WebAccess Application, POA, and DVA Web console) by encrypting the complete communication flow between the programs. By default, SSL is not enabled for the DVA.

For background information about using SSL with GroupWise agents, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107. The server where the DVA is installed must have a public certificate file and private key file before you can enable SSL for the DVA.

NOTE: When you enable SSL for the DVA, any POAs that it communicates with must also be enabled for SSL.

- 1 Open the `gwdva.dva` file in a text editor.
- 2 Search to find the following switch:

```
/https1
```
- 3 Remove the semicolon (;) to activate the setting.
- 4 For subsequent switches:
 - 4a Specify the full path name to the SSL public certificate file.
The DVA requires that the certificate file be in PEM format.
 - 4b Specify the full path name to the SSL private key file.
 - 4c Specify the password for the private key file.
- 5 Save the `gwdva.dva` file.
- 6 Skip to [Section 48.4, “Putting DVA Configuration Changes into Effect,”](#) on page 722.

48.3 Enabling the DVA Document Quarantine

You can configure the DVA to quarantine document files that cannot be converted to HTML format for viewing in GroupWise WebAccess, so that they can be examined manually if necessary. You can control the maximum amount of disk space that the document quarantine is allowed to occupy. You can also control the maximum amount of time that document files remain in the quarantine.

- 1 Open the `gwdva.dva` file in a text editor.
- 2 Search to find the following switch:

```
/quarantine
```

- 3 Remove the semicolon (;) to activate the setting.

With the quarantine activated, document files that fail HTML conversion are placed in the `quarantine` subdirectory of the DVA working directory (`gwdva.dir`).

- 4 (Optional) As needed, increase or decrease the number of days that document files are held in quarantine.

The default is 7 days.

- 5 (Optional) As needed, increase or decrease the amount of disk space that the quarantine is allowed to consume.

The default is 100 MB. Quarantined document files that exceed the maximum time limit are removed even if the maximum quarantine size has not been exceeded.

- 6 (Conditional) When you are finished examining the quarantined document files, set the maximum quarantine size to 0 (zero).

This disables the quarantine and deletes all the quarantined document files.

IMPORTANT: Quarantined document files are not encrypted, so you should disable the quarantine as soon as you are finished examining the quarantined files.

- 7 Save the `gwdva.dva` file.
- 8 Continue with [Putting DVA Configuration Changes into Effect](#).

NOTE: If files passed to the DVA from the POA for HTML conversion in preparation for indexing fail in HTML conversion by the DVA, they are placed in the `post_office/oftemp/gwdca/problem` directory, as if they had been processed by the DCA rather than the DVA. For more information about the DCA, see [Section 39.2, “Configuring the Document Converter Agent \(DCA\),” on page 575](#).

48.4 Putting DVA Configuration Changes into Effect

After you edit the `gwdva.dva` file, stop and then start the DVA to put the changes into effect.

- ♦ [Section 48.4.1, “Linux: Stopping and Starting the DVA,” on page 722](#)
- ♦ [Section 48.4.2, “Windows: Stopping and Starting the DVA,” on page 723](#)

48.4.1 Linux: Stopping and Starting the DVA

On Linux, use the following commands to stop and start the Linux DVA:

```
rcgrpwise stop gwdva  
rcgrpwise start gwdva
```

48.4.2 Windows: Stopping and Starting the DVA

On Windows, stop and start the DVA as you would any other Windows GroupWise agent, as described in the following sections of the [GroupWise 2012 Installation Guide](#):

- ♦ [“Starting the Windows GroupWise Agents”](#)
- ♦ [“Stopping the Windows GroupWise Agents”](#)

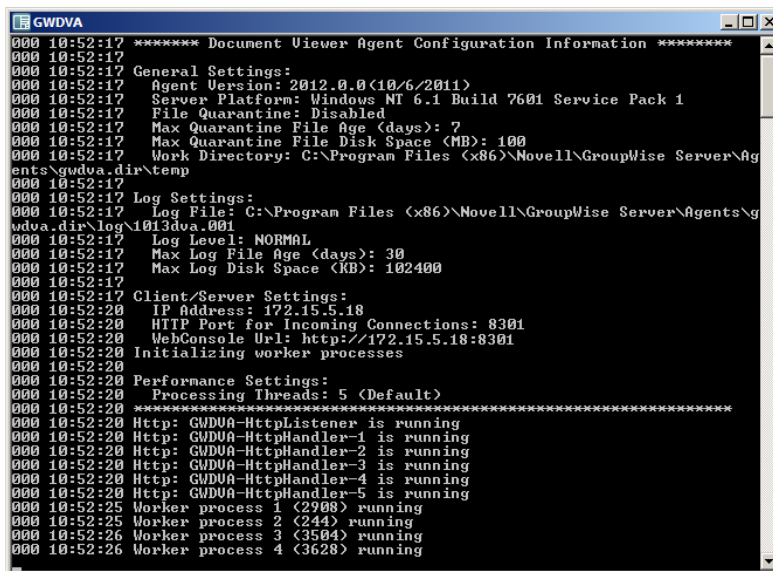
49 Monitoring the DVA

The DVA can be monitored at the server where it runs (Windows only) and also in your Web browser. You can also use log files to monitor the DVA.

- ♦ [Section 49.1, “Using the DVA Server Console \(Windows Only\),” on page 725](#)
- ♦ [Section 49.2, “Using the DVA Web Console,” on page 725](#)
- ♦ [Section 49.3, “Using DVA Log Files,” on page 727](#)

49.1 Using the DVA Server Console (Windows Only)

The DVA server console displays messages about DVA functioning.



```
GWDVA
000 10:52:17 ***** Document Viewer Agent Configuration Information *****
000 10:52:17
000 10:52:17 General Settings:
000 10:52:17 Agent Version: 2012.0.0 (10/6/2011)
000 10:52:17 Server Platform: Windows NT 6.1 Build 7601 Service Pack 1
000 10:52:17 File Quarantine: Disabled
000 10:52:17 Max Quarantine File Age (days): 7
000 10:52:17 Max Quarantine File Disk Space (MB): 100
000 10:52:17 Work Directory: C:\Program Files (x86)\Novell\GroupWise Server\Ag
ents\gwdva.dir\temp
000 10:52:17
000 10:52:17 Log Settings:
000 10:52:17 Log File: C:\Program Files (x86)\Novell\GroupWise Server\Agents\g
wdva.dir\log\1013dva.001
000 10:52:17 Log Level: NORMAL
000 10:52:17 Max Log File Age (days): 30
000 10:52:17 Max Log Disk Space (KB): 102400
000 10:52:17
000 10:52:17 Client/Server Settings:
000 10:52:20 IP Address: 172.15.5.18
000 10:52:20 HTTP Port for Incoming Connections: 8301
000 10:52:20 WebConsole Url: http://172.15.5.18:8301
000 10:52:20 Initializing worker processes
000 10:52:20
000 10:52:20 Performance Settings:
000 10:52:20 Processing Threads: 5 (Default)
000 10:52:20 *****
000 10:52:20 Http: GWDVA-HttpListener is running
000 10:52:20 Http: GWDVA-HttpHandler-1 is running
000 10:52:20 Http: GWDVA-HttpHandler-2 is running
000 10:52:20 Http: GWDVA-HttpHandler-3 is running
000 10:52:20 Http: GWDVA-HttpHandler-4 is running
000 10:52:20 Http: GWDVA-HttpHandler-5 is running
000 10:52:25 Worker process 1 (2908) running
000 10:52:25 Worker process 2 (244) running
000 10:52:26 Worker process 3 (3504) running
000 10:52:26 Worker process 4 (3628) running
```

These messages are also written to the DVA log file, described in [Section 49.3, “Using DVA Log Files,” on page 727](#).

49.2 Using the DVA Web Console

The DVA Web console enables you to monitor the DVA from any location where you have access to a Web browser and the Internet.

- ♦ [“Configuring the DVA Web Console” on page 726](#)
- ♦ [“Viewing the DVA Web Console” on page 726](#)

49.2.1 Configuring the DVA Web Console

- 1 Open the [gwdva.dva file](#) in a text editor.
- 2 To specify the user name for logging into the DVA Web console:
 - 2a Search to find the following line:

```
httpuser
```

- 2b Remove the semicolon (;) to activate the setting.
 - 2c Specify a unique user name.
- 3 To specify the password for logging into the DVA Web console:
 - 3a Search to find the following line:

```
httppassword
```

- 3b Remove the semicolon (;) to activate the setting.
 - 3c Specify the password for the Web console user.

Unless you are using an SSL connection, do not use a Novell eDirectory user name and password because the information passes over the non-secure connection between your Web browser and the DVA.
- 4 (Conditional) If the default DVA HTTP port of 8301 is already in use on the server:
 - 4a Search to find the following line:

```
httpport
```

- 4b Remove the semicolon (;) to activate the setting.
 - 4c Specify a unique port number.
- 5 Save the `gwdva.dva` file.
- 6 Skip to [Section 48.4, "Putting DVA Configuration Changes into Effect,"](#) on page 722.

49.2.2 Viewing the DVA Web Console

- 1 In a Web browser, enter the following URL:

```
http://server_address:port_number
```

Replace *server_address* with the DVA server IP address or DNS hostname, and replace *port_number* with 8301 or whatever port number you have specified in the DVA startup file.

- 2 When prompted, enter the user name and password.

The DVA Web console is displayed.

The screenshot shows the GroupWise 2012 Document Viewer Agent web console. It includes a navigation menu with links for Status, Configuration, Environment, Log Files, Quarantine Files, and Help. The status bar shows 'Up Time: 0 Days 5 Hours 27 Minutes'. Below this are two tables: 'Worker Processes' and 'Request Statistics'.

GroupWise 2012 Document Viewer Agent		
Status Configuration Environment Log Files Quarantine Files Help		
Up Time: 0 Days 5 Hours 27 Minutes		
	Total	Busy Peak
Worker Processes	5	1 1

Server Information	
Platform Name	Linux Release 2.6.16.60-0.54.5-default
High Availability Port	8400

Request Statistics	
	Total
File Conversion Requests	0
Conversion Success	0
Conversion Failure	0
Worker Abends	0
Exceeded Time Limit	0

Through the DVA Web console you can view the following information:

- ♦ **Status:** Displays how long the DVA has been up, the number of worker threads it has started, the current server utilization, and statistics about the files the worker threads have processed.
- ♦ **Configuration:** Displays the current settings of all the options that you can set in the DVA startup file (`gwdva.dva`). For more information, see [Chapter 48, “Configuring the DVA,” on page 719](#).
- ♦ **Environment:** Displays server information such as name, operating system date, memory, processor utilization, and loaded modules.
- ♦ **Log Files:** Lets you view the contents of the DVA’s log files and the current log settings. For more information, see [Section 49.3, “Using DVA Log Files,” on page 727](#).
- ♦ **Quarantine Files:** Indicates whether the document quarantine is enabled, and if so, what files have been quarantined. For more information, see [Section 48.3, “Enabling the DVA Document Quarantine,” on page 722](#)

For detailed information about each field on the DVA Web console pages, click *Help*.

You cannot use the Web console to change any of the DVA’s settings. Changes must be made through the DVA startup file (`gwdva.dva`).

49.3 Using DVA Log Files

Error messages and other information about DVA functioning are written to log files as well as displaying on the DVA server console (Windows only). Log files can provide a wealth of information for resolving problems with DVA functioning. Logging is enabled by default.

- ♦ [Section 49.3.1, “Locating DVA Log Files,” on page 727](#)
- ♦ [Section 49.3.2, “Configuring DVA Log Settings,” on page 727](#)
- ♦ [Section 49.3.3, “Viewing DVA Log Files,” on page 728](#)
- ♦ [Section 49.3.4, “Interpreting DVA Log File Information,” on page 728](#)

49.3.1 Locating DVA Log Files

The default location of the DVA log files varies by platform:

Linux: `/var/log/novell/groupwise/gwdva`

Windows: `c:\Program Files\Novell\GroupWise Server\Agents\gwdva.dir\log`

You can change the location where the DVA creates its log files, as described in [Configuring DVA Log Settings](#).

49.3.2 Configuring DVA Log Settings

- 1 Open the `gwdva.dva` file in a text editor.
- 2 Search to find the `Log Switches` section.
- 3 Adjust the following log settings as needed:
 - loglevel:** There are three log levels:
 - ♦ **Normal (default)** Displays warnings and errors.

- ◆ **Verbose:** Displays the Normal log level information, plus information messages and user requests.
- ◆ **Diagnostic:** Displays all possible information. Use Diagnostic only if you are troubleshooting a problem with the DVA.

The Verbose and Diagnostic log levels do not degrade DVA performance, but log files consume more disk space when Verbose or Diagnostic logging is in use.

--log: For the default location of DVA log files, see [Section 49.3.1, “Locating DVA Log Files,”](#) on [page 727](#). Specify a different location for DVA log files as needed.

--logdays: Specify the number of days you want to retain the log files. The DVA retains log files for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 30 days.

--logmax: Specify the maximum amount of disk space you want to use for DVA log files. If the disk space limit is exceeded, the DVA deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 102400 KB (100 MB).

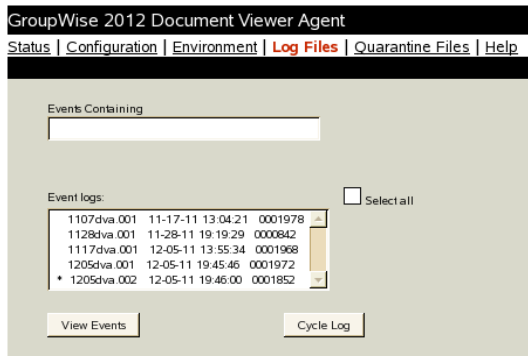
- 4 Save the `gwdva.dva` file.
- 5 Skip to [Section 48.4, “Putting DVA Configuration Changes into Effect,”](#) on [page 722](#).

49.3.3 Viewing DVA Log Files

For the default location of the DVA log files, see [Section 49.3.1, “Locating DVA Log Files,”](#) on [page 727](#)

When logging is turned on, the DVA creates a new log file each day and each time it is restarted. Therefore, you find multiple log files in the log file directory. The first four characters represent the date (*mmdd*). The next three characters identify the agent (*dva*). A three-digit extension allows for multiple log files created on the same day. For example, a log file named `0518dva.001` indicates that it is a DVA log file created on May 18.

For convenience, you can view DVA log files in the [DVA Web console](#):



49.3.4 Interpreting DVA Log File Information

On startup, the DVA records the DVA settings currently in effect. Thereafter, it logs events that take place, including errors.

Because the DVA consists of multiple threads, you might find it useful to retrieve the log file into an editor and sort it on the thread ID that follows the date and time information. Sorting groups all messages together for the same DVA thread. You can also use the search capability of the [DVA Web console](#) to gather information about events that contain a specific string.

50 Optimizing the DVA

- ♦ [Section 50.1, “Controlling Thread Usage,” on page 729](#)
- ♦ [Section 50.2, “Controlling Maximum Document Conversion Size and Time Limits,” on page 730](#)

50.1 Controlling Thread Usage

By default, the DVA starts 5 worker threads for converting attached document files into HTML format. It adds threads as demand for document file conversion increases. By default, the DVA can start a maximum of 20 worker threads.

- 1 Open the [gwdva.dva file](#) in a text editor.
- 2 To set the initial number of worker threads to start:

2a Search to find the following switch:

```
/httpthread
```

2b Remove the semicolon (;) to activate the setting.

2c Specify the maximum number of worker threads that you want the DVA to start automatically.

- 3 To set the maximum number of worker threads:

3a Search to find the following switch:

```
/httpmaxthread
```

3b Remove the semicolon (;) to activate the setting.

3c Specify the maximum number of worker threads that the DVA is allowed to start.

You can increase the maximum number of worker threads to allow the DVA to use more server resources, or you can decrease the maximum number of worker threads to cause the DVA to use fewer server resources.

- 4 Save the `gwdva.dva` file.
- 5 Skip to [Section 48.4, “Putting DVA Configuration Changes into Effect,” on page 722](#).

50.2 Controlling Maximum Document Conversion Size and Time Limits

If the DVA starts converting a very large document file, it can take a very long time to complete the conversion into HTML format. The maximum size limit for document files processed by the DVA is initially set by the program that sends the document files to the DVA for conversion. For more information, see:

- ♦ WebAccess: [Section 62.3.3, “Controlling Viewable Attachment Size,” on page 913](#)
- ♦ POA: [Section 39.4, “Controlling Maximum Document Conversion Size and Time,” on page 577](#)

However, you can prevent the DVA from ever accepting document files over a specific size. You can also limit the amount of time a DVA worker thread spends converting a single document file.

- 1 Open the [gwdva.dva file](#) in a text editor.
- 2 To establish a maximum document file size:
 - 2a Search to find the following switch:

```
/maxsize
```
 - 2b Remove the semicolon (;) to activate the setting.
 - 2c Specify the maximum size in kilobytes for document files that you want the DVA to accept for conversion.

By default, the DVA accepts all files that are sent to it by the WebAccess Application and the POA.
- 3 To change the maximum length of time the DVA processes a single document file:
 - 3a Search to find the following switch:

```
/maxtime
```
 - 3b Remove the semicolon (;) to activate the setting.
 - 3c Specify the maximum number of seconds that you want the DVA to work at converting a single document file.

The default is 300 seconds (5 minutes). Valid values range from 60 seconds (1 minute) to 1200 seconds (20 minutes).
- 4 Save the [gwdva.dva file](#).
- 5 Skip to [Section 48.4, “Putting DVA Configuration Changes into Effect,” on page 722](#).

51 Using Document Viewer Agent Startup Switches

The DVA is configured by editing its startup file (`gwdva.dva`). The default location for the startup file varies by platform.

Linux: `/opt/novell/groupwise/agents/share`

Windows: `c:\Program Files\Novell\GroupWise Server\Agents`

When you update the agent software, the existing DVA startup file can be retained or overwritten as needed.

Linux: When you use both the *Install* and *Configure* options in the Agent Installation program, the existing DVA startup file is backed up and then overwritten. When you use only the *Install* option, the existing DVA startup file is retained.

Windows: When you select *Install the software files, but do not configure the agents* in the Agent Installation program, the existing DVA startup file is retained. When you do not select this option, the existing DVA startup file is backed up and then overwritten.

The table below summarizes DVA startup switches and how they correspond to configuration settings in ConsoleOne.

Switch starts with: a b c d e f g h i j k l m n o p q r s t u v w x y z

Linux DVA	Windows DVA	ConsoleOne Settings
<code>--home</code>	<code>/home</code>	N/A
<code>--httpmaxthread</code>	<code>/httpmaxthread</code>	N/A
<code>--httppassword</code>	<code>/httppassword</code>	N/A
<code>--httpport</code>	<code>/httpport</code>	N/A
<code>--httpssl</code>	<code>/httpssl</code>	N/A
<code>--httpthread</code>	<code>/httpthread</code>	N/A
<code>--httpuser</code>	<code>/httpuser</code>	N/A
<code>--ip</code>	<code>/ip</code>	N/A
<code>--lang</code>	<code>/lang</code>	N/A
<code>--log</code>	<code>/log</code>	N/A
<code>--logdays</code>	<code>/logdays</code>	N/A

Linux DVA	Windows DVA	ConsoleOne Settings
--loglevel	/loglevel	N/A
--logmax	/logmax	N/A
--maxquarantineage	/maxquarantineage	N/A
--maxquarantinesize	/maxquarantinesize	N/A
--maxsize	/maxsize	N/A
--maxtime	/maxtime	N/A
--quarantine	/quarantine	N/A
--sslcert	/sslcert	N/A
--sslkey	/sslkey	N/A
--sslkeypassword	/sslkeypassword	N/A
--temp	/temp	N/A
--template	/template	N/A

51.1 --home

Specifies the location for the DVA working directory. The default is `gwdva.dir` in the DVA installation directory. See [Section 48.2.1, “Setting the DVA Home Directory,”](#) on page 719.

	Linux DVA	Windows DVA
Syntax:	--home <i>/directory</i>	<i>/home-[drive:]/dir</i> <i>/home-\\sv\sharename\dir</i>
Example:	--home <i>/opt/novell/groupwise/gwdva</i>	<i>/home-\\Program Files\Novell\GroupWise Server\gwdva</i> <i>/home-m:\temp\gwdva</i> <i>/home-\\server2\c\temp\gwdva</i>

If you specify a UNC path with the `--home` switch when you run the DVA as a Windows service, you must configure the DVA service to run under a specific Windows user account. If you specify a local directory or a mapped drive, you can configure the DVA service to run under the local system account. However, running under the Administrator account is highly recommended.

51.2 --httpmaxthread

Specifies the maximum number of worker threads that the DVA can start. By default, the DVA creates new worker threads as needed to handle the current document conversion load, and the default maximum is 20 threads. See [Section 50.1, “Controlling Thread Usage,”](#) on page 729

	Linux DVA	Windows DVA
Syntax:	--httpmaxthread <i>number</i>	<i>/httpmaxthread-number</i>
Example:	--httpmaxthread 7420	<i>/httpmaxthread-7410</i>

See also [--httpthread](#).

51.3 --httpport

Sets the HTTP port number used for the DVA to communicate with other programs (the WebAccess Application, the POA, and the DVA Web console). The default is 8301; the setting must be unique. See [Section 48.2.2, “Changing the DVA IP Address or Port Number,”](#) on page 720.

	Linux DVA	Windows DVA
Syntax:	<code>--httpport <i>port_number</i></code>	<code>/httpport-<i>port_number</i></code>
Example:	<code>--httpport 8302</code>	<code>/httpport-8303</code>

See also [--httppassword](#), and [--httpuser](#).

51.4 --httppassword

Specifies the password for the DVA to prompt for before allowing DVA status information to be displayed in your Web browser in the DVA Web console. See [“Configuring the DVA Web Console”](#) on page 726.

	Linux DVA	Windows DVA
Syntax:	<code>--httppassword <i>unique_password</i></code>	<code>/httppassword-<i>unique_password</i></code>
Example:	<code>--httppassword AgentWatch</code>	<code>/httppassword-AgentWatch</code>

See also [--httpport](#), and [--httpuser](#).

51.5 --httpsll

Enables secure SSL connections between the DVA and other programs (the WebAccess Application, the POA, and your Web browser for the DVA Web console). See [Section 48.2.3, “Securing Document Conversion with SSL Connections,”](#) on page 721.

	Linux DVA	Windows DVA
Syntax:	<code>--httpsll</code>	<code>/httpsll</code>

See also [--sslcert](#), [--sslkey](#), and [--sslkeypassword](#).

51.6 --httpthread

Sets the default number of worker threads that the DVA starts. The default is 5 threads. As the document conversion load increases, the DVA starts additional worker threads until the number set by the `--httpmaxthread` startup switch is reached. See [Section 50.1, “Controlling Thread Usage,” on page 729](#).

	Linux DVA	Windows DVA
Syntax:	<code>--httpthread <i>threads</i></code>	<code>/httpthread <i>threads</i></code>
Example:	<code>--httpthread 10</code>	<code>/httpthread 15</code>

See also [--httpmaxthread](#).

51.7 --httpuser

Specifies the user name for the DVA to prompt for before allowing DVA status information to be displayed in a Web browser at the DVA Web console. See [“Configuring the DVA Web Console” on page 726](#).

	Linux DVA	Windows DVA
Syntax:	<code>--httpuser <i>unique_name</i></code>	<code>/httpuser-<i>unique_name</i></code>
Example:	<code>--httpuser DVAWebCon</code>	<code>/httpuser-DVAWebCon</code>

See also [--httpport](#) and [--httppassword](#).

51.8 --ip

Specifies the IP address that the DVA listens on for HTTP requests from other programs (the WebAccess Application, the POA, and the DVA Web console). The default is the first IP address that the DVA finds on the server. See [Section 48.2.2, “Changing the DVA IP Address or Port Number,” on page 720](#).

	Linux DVA	Windows DVA
Syntax:	<code>--ip <i>IP_address</i></code>	<code>/ip-<i>IP_address</i></code>
Example:	<code>--ip 172.16.5.18</code>	<code>/ip-172.16.5.18</code>

See also [--httpport](#).

51.9 --lang

Specifies the ISO language code that the DVA should use if it cannot determine the language of a document that needs conversion. The default is en for English.

	Linux DVA	Windows DVA
Syntax:	<code>--lang /ISO_code</code>	<code>/lang-ISO_code</code>
Example:	<code>--lang de</code>	<code>/lang-es</code>

See [Chapter 7, “Multilingual GroupWise Systems,” on page 123](#) for a list of GroupWise language codes.

51.10 --log

Sets the directory where the DVA stores its log files. For more information, see [Section 49.3.2, “Configuring DVA Log Settings,” on page 727](#).

	Linux DVA	Windows DVA
Syntax:	<code>--log /dir</code>	<code>/log-[drive:]dir</code> <code>/log-\\sv\sharename\dir</code>
Example:	<code>--log /gwsystem/logs</code>	<code>/log-\agt\log</code> <code>/log-m:\agt\log</code> <code>/log-\\server2\c\mail\agt\log</code>

See also [--loglevel](#), [--logdays](#), and [--logmax](#).

51.11 --logdays

Specifies how many days to keep DVA log files on disk. The default is 30 days. See [Section 49.3.2, “Configuring DVA Log Settings,” on page 727](#).

	Linux DVA	Windows DVA
Syntax:	<code>--logdays days</code>	<code>/logdays-days</code>
Example:	<code>--logdays 10</code>	<code>/logdays-14</code>

See also [--log](#), [--loglevel](#), and [--logmax](#).

51.12 --loglevel

Controls the amount of information logged by the DVA. Valid settings are Normal, Verbose, Diagnostic, and Off. The default is Normal. For more information, see [Section 49.3.2, “Configuring DVA Log Settings,”](#) on page 727.

	Linux DVA	Windows DVA
Syntax:	--loglevel <i>level</i>	/loglevel- <i>level</i>
Example:	--loglevel verbose	/loglevel-verbose

See also [--log](#), [--logdays](#), and [--logmax](#).

51.13 --logmax

Sets the maximum amount of disk space for all DVA log files. When the specified disk space is consumed, the DVA deletes existing log files, starting with the oldest. The default is 102400 KB (100 MB). The maximum allowable setting is 102400000 (1 GB). See [Section 49.3.2, “Configuring DVA Log Settings,”](#) on page 727.

	Linux DVA	Windows DVA
Syntax:	--logmax <i>kilobytes</i>	/logmax- <i>kilobytes</i>
Example:	--logmax 130000	/logmax-1600

See also [--log](#), [--logdays](#), and [--logmax](#).

51.14 --maxquarantineage

Specifies the maximum number of days that document files that fail in HTML conversion are retained in the quarantine. By default, the quarantine is disabled. See [Section 48.3, “Enabling the DVA Document Quarantine,”](#) on page 722

	Linux DVA	Windows DVA
Syntax:	--maxquarantineage <i>days</i>	/maxquarantineage- <i>days</i>
Example:	--maxquarantineage 15	/maxquarantineage-60

See also [--quarantine](#) and [--maxquarantinesize](#).

51.15 --maxquarantinesize

Specifies in megabytes the maximum amount of disk space that the document quarantine can occupy. The default is 100 MB. To clear out the contents of the quarantine, set `--maxquarantinesize` to 0 (zero); this also disables the quarantine in the future. See [Section 48.3, “Enabling the DVA Document Quarantine,”](#) on page 722.

	Linux DVA	Windows DVA
Syntax:	<code>--maxquarantinesize megabytes</code>	<code>/maxquarantinesize-megabytes</code>
Example:	<code>--maxquarantinesize 200</code>	<code>/maxquarantinesize-300</code>

See also `--quarantine` and `--maxquarantineage`.

51.16 --maxsize

Specifies in kilobytes the maximum size for document files that you want the DVA to accept for conversion. The default maximum size is 20480 (20 MB). See [Section 50.2, “Controlling Maximum Document Conversion Size and Time Limits,”](#) on page 730.

	Linux DVA	Windows DVA
Syntax:	<code>--maxsize kilobytes</code>	<code>/maxsize-kilobytes</code>
Example:	<code>--maxsize 30240</code>	<code>/maxsize-10240</code>

The DVA receives files to convert from the WebAccess Application and the POA. The initial maximum size limit for document files processed by the DVA is set by the program that sends the document files. The sending programs should be configured to send document files within the maximum size allowed by the DVA. See:

- WebAccess: [Section 62.3.3, “Controlling Viewable Attachment Size,”](#) on page 913
- POA: [Section 39.4, “Controlling Maximum Document Conversion Size and Time,”](#) on page 577

51.17 --maxtime

Specifies in seconds the maximum amount of time a DVA worker thread is allowed to work on a converting a single document file. The default is 300 seconds (5 minutes). Valid values range from 60 seconds (1 minute) to 1200 seconds (20 minutes). See [Section 50.2, “Controlling Maximum Document Conversion Size and Time Limits,”](#) on page 730.

	Linux DVA	Windows DVA
Syntax:	<code>--maxtime seconds</code>	<code>/maxtime-seconds</code>
Example:	<code>--maxtime 600</code>	<code>/maxtime-60</code>

When the DVA provides HTML conversion for the POA, the setting of the DVA `--maxtime` switch interacts with the setting of the POA `--dcamaxtime` switch, which sets the amount of time that the POA waits for a response from the DVA.

51.18 --quarantine

Enables the document quarantine feature of the DVA, which is disabled by default. See [Section 48.3, “Enabling the DVA Document Quarantine,”](#) on page 722

	Linux DVA	Windows DVA
Syntax:	--quarantine	/quarantine

See also [--maxquarantineage](#) and [--maxquarantinesize](#).

NOTE: If files passed to the DVA from the POA for HTML conversion in preparation for indexing fail in HTML conversion by the DVA, they are placed in the `post_office/oftemp/gwdca/problem` directory, as if they had been processed by the DCA rather than the DVA. For more information about the DCA, see [Section 39.2, “Configuring the Document Converter Agent \(DCA\),”](#) on page 575.

51.19 --sslcert

For secure SSL connections between the DVA and other programs (the WebAccess Application, the POA, and your Web browser for the DVA Web console), specifies the full path name of the SSL certificate file. See [Section 48.2.3, “Securing Document Conversion with SSL Connections,”](#) on page 721.

	Linux DVA	Windows DVA
Syntax:	--sslcert <i>/directory/certificate_file</i>	/sslcert-[drive:]\dir\file /sslcert-\\svr\sharename\dir\file
Example:	--sslcert /certs/gw.crt	/sslcert-ssl\gw.crt /sslcert-m:ssl\gw.crt /sslcert-\\server2\c\ssl\gw.crt

See also [--https](#), [--sslkey](#), and [--sslkeypassword](#).

51.20 --sslkey

Specifies the full path to the private file used to provide secure SSL communication between the DVA and other programs (the WebAccess Application, the POA, and the DVA Web console). See [Section 48.2.3, “Securing Document Conversion with SSL Connections,”](#) on page 721.

	Linux DVA	Windows DVA
Syntax:	--sslkey <i>/dir/file</i>	/sslkey-[drive:]\dir\file /sslkey-\\svr\sharename\dir\file
Example:	--sslkey /certs/gw.key	/sslkey-ssl\gw.key /sslkey-m:ssl\gw.key /sslkey-\\server2\c\ssl\gw.key

See also [--https](#), [--sslcert](#), and [--sslkeypassword](#).

51.21 --sslkeypassword

Specifies the password used to encrypt the private SSL key file when it was created. See [Section 48.2.3, “Securing Document Conversion with SSL Connections,”](#) on page 721.

	Linux DVA	Windows PDV
Syntax:	--sslkeypassword <i>password</i>	/sslkeypassword- <i>password</i>
Example:	--sslkeypassword gwssl	/sslkeypassword-gwssl

See also [--httpssl](#), [--sslcert](#), and [--sslkeypassword](#).

51.22 --temp

Sets the path to the directory where the DVA creates its temporary files. The default location varies by platform. The default is a subdirectory of the DVA working directory (`gwdva.dir`). See [Section 48.2.1, “Setting the DVA Home Directory,”](#) on page 719

	Linux DVA	Windows DVA
Syntax:	--temp <i>dir</i>	/temp-[<i>drive:</i>]\ <i>dir</i> /temp-\\sv\ <i>sharename</i> \ <i>dir</i>
Example:	--temp /gwsystem/temp	/temp-dva\temp /temp-m:\dva\temp /temp-\\server2\c\mail\dva\temp

51.23 --template

Specifies the full path to the directory for storing the HTML template files. Template files provide the basic HTML format into which document files of all formats are converted for display in your Web browser. The default is a subdirectory of the DVA home directory. See [Section 48.2.1, “Setting the DVA Home Directory,”](#) on page 719

	Linux DVA	Windows DVA
Syntax:	--template <i>dir</i>	/template-[<i>drive:</i>]\ <i>dir</i> /template-\\sv\ <i>sharename</i> \ <i>dir</i>
Example:	--template /gwsystem/temp	/template-dva\template /template-m:\dva\template /template-\\server2\c\mail\dva\template

XII Internet Agent

- ♦ Chapter 52, “Configuring Internet Addressing,” on page 743
- ♦ Chapter 53, “Configuring Internet Services,” on page 757
- ♦ Chapter 54, “Managing Internet Access,” on page 787
- ♦ Chapter 55, “Configuring the GWIA,” on page 809
- ♦ Chapter 56, “Monitoring the GWIA,” on page 817
- ♦ Chapter 57, “Optimizing the GWIA,” on page 839
- ♦ Chapter 58, “Connecting GroupWise Systems and Domains Using the GWIA,” on page 843
- ♦ Chapter 59, “Using GWIA Startup Switches,” on page 851

For a complete list of port numbers used by the GWIA, see [Section A.6, “Internet Agent Port Numbers,”](#) on page 1170.

For detailed Linux-specific GWIA information, see [Appendix C, “Linux Commands, Directories, and Files for GroupWise Administration,”](#) on page 1179.

For additional assistance in managing the GWIA, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

52 Configuring Internet Addressing

By default, GroupWise uses a proprietary address format consisting of a user's ID, post office, and domain (*userID.post_office.domain*). However, when you install the GroupWise Internet Agent (GWIA), GroupWise also supports native Internet-style addressing consisting of a user name and Internet domain name (for example, *userID@Internet_domain_name*).

Internet-style addressing is the preferred addressing format if you are connected to the Internet, because with Internet-style addressing, users have the same address within the GroupWise system as they do outside the GroupWise system. For example, if John Smith's address at Novell is *jsmith@novell.com*, this address can be used by users within the GroupWise system and users external to the system.

To set up Internet addressing, you do the following:

- ◆ Define Internet domain names for your GroupWise system. You can have one or more domain names (for example, *novell.com*, *gw.novell.com*, and *support.novell.com*).
- ◆ Set up the default Internet address format for use when displaying user addresses in the GroupWise Address Book and sent messages. There are six formats that can be assigned at the system, domain, post office, or user level. In addition, there is a free-form format that can be used at the user level.
- ◆ Designate the address formats that can be used to address messages to your GroupWise users. There are five possible formats to choose from. You can allow all five formats, or only one.
- ◆ Specify the default GWIA to be used when sending messages from your GroupWise system to the Internet. This becomes your system's default GWIA for outbound messages sent from all domains; however, if you have multiple GWIAs, you can override this setting by assigning GWIAs at the domain level.

The following sections help you plan and set up Internet addressing:

- ◆ [Section 52.1, "Planning Internet Addressing," on page 743](#)
- ◆ [Section 52.2, "Setting Up Internet Addressing," on page 748](#)
- ◆ [Section 52.3, "Transitioning from SMTP Gateway Aliases to Internet Addressing," on page 754](#)

52.1 Planning Internet Addressing

The following sections help you prepare to set up Internet-style addressing for your GroupWise system:

- ◆ [Section 52.1.1, "GWIA Requirement," on page 744](#)
- ◆ [Section 52.1.2, "GWIA Used for Outbound Messages," on page 744](#)
- ◆ [Section 52.1.3, "Internet Domain Names," on page 744](#)
- ◆ [Section 52.1.4, "Preferred Address Format," on page 744](#)

- ♦ [Section 52.1.5, “Allowed Address Formats,”](#) on page 747
- ♦ [Section 52.1.6, “Override Options,”](#) on page 748

52.1.1 GWIA Requirement

Internet addressing requires you to have the GroupWise GWIA installed in your GroupWise system. The GWIA connects your GroupWise system to the Internet. To install the GWIA, see “[Installing the GroupWise Internet Agent](#)” in the *GroupWise 2012 Installation Guide*.

52.1.2 GWIAs Used for Outbound Messages

Each domain in your GroupWise system must be assigned an GWIA for outbound messages. A domain’s assigned GWIA handles all outbound messages sent by the domain’s users.

If your GroupWise system includes only one GWIA, that GWIA must be assigned to all domains and is used for all outbound messages.

If your GroupWise system includes multiple GWIAs, you must decide which GWIA you want to be responsible for outbound messages for each domain. You must select one GWIA as your system’s default GWIA, but you can override the default at each domain.

52.1.3 Internet Domain Names

You must associate at least one Internet domain (such as `novell.com`, `gw.novell.com`, or `support.novell.com`) with your GroupWise system. These Internet domains need to exist in the domain name service (DNS).

After you have associated Internet domains with your GroupWise system, all users in your system can be addressed using any of the domains (for example, `jsmith@novell.com`, `jsmith@gw.novell.com`, and `jsmith@support.novell.com`). The addresses can be used both internally and externally.

Preferred Internet Domain Name

You must assign each GroupWise user a preferred Internet domain. GroupWise uses the preferred Internet domain name when constructing the email addresses that are displayed in the GroupWise Address Book and in the To field of sent messages.

To make this process easier, GroupWise lets you assign a preferred Internet domain to be used as the default for your GroupWise system (for example, `novell.com`). The system’s preferred Internet domain is applied to all users in your GroupWise system. However, you can override the system’s preferred Internet domain at the domain, post office, or user level, meaning that different users within your GroupWise system can be assigned different preferred Internet domains. For example, users in one domain can be assigned `gw.novell.com` as their preferred Internet domain while users in another domain are assigned `support.novell.com`.

52.1.4 Preferred Address Format

You must choose a preferred address format for your GroupWise users. GroupWise uses the preferred address format, along with the preferred Internet domain, to construct the email addresses that are published in the GroupWise Address Book and in the To field of sent messages.

GroupWise supports the following address formats:

userID.post_office.domain@internet_domain_name

userID.post_office@internet_domain_name
userID@internet_domain_name
firstname.lastname@internet_domain_name
lastname.firstname@internet_domain_name
firstinitial lastname@internet_domain_name

As with the preferred Internet domain, you must assign a preferred address format to be used as the default for your GroupWise system. The system's preferred address format is applied to all users in your GroupWise system. However, you can override the system's preferred address format at the domain, post office, and user/resource level.

The following sections explain some of the advantages and disadvantages of each address format:

- ♦ [“userID.post_office.domain@internet_domain_name” on page 745](#)
- ♦ [“userID.post_office@internet_domain_name” on page 745](#)
- ♦ [“userID@internet_domain_name” on page 746](#)
- ♦ [“firstname.lastname@internet_domain_name” on page 746](#)
- ♦ [“lastname.firstname@internet_domain_name” on page 746](#)
- ♦ [“firstinitial lastname@internet_domain_name” on page 747](#)

userID.post_office.domain@internet_domain_name

Advantages

- ♦ Reliable format. GroupWise guarantees that each address is unique.
- ♦ Identical user names can be used in different post offices.

Disadvantages

- ♦ Addresses tend to be long and hard to remember.
- ♦ Addresses might change over time as users are moved from one post office to another.

userID.post_office@internet_domain_name

Advantages

- ♦ Guarantees uniqueness if all your post offices have unique names.
- ♦ Identical user names can be placed in different post offices.

Disadvantages

- ♦ Addresses tend to be long and hard to remember.
- ♦ Addresses might change over time as users are moved from one post office to another.

userID@internet_domain_name

Advantages

- ◆ Addresses are short and easy to remember.
- ◆ Backward-compatible with previous versions of GroupWise. (Users won't need to update their business cards.)
- ◆ Addresses do not change as users are moved.

Disadvantages

- ◆ When you first enable this address format, you might have duplicate user IDs in your GroupWise system. However, in the future, ConsoleOne prevents you from creating duplicate user IDs within the same Internet domain name. The same user ID can be used in different Internet domains without problem.

firstname.lastname@internet_domain_name

Advantages

- ◆ Addresses are intuitive and easy to remember.
- ◆ Addresses do not change as users are moved.

Disadvantages

- ◆ When you first enable this address format, you might have duplicate first and last names in your GroupWise system. However, in the future, ConsoleOne prevents you from creating users with the same first and last names within the same Internet domain name. The same first name and last name combination can be used in different Internet domains without problem.
- ◆ The probability of conflicts increases if any user's first and last names match any GroupWise domain or post office name, if any two users have the same first and last names, or if any two users have the opposite first and last names (such as James Dean and Dean James).

lastname.firstname@internet_domain_name

Advantages

- ◆ Addresses are intuitive and easy to remember.
- ◆ Addresses do not change as users are moved.

Disadvantages

- ♦ When you first enable this address format, you might have duplicate first and last names in your GroupWise system. However, in the future, ConsoleOne prevents you from creating users with the same first and last names within the same Internet domain name. The same last name and first name combination can be used in different Internet domains without a problem.
- ♦ The probability of conflicts increases if any user's first and last names match any GroupWise domain or post office name, if any two users have the same first and last names, or if any two users have the opposite first and last names (such as James Dean and Dean James).

firstinitial lastname@internet_domain_name

Advantages

- ♦ Addresses are intuitive and easy to remember.
- ♦ Addresses do not change as users are moved.

Disadvantages

- ♦ When you first enable this address format, you might have duplicate first initial and last names in your GroupWise system. However, in the future, ConsoleOne prevents you from creating users with the same first initials and last names within the same Internet domain name. The same first initial and last name combination can be used in different Internet domains without problem
- ♦ The probability of conflicts increases when using first initials instead of complete first names.

52.1.5 Allowed Address Formats

The preferred Internet domain and preferred address format apply to user addresses as displayed in the GroupWise Address Book or in the address displayed on sent messages.

The allowed address formats, on the other hand, determine which address formats are accepted by the GWIA. There are five possible allowed formats:

userID.post_office@internet_domain_name
userID@internet_domain_name
firstname.lastname@internet_domain_name
lastname.firstname@internet_domain_name
firstinitial lastname@internet_domain_name

If you select all five formats, the GWIA accepts messages addressed to users in any of the formats. For example, John Peterson would receive messages sent using any of the following addresses:

jpgerson.research@novell.com
jpgerson@novell.com
john.peterson@novell.com
peterson.john@novell.com
jpgerson@novell.com

You must designate the allowed address formats to be used as the default formats for your GroupWise system. The system's allowed address formats are applied to all users in your GroupWise system. However, you can override the system's allowed address formats at the domain, post office, and user/resource level.

For example, assume you have two John Petersons with userIDs of jpeterson and japeterson. The *userID.post_office* and *userID* address formats do not cause message delivery problems, but the *firstname.lastname*, *lastname.firstname*, and *firstinitial lastname* address formats do. To overcome this problem, you could disallow the three problem formats for these users at the user level.

52.1.6 Override Options

In spite of the best planning, some email addresses do not fit the rules and are not processed correctly. You can handle such addresses by overriding the regular address processing, as described in [Section 52.2.3, "Overriding Internet Addressing Defaults,"](#) on page 751.

52.2 Setting Up Internet Addressing

The following sections help you to set up Internet addressing:

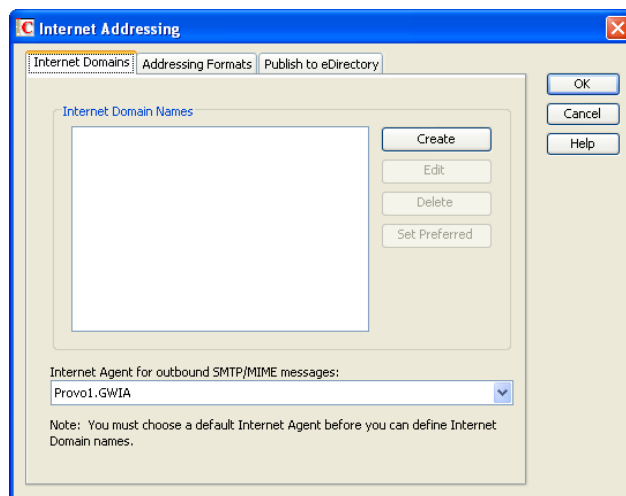
- [Section 52.2.1, "Installing the GWIA,"](#) on page 748
- [Section 52.2.2, "Enabling Internet Addressing,"](#) on page 748
- [Section 52.2.3, "Overriding Internet Addressing Defaults,"](#) on page 751

52.2.1 Installing the GWIA

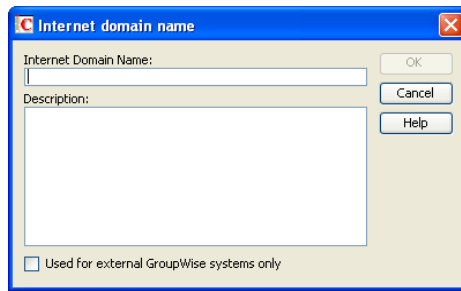
Before you can set up Internet addressing, you must install the GWIA for at least one domain. If you have not already installed the agent, see ["Installing the GroupWise Internet Agent"](#) in the *GroupWise 2012 Installation Guide*.

52.2.2 Enabling Internet Addressing

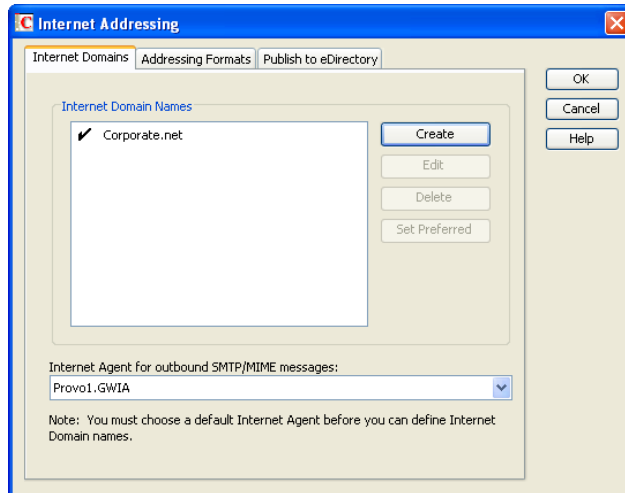
- 1 In ConsoleOne, click *Tools > GroupWise System Operations > Internet Addressing*.



- 2 On the *Internet Domains* tab, click *Create*.



- 3 Specify the Internet domain name (for example, `yourcompanyname.com`), then click *OK* to set up the first Internet domain for your GroupWise system.



- 4 If you want your GroupWise system to receive email addressed to additional Internet domain names:

- 4a Repeat [Step 2](#) and [Step 3](#).

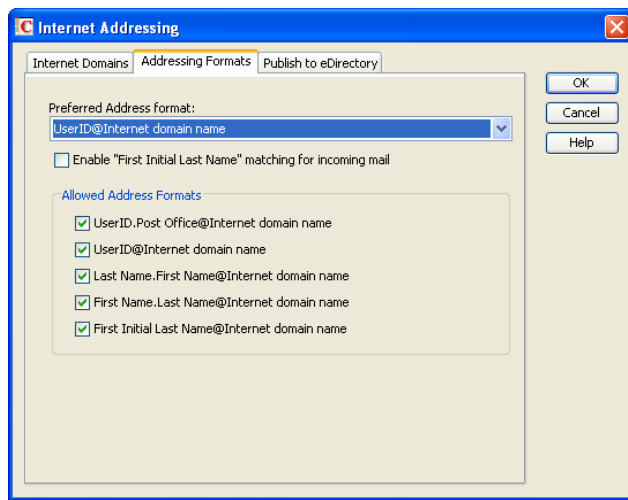
- 4b When you are finished adding Internet domain names to the list, select the preferred Internet domain name for your GroupWise system, then click *Set Preferred*.

The preferred Internet domain name is used in addresses published in the GroupWise Address Book and in the *To* field of sent messages. This can be overridden on the Internet Addressing properties pages for domains, post offices, users, and resources. For more information, see [Section 52.2.3, "Overriding Internet Addressing Defaults," on page 751](#).

- 5 In the *Internet Agent for Outbound SMTP/MIME Messages* list, select the GWIA to use as the default GWIA for your GroupWise system.

By default, all GroupWise domains use this GWIA for outbound messages sent by users in the domain. If you have multiple GWIAs in your GroupWise system, you can override the default setting at the domain level, as described in ["Domain Overrides" on page 751](#).

- 6 Click the *Addressing Formats* tab.



- 7 In the *Preferred Address Format* field, select your GroupWise system's default Internet address format.

This is the format that is used when displaying addresses in the GroupWise Address Book and in a message's *From* field if it is not overridden at a lower level. For a list of the available addressing formats and their respective advantages and disadvantages, see [Section 52.1.4, "Preferred Address Format,"](#) on page 744.

You can override the preferred address format at the domain, post office, and user/resource levels. For more information, see [Section 52.2.3, "Overriding Internet Addressing Defaults,"](#) on page 751.

- 8 If desired, turn on the *Enable "First Initial Last Name" Matching for Incoming Mail* option.

This option allows the GWIA to resolve addresses for incoming messages by performing first initial last name lookups on the user name portion of the address. When doing so, the GWIA uses the first letter of the user name as the first initial and the remainder of the user name as the last name. It then resolves the address to any GroupWise users whose Last Name field (in their eDirectory User object properties) contains the last name and whose Given Name field starts with the first initial.

For example, if the recipient's address is `jpg Peterson@novell.com`, the first initial would be J and the last name would be Peterson. The address would resolve to the user whose Last Name field is Peterson and Given Name field starts with J. If more than one user's given name starts with J (for example, John and Janice), the message is undeliverable.

This option is useful if you want to be able to use the `UserID@Internet_domain_name` format but your userIDs do not really reflect your users' actual names (for example, John Peterson's user ID is 46789 so his address is `46789@novell.com`). In this case, you could publish users' addresses as the first initial last name (for example, `jpg Peterson@novell.com`) and enable this option so that the GWIA resolves the addresses to the appropriate users.

- 9 In the *Allowed Address Formats* list, select the address formats that you want to be supported for incoming messages. GroupWise delivers a message to the recipient if any of the allowed formats have been used in the address. By default, all formats are supported.

You can override the allowed address formats at the domain, post office, and user/resource levels. For more information, see [Section 52.2.3, "Overriding Internet Addressing Defaults,"](#) on page 751.

- 10 Click OK to save your changes.

If you changed the preferred address format, you are prompted to update the Internet email address (User object > *General* > *Identification* > *E-Mail Address*) for all affected users. The Internet email address is the address returned in response to LDAP queries to eDirectory. We recommend that you allow this update; however, performing it for the entire GroupWise system might take a while.

At this point, Internet addressing is enabled and configured.

52.2.3 Overriding Internet Addressing Defaults

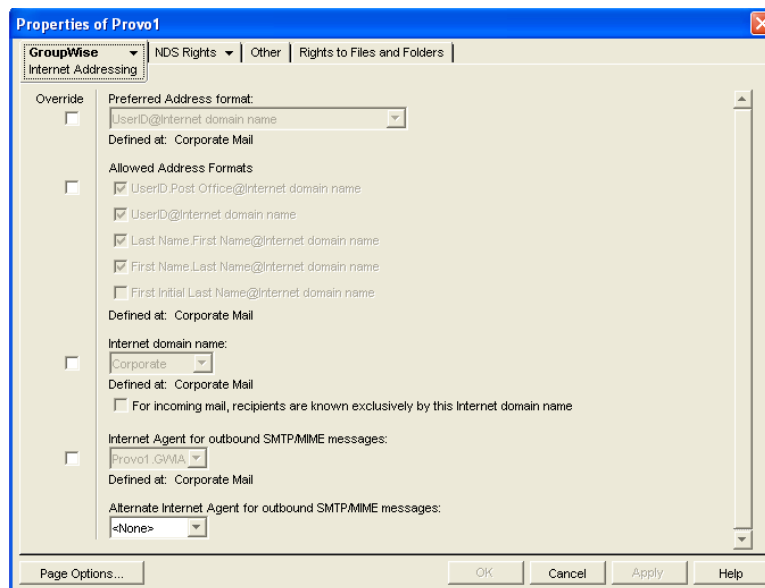
All domains, post offices, and users/resources in your GroupWise system inherit the defaults (GWIA for outbound messages, preferred Internet domain name, preferred address format, and allowed address formats) you established when enabling Internet addressing for your system. However, if desired, you can override these defaults for individual domains, post offices, or users/resources.

- ♦ [“Domain Overrides” on page 751](#)
- ♦ [“Post Office Overrides” on page 752](#)
- ♦ [“User/Resource Overrides” on page 753](#)

Domain Overrides

At the domain level, you can override all Internet addressing defaults assigned to your GroupWise system.

- 1 In ConsoleOne, right-click a Domain object, then click *Properties*.
- 2 Click *GroupWise* > *Internet Addressing*.



- 3 To override one of the options, select the *Override* box, then select the option you prefer for this domain.

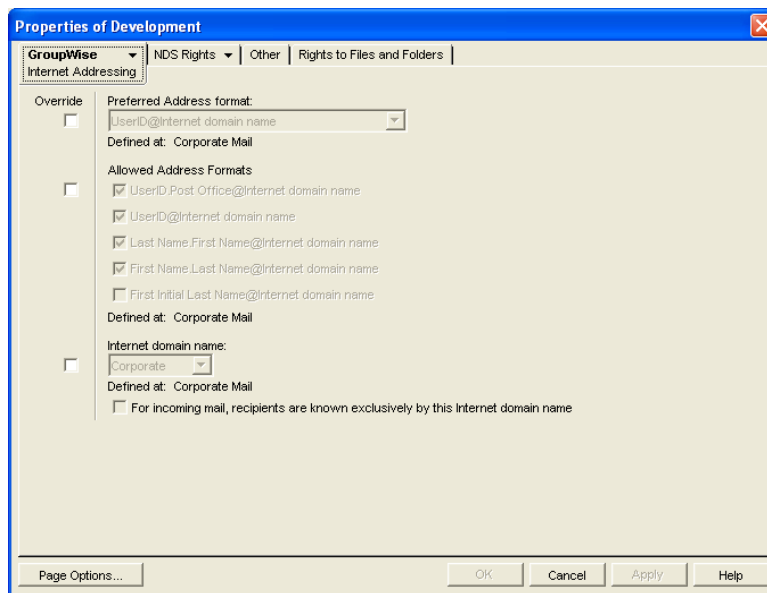
- 4 Click *OK* to save the changes.

If you changed the preferred address format, you are prompted to update the Internet email address (User object > *General* > *Identification* > *E-Mail Address*) for all affected users. The Internet email address is the address returned in response to LDAP queries to eDirectory. We recommend that you allow this update; however, performing it for an entire GroupWise domain might take a while.

Post Office Overrides

At the post office level, you can override the preferred Internet domain name, preferred address format, and allowed address formats the post office has inherited from its domain. You cannot override the GWIA that is assigned to handle outbound messages.

- 1 In ConsoleOne, right-click a Post Office object, then click *Properties*.
- 2 Click *GroupWise* > *Internet Addressing*.



- 3 To override one of the options, select the *Override* box, then select the option you prefer for this post office.

If you need additional information about any of the fields, click *Help*.

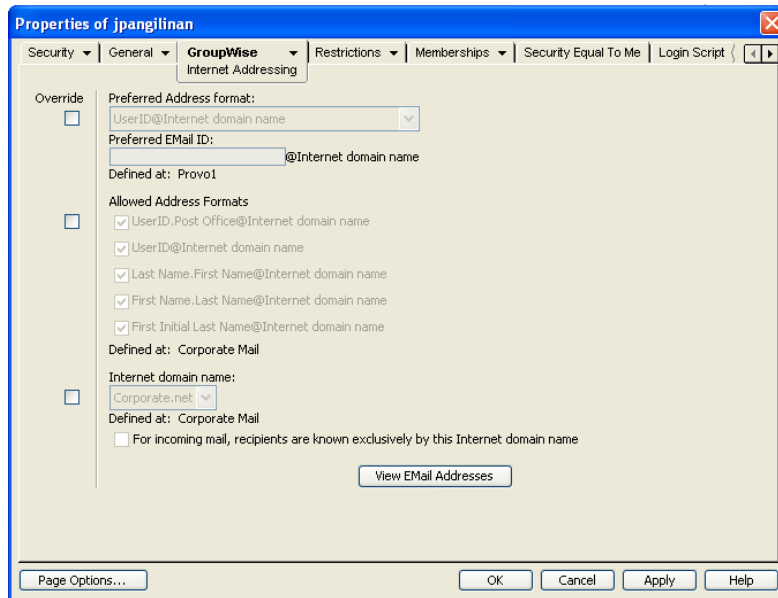
- 4 Click *OK* to save the changes.

If you changed the preferred address format, you are prompted to update the Internet email address (User object > *General* > *Identification* > *E-Mail Address*) for all affected users. The Internet email address is the address returned in response to LDAP queries to eDirectory. We recommend that you allow this update; however, performing it for an entire GroupWise post office might take a while.

User/Resource Overrides

At the user and resource level, you can override the preferred Internet domain, preferred address format, and allowed address formats that the user/resource has inherited from its post office. You cannot override the GWIA that is assigned to handle outbound messages.

- 1 In ConsoleOne, right-click a User or Resource object, then click *Properties*.
- 2 Click *GroupWise > Internet Addressing*.



- 3 To override one of the options, select the *Override* box, then select the option you prefer for this user or resource.

At the user and resource level, the preferred address format can be completely overridden by explicitly defining the user portion of the address format (*user@Internet domain name*). The user portion can include any RFC-compliant characters (no spaces, commas, and so on).

For example, if you have selected *First Name.Last Name@Internet domain name* as your system's preferred address format and you have two John Petersons, each on a different post office in your system, you would end up two users having the same address (John.Peterson@novell.com). You could use this field to differentiate them by including their middle initials in their address (John.S.Peterson@novell.com and John.A.Peterson@novell.com).

You can use the same email ID for more than one user in your GroupWise system, if each user is in a different Internet domain. Rather than requiring that each email ID be unique in your GroupWise system, each combination of email ID and Internet domain must be unique. This provides more flexibility for handling the situation where two people have the same name.

If you need additional information about any of the fields, click *Help*.

- 4 Click *OK* to save the changes.

If you changed the preferred address format for a user, you are prompted to update the user's Internet email address (*General > Identification > E-Mail Address*). The Internet email address is the address returned in response to LDAP queries to eDirectory. We recommend that you allow this update.

52.3 Transitioning from SMTP Gateway Aliases to Internet Addressing

For those who have been using SMTP gateway aliases to handle email addresses that do not fit the default format expected by the GWIA or to customize users' Internet addresses, the Gateway Alias Migration utility can convert the user names in those gateway aliases into preferred email IDs. The Preferred E-Mail ID feature was first introduced in GroupWise 6.5 and is the suggested method for overriding the current email address format, as described in [Section 14.7.2, "Changing a User's Internet Addressing Settings,"](#) on page 249. The Gateway Alias Migration utility can also update users' preferred Internet domain names based on their existing gateway aliases.

- ♦ [Section 52.3.1, "Planning to Migrate Gateway Aliases,"](#) on page 754
- ♦ [Section 52.3.2, "Preparing to Migrate Gateway Aliases,"](#) on page 754
- ♦ [Section 52.3.3, "Performing the Gateway Alias Migration,"](#) on page 754
- ♦ [Section 52.3.4, "Verifying the Gateway Alias Migration,"](#) on page 756

52.3.1 Planning to Migrate Gateway Aliases

You can migrate SMTP gateway aliases by individual user, by post office, by domain, or for your entire GroupWise system. Migrating at the post office level is recommended, although you can test the process by migrating individual users. Assess the gateway aliases in your GroupWise system and decide how you want to organize the migration process.

The Gateway Alias Migration utility runs most efficiently if you are connected to the domain that owns the users whose aliases you are migrating. This reduces network traffic between domains during the migration process.

The Gateway Alias Migration utility requires that you connect to a GroupWise 7 or later domain, although you can select users from 6.x and 5.x domains for migration. If you still have 4.x domains, you can migrate aliases by connecting to the GroupWise System object before connecting to a domain.

Determine the domains you need to connect to as you perform the migration.

52.3.2 Preparing to Migrate Gateway Aliases

Before starting the SMTP gateway alias migration process:

- ♦ Validate each domain database (`wpdomain.db`) that you will connect to in order to clean up any orphaned aliases that might exist. See [Section 26.1, "Validating Domain or Post Office Databases,"](#) on page 401.
- ♦ Create a current backup of each domain database before performing the migration. See [Section 31.1, "Backing Up a Domain,"](#) on page 431

52.3.3 Performing the Gateway Alias Migration

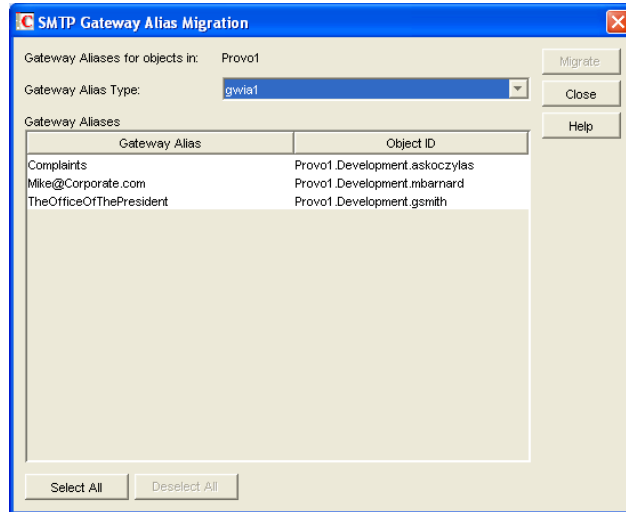
To run the Gateway Alias Migration utility in ConsoleOne:

- 1 (Conditional) If you want to migrate all gateway aliases in your GroupWise system, connect to the primary domain in the GroupWise View.
or

(Conditional) If you want to migrate the gateway aliases in a particular domain or post office, connect to the domain where the aliases are located.

If you need assistance with this task in a GroupWise system that includes domains on Linux servers, see [Section 4.1, "Select Domain,"](#) on page 69.

- 2 Browse to and select the object representing the set of gateway aliases that you want to migrate (GroupWise system, domain, post office, or user).
- 3 Click *Tools > GroupWise Utilities > Gateway Alias Migration*.
- 4 In the *SMTP Gateway Alias Type* drop-down list, select the type of alias you want to migrate.



The list of available gateway alias types is generated from the *Gateway Alias Type* fields on the Identification property pages of the GWIA objects in your GroupWise system.

The resulting alias list provides the SMTP gateway aliases for all users associated with the object selected in [Step 2](#). If the list is extremely long, you can click *Stop* and just work with a subset of the alias list.

The list does not include any aliases that have a pending operation on them.

- 5 Select one or more gateway aliases to migrate.

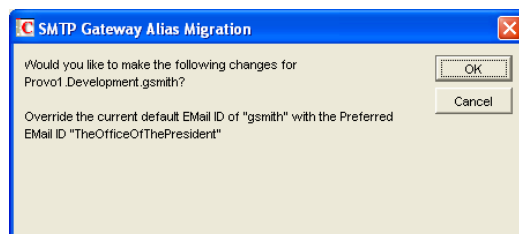
or

Click *Select All*.

- 6 Click *Migrate* to start the migration process.

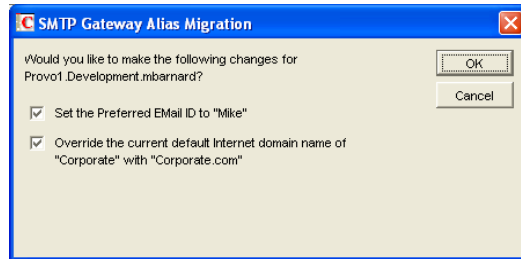
You are prompted for how to handle each gateway alias.

- ♦ If the alias is just a user name, you can select whether or not you want to use that user name as the user's preferred email ID.



If you do, the user name is transferred into the *Preferred E-Mail ID* field on the Internet Addressing property page of the User object.

- ◆ If the alias also includes an Internet domain name, you can select whether or not you want to use that Internet domain name with the user's preferred email ID.



If you do, the domain name is transferred into the *Internet Domain Name* field on the Internet Addressing property page of the User object.

For an internal user, if the Internet domain name is not defined in your GroupWise system under *Tools > GroupWise System Operations > Internet Addressing*, then the Internet domain name is not transferred into the *Internet Domain Name* field on the Internet Addressing property page of the User object. However, for external users, undefined Internet domain names are transferred into the *Internet Domain Name* field on the Internet Addressing property page of the External User or External Entity object.

By default, both user names and domain names are selected for migration.

- 7 For each gateway alias, deselect the check boxes for any actions that you do not want the Alias Migration utility to perform, then click *OK*.

For convenience when migrating multiple aliases, you can click *OK to All* to apply your current selections to all aliases.

- 8 When the migration is complete, select a different gateway alias type to migrate.

or

Click *Close*.

52.3.4 Verifying the Gateway Alias Migration

To see what the Gateway Alias Migration utility has accomplished:

- 1 Browse to and right-click a User object that used to have a gateway alias, then click *Properties*.
- 2 Click *GroupWise > Gateway Aliases*.
The alias list should be empty.
- 3 On the same User object, click *GroupWise > Internet Addressing*.

The *Preferred EMail ID* field should be filled in with the information from the old gateway alias.

53 Configuring Internet Services

For detailed instructions about installing and starting the GWIA for the first time, see [“Installing the GroupWise Internet Agent”](#) in the *GroupWise 2012 Installation Guide*.

The GWIA offers several useful services that you can configure to meet the needs of your GroupWise system.

- ♦ [Section 53.1, “Configuring SMTP/MIME Services,”](#) on page 757
- ♦ [Section 53.2, “Configuring POP3/IMAP4 Services,”](#) on page 777
- ♦ [Section 53.3, “Configuring LDAP Services,”](#) on page 782
- ♦ [Section 53.4, “Configuring Paging Services,”](#) on page 785

53.1 Configuring SMTP/MIME Services

SMTP and MIME are standard protocols that the GWIA uses to send and receive email messages over the Internet. SMTP, or Simple Mail Transfer Protocol, is the message transmission protocol. MIME, or Multipurpose Internet Mail Extension, is the message format protocol. Choose from the following topics for information about how to enable SMTP/MIME services and configure various SMTP/MIME settings:

- ♦ [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,”](#) on page 757
- ♦ [Section 53.1.2, “Using Extended SMTP \(ESMTP\) Options,”](#) on page 760
- ♦ [Section 53.1.3, “Configuring How the GWIA Handles Email Addresses,”](#) on page 761
- ♦ [Section 53.1.4, “Determining Format Options for Messages,”](#) on page 763
- ♦ [Section 53.1.5, “Configuring the SMTP Timeout Settings,”](#) on page 765
- ♦ [Section 53.1.6, “Determining What to Do with Undeliverable Messages,”](#) on page 766
- ♦ [Section 53.1.7, “Configuring SMTP Dial-Up Services,”](#) on page 767
- ♦ [Section 53.1.8, “Enabling SMTP Relaying,”](#) on page 770
- ♦ [Section 53.1.9, “Using a Route Configuration File,”](#) on page 772
- ♦ [Section 53.1.10, “Customizing Delivery Status Notifications,”](#) on page 773
- ♦ [Section 53.1.11, “Managing MIME Messages,”](#) on page 773

53.1.1 Configuring Basic SMTP/MIME Settings

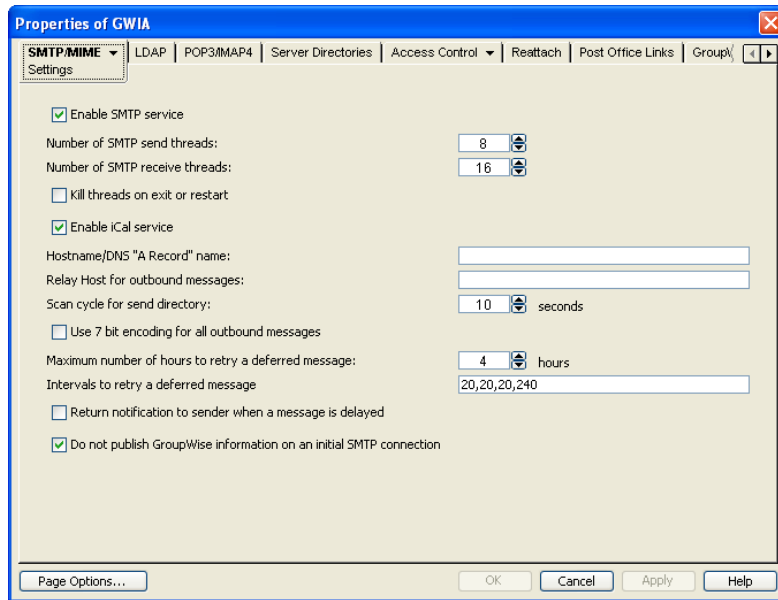
Basic SMTP/MIME settings configure the following aspects of GWIA functioning:

- ♦ Number of send and receive threads that the GWIA starts and how often the send threads poll for outgoing messages
- ♦ Hostname of the server where the GWIA is running and of a relay host if your system includes one

- ♦ IP address to bind to at connection time if the server has multiple IP addresses
- ♦ Whether to use 7-bit or 8-bit encoding for outgoing messages
- ♦ How to handle messages that cannot be sent immediately and must be deferred
- ♦ Whether to notify senders when messages are delayed
- ♦ Whether to display GroupWise version information when establishing an SNMP connection

To set the GWIA basic SMTP/MIME settings:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 If the SMTP/MIME Settings page is not the default page, click *SMTP/MIME > Settings*.



- 3 Fill in the fields:

Enable SMTP Service: SMTP service is on by default. This setting allows SMTP Internet messaging. This setting corresponds with the GWIA's `--smtp` switch.

Number of SMTP Send Threads: The SMTP send threads setting lets you specify the number of threads that process SMTP send requests. Each thread is equivalent to one connection. The default is 8 threads. This setting corresponds with the GWIA's `--sd` switch.

Number of SMTP Receive Threads: The SMTP receive threads setting lets you specify the number of threads that process SMTP receive requests. Each thread is equivalent to one connection. The default is 16 threads. This setting corresponds with the GWIA's `--rd` switch.

Kill Threads on Exit or Restart: Select this option to cause the GWIA to stop immediately, without allowing its send/receive threads to perform their normal shutdown procedures. The normal termination of all send/receive threads can take several minutes, especially if a large message is being processed. By terminating immediately, a needed restart can occur immediately as well. This setting corresponds with the GWIA's `--killthreads` switch.

Enable iCal Service: Select this option if you want the GWIA to convert outbound GroupWise Calendar items into MIME text/calendar *iCal* objects and to convert incoming MIME text/calendar messages into GroupWise Calendar items. Enabling the iCal service provides the functionality described in "Accepting or Declining Internet Items" in "Calendar" in the *GroupWise 2012 Windows Client User Guide*. This setting corresponds with the GWIA's `--imip` switch.

Hostname/DNS "A Record" Name: The Hostname/DNS "A Record" name setting lets you identify the hostname of the server where the GWIA resides, or in other words the A Record in your DNS table that associates a hostname with the server's IP address (for example, gwia.novell.com). This setting corresponds with the GWIA's `--hn` switch.

If you leave this field blank, the GWIA uses the hostname obtained by querying the hosts file from the server.

Relay Host for Outbound Messages: The relay host setting can be used if you want to use one or more relay hosts to route all outbound Internet email. Specify the IP address or DNS hostname of the relay hosts. Use a space between relay hosts in a list. Relay hosts can be part of your network or can reside at the Internet service provider's site. This setting corresponds with the GWIA's `--mh` switch.

If you want to use a relay host, but you want some outbound messages sent directly to the destination host rather than to the relay host, you can use a route configuration file (`route.cfg`). Whenever a message is addressed to a user at a host that is included in the `route.cfg` file, the GWIA sends the message directly to the host rather than to the relay host. For information about creating a `route.cfg` file, see [Section 53.1.9, "Using a Route Configuration File," on page 772](#).

Scan Cycle for Send Directory: The Scan cycle setting specifies how often the GWIA polls for outgoing messages. The default is 10 seconds. This setting corresponds with the GWIA's `--p` switch.

Use 7 Bit Encoding for All Outbound Messages: By default, the GWIA uses 8-bit MIME encoding for any outbound messages that are HTML-formatted or that contain 8-bit characters. If, after connecting with the receiving SMTP host, the GWIA discovers that the receiving SMTP host cannot handle 8-bit MIME encoded messages, the GWIA converts the messages to 7-bit encoding.

With this option selected, the GWIA automatically uses 7-bit encoding and does not attempt to use 8-bit MIME encoding. You should use this option if you are using a relay host that does not support 8-bit MIME encoding. This setting corresponds with the GWIA's `--force7bitout` switch.

Maximum Number of Hours to Retry a Deferred Message: Specify the number of hours after which the GWIA stops trying to send deferred messages. The default is 96 hours (four days). A deferred message is any message that can't be sent because of a temporary problem (host down, MX record not found, and so on). This setting corresponds with the GWIA's `--maxdeferhours` switch.

Intervals to Retry a Deferred Message: Specify in a comma-delimited list the number of minutes after which the GWIA retries sending deferred messages. The default is 20, 20, 20, 60. The GWIA interprets this list as follows: It retries 20 minutes after the initial send, 20 minutes after the first retry, 20 minutes after the second retry, and 60 minutes (1 hour) after the third retry. Thereafter, it retries every hour until the number of hours specified in the *Maximum Number of Hours to Retry a Deferred Message* field is reached. You can provide additional retry intervals as needed. It is the last retry interval that repeats until the maximum number of hours is reached. This setting corresponds with the GWIA's `--msgdeferinterval` switch.

Return Notification to Sender When a Message Is Delayed: Select this option to provide a notification message to users whose email messages cannot be immediately sent out across the Internet. This provides more noticeable notification to users than manually checking the Properties page of the sent item to see whether it has been sent. This setting corresponds with the GWIA's `--delayedmsgnotification` switch.

Do Not Publish GroupWise Information on an Initial SMTP Connection: This option suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by another SMTP host or a telnet session. It is enabled by default. This setting corresponds with the GWIA's `--nosmtpversion` switch.

- 4 Click OK to save the changes.

53.1.2 Using Extended SMTP (ESMTP) Options

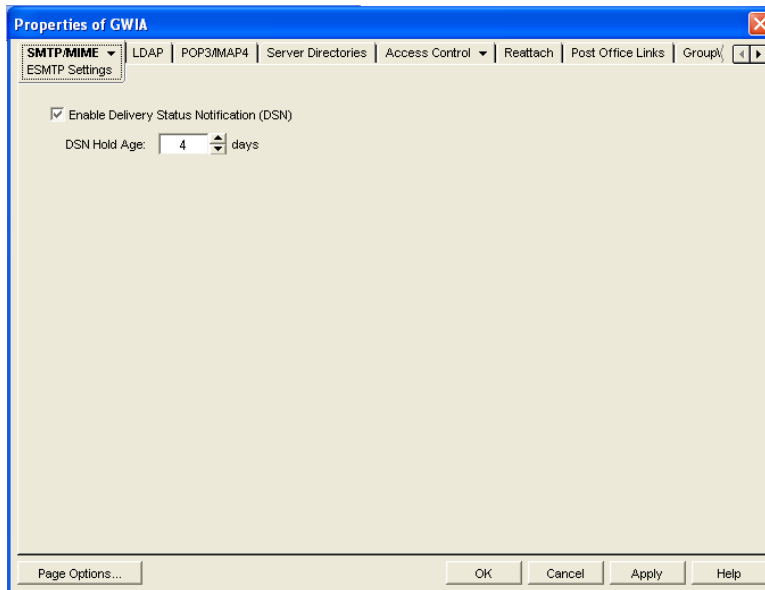
The GWIA supports several Extended SMTP (ESMTP) settings. These are settings that might or might not be supported by another SMTP system.

The following ESMTP extensions are supported:

- ♦ **SIZE:** For more information, see [RFC 1870](http://www.ietf.org/rfc/rfc1870.txt) (<http://www.ietf.org/rfc/rfc1870.txt>).
- ♦ **AUTH:** For more information, see [RFC 2554](http://www.ietf.org/rfc/rfc2554.txt) (<http://www.ietf.org/rfc/rfc2554.txt>).
- ♦ **DSN:** For more information, see [RFC 3464](http://www.ietf.org/rfc/rfc3464.txt) (<http://www.ietf.org/rfc/rfc3464.txt>) and [RFC 3461](http://www.ietf.org/rfc/rfc3461.txt) (<http://www.ietf.org/rfc/rfc3461.txt>).
- ♦ **8BITMIME:** For more information, see [RFC 1652](http://www.ietf.org/rfc/rfc1652.txt) (<http://www.ietf.org/rfc/rfc1652.txt>).
- ♦ **STARTTLS:** For more information, see [RFC 3207](http://www.ietf.org/rfc/rfc3207.txt) (<http://www.ietf.org/rfc/rfc3207.txt>).

To configure ESMTP settings:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > ESMTP Settings*.



- 3 Fill in the fields:

Enable Delivery Status Notification: Turn on this option to allow the GWIA to request status notifications for outgoing messages and to supply status notifications for incoming messages. This requires the external email system to also support *Delivery Status Notification*. Currently, notification consists of two delivery statuses: successful or unsuccessful.

If you enable the *Delivery Status Notification* option, you need to select the number of days that you want the GWIA to retain information about the external sender so that status updates can be delivered to him or her. For example, the default hold age causes the sender information to be retained for 4 days. If the GWIA does not receive delivery status notification from the GroupWise recipient's Post Office Agent (POA) within that time period, it deletes the sender information and the sender does not receive any delivery status notification.

If you enable this option for the GWIA, it overrides what GroupWise Windows client users set under *Tools > Options > Send > Mail > Send Notification to My Mailbox*. By default, this option is deselected in the GroupWise Windows client, but if you select *Enable Delivery Status Notification* in ConsoleOne, users receive delivery status notifications in their mailboxes even when the option is deselected in the Windows client.

- 4 Click *OK* to save the changes.

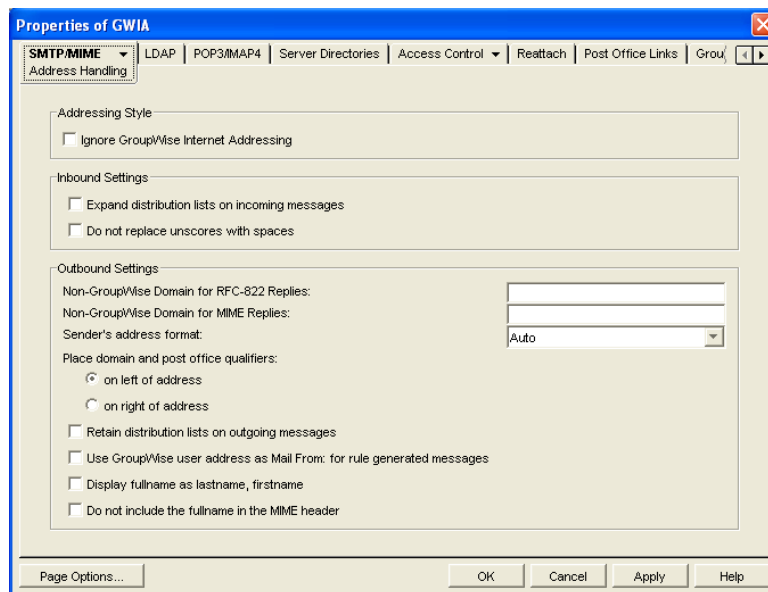
53.1.3 Configuring How the GWIA Handles Email Addresses

The GWIA can handle email addresses in a variety of ways:

- ♦ Internet addressing vs. GroupWise proprietary addressing
- ♦ Group membership expansion on inbound messages
- ♦ Distribution membership expansion on outbound messages
- ♦ Using non-GroupWise domains
- ♦ Using sender's address format
- ♦ Using domain and post office information

To set the GWIA address handling options:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Address Handling*.



- 3 Fill in the fields:

Ignore GroupWise Internet Addressing: GroupWise supports both Internet-style addressing (*user@host*) and GroupWise proprietary addressing (*user_ID.post_office.domain*). By default, the GWIA uses Internet-style addressing.

If you do not want the GWIA to use standard Internet-style addressing (*user@host*), turn on the *Ignore GroupWise Internet Addressing* option. With this option turned on, messages use the mail domain name in the *Foreign ID* field (GWIA object > *GroupWise > Identification*) for the domain

portion of a user's Internet address. If you included multiple mail domain names in the *Foreign ID* field or the `frgnames.cfg` file, as described in "Listing Foreign Domain Names" on page 763, the first mail domain name listed is the one used in addresses.

The GWIA supports user and post office aliases in either mode. This setting corresponds with the GWIA's `--dia` switch.

Expand Distribution Lists on Incoming Messages: Turn on this option to have incoming Internet messages addressed to a distribution list sent to all members of the distribution list. This setting corresponds with the GWIA's `--group` switch. See also the `--nickgroup` switch to turn on distribution list expansion for distribution lists that have nicknames.

Do Not Replace Underscores with Spaces: Select this option if you do not want the GWIA to convert user names in email addresses from the format `Firstname_Lastname` into the format `Firstname Lastname` by replacing the underscore with a space. By default, this conversion takes place automatically, even though `Firstname_Lastname` is not an address format that is included in the *Allowed Address Formats* list in the Internet Addressing dialog box, as described in Section 52.2.2, "Enabling Internet Addressing," on page 748. This setting corresponds with the GWIA's `--dontreplaceunderscore` switch.

Non-GroupWise Domain for RFC-822 Replies: This setting can be used only if 1) you created a non-GroupWise domain to represent all or part of the Internet, as described in Section 6.8, "Adding External Users to the GroupWise Address Book," on page 116, and 2) you defined the non-GroupWise domain's outgoing conversion format as RFC-822 when you linked the GWIA to the domain.

Specify the name of the non-GroupWise domain associated with the RFC-822 conversion format. When a GroupWise user replies to a message that was originally received by the GWIA in RFC-822 format, the reply is sent to the specified non-GroupWise domain and converted to RFC-822 format so that it is in the same format as the original message.

This setting corresponds with the GWIA's `--fd822` switch.

Non-GroupWise Domain for MIME Replies: This setting can be used only if 1) you created a non-GroupWise domain that represents all or part of the Internet, as described in Section 6.8, "Adding External Users to the GroupWise Address Book," on page 116, and 2) you defined the non-GroupWise domain's outgoing conversion format as MIME when you linked the GWIA to the domain.

Specify the name of the non-GroupWise domain associated with the MIME conversion format. When a GroupWise user replies to a message that was originally received by the GWIA in MIME format, the reply is sent to the specified non-GroupWise domain and converted to MIME format so that it is in the same format as the original message.

This setting corresponds with the GWIA's `--fdmime` switch.

Sender's Address Format: This setting applies only if you have not enabled GroupWise Internet addressing (in other words, you selected the *Ignore GroupWise Internet Addressing* option). If GroupWise Internet addressing is enabled, the GWIA ignores this setting and uses the preferred address format established for outbound messages (*Tools > GroupWise System Operations > Internet Addressing*).

The Sender's Address Format setting lets you specify which GroupWise address components (`domain.post_office.user_ID`) are included as the user portion of the address on outbound messages. You can choose from the following options:

- ◆ **Domain, Post Office, User, and Hostname:** Uses the `domain.post_office.user_ID@host` syntax.
- ◆ **Post Office, User, and Hostname:** Uses the `post_office.user_ID@host` syntax.
- ◆ **User and Hostname:** Uses the `user_ID@host` syntax.

- ♦ **Auto (default):** Uses the GroupWise addressing components required to make the address unique within the user's GroupWise system. If a user ID is unique in a GroupWise system, the outbound address uses only the user ID. If the post office or domain.post office components are required to make the address unique, these components are also included in the outbound address.

The Sender's Address Format setting corresponds with the GWIA's `--aql` switch.

Place Domain and Post Office Qualifiers: If the sender's address format must include the domain and/or post office portions to be unique, you can use this option to determine where the domain and post office portions are located within the address.

- ♦ **On Left of Address (default):** Leaves the domain and post office portions on the left side of the @ sign (for example, `domain.post_office.user_ID@host`).
- ♦ **On Right of Address:** Moves the domain and post office portions to the right side of the @ sign, making the domain and post office part of the host portion of the address (for example, `user_ID@post_office.domain.host`). If you choose this option, you must ensure that your DNS server can resolve each `post_office.domain.host` portion of the address. This setting corresponds with the GWIA's `--aqor` switch.

Retain Distribution Lists on Outgoing Messages: Select this option if you do not want the GWIA to expand distribution lists on messages going to external Internet users. Expansion of distribution lists can result in large SMTP headers on outgoing messages. This setting corresponds with the GWIA's `--keepsendgroups` switch.

Use GroupWise User Address as Mail From: for Rule Generated Messages: Select this option if you want the GWIA to use the real user in the *Mail From* field instead of having auto-forwards come from Postmaster and auto-replies come from Mailer-Daemon. This setting corresponds with the GWIA's `--realmailfrom` switch.

- 4 Click OK to save the changes.

Listing Foreign Domain Names

The *Foreign ID* field (GWIA object > *GroupWise* > *Identification*) identifies the Internet domain names for which the GWIA accepts messages. The field should always include your mail domain name (for example, `novell.com`). You can include additional domain names by separating them with a space, as in the following example:

```
novell.com gw.novell.com gwia.novell.com
```

When you list multiple Internet domain names, the GWIA accepts messages for a GroupWise user if any of the Internet domain names are used (for example, `jsmith@novell.com`, `jsmith@gw.novell.com`, or `jsmith@gwia.novell.com`).

The field limit is 255 characters. If you need to exceed that limit, you can create a `frgnames.cfg` text file in the `domain\wpgate\gwia` directory. List each Internet domain name on a separate line.

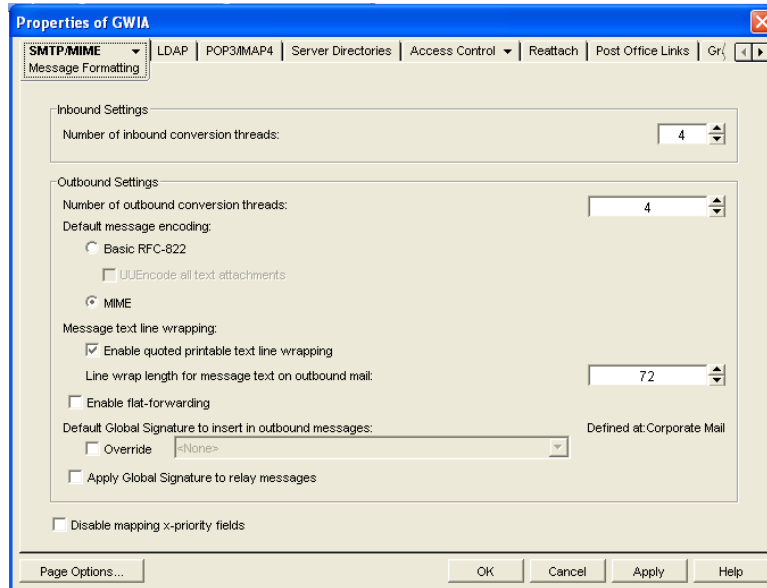
53.1.4 Determining Format Options for Messages

You can control aspects of how the GWIA formats incoming and outgoing messages:

- ♦ Number of GWIA threads for converting messages into the specified format
- ♦ The view in which incoming messages are displayed to GroupWise users
- ♦ Text encoding method (Basic RFC-822 or MIME)
- ♦ Text wrapping
- ♦ Message prioritization based on x-priority fields

To set the GWIA format options:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Message Formatting*.



- 3 Fill in the fields:

Number of Inbound Conversion Threads: The inbound conversion threads setting lets you specify the number of threads that convert inbound messages from MIME or RFC-822 format to the GroupWise message format. The default setting is 4. This setting corresponds with the GWIA's `--rt` switch.

Number of Outbound Conversion Threads: The outbound conversion threads setting lets you specify the number of threads that convert outbound messages from the GroupWise message format to MIME or RFC-822 format. The default setting is 4. This setting corresponds with the GWIA's `--st` switch.

Default Message Encoding: The default message encoding setting lets you select the encoding method for your outbound Internet messages. You can select either *Basic RFC-822* formatting or *MIME* formatting. *MIME* is the default message format. This setting corresponds with the GWIA's `--mime` switch.

If you select the *Basic RFC-822* option, you can decide whether or not to have the GWIA UUEncode all ASCII text attachments to RFC-822 formatted messages. By default, this option is turned off, which means ASCII text attachments are included as part of the message body. This setting corresponds with the GWIA's `--ueea` switch.

NOTE: RFC-822 is a very old format. Use it only if you have a specific need for it.

Message Text Line Wrapping: The *Quoted Printable* text line wrapping setting lets you select the Quoted Printable MIME standard for line wrapping, which provides "soft returns". By default this setting is turned on. If you turn the setting off, MIME messages go out as plain text and wrap text with "hard returns" according to the number of characters specified in the line wrap length setting. This setting corresponds with the GWIA's `--nqpmt` switch.

The *Line Wrap Length for Message Text on Outbound Mail* setting lets you specify the line length for outgoing messages. This is useful if the recipient's email system requires a certain line length. The default line length is 72 characters. This setting corresponds with the GWIA's `--wrap` switch.

Enable Flat Forwarding: Select this option to automatically strip out the empty message that is created when a message is forwarded without adding text, and retain the original sender of the message, rather than showing the user who forwarded it. This facilitates users forwarding messages from GroupWise to other email accounts. Messages arrive in the other accounts showing the original senders, not the users who forwarded the messages from GroupWise. This setting corresponds with the GWIA's `--flatfwd` switch.

Default Global Signature to Insert in Outbound Messages: Displays the default global signature for your GroupWise system as described in [Section 14.3.2, "Selecting a Default Global Signature for All Outgoing Messages,"](#) on page 232. If you want this GWIA to append a different global signature, select *Override*, then select the desired signature.

Apply Global Signature to Relay Messages: Select this option to append the global signature to messages that are relayed through your GroupWise system (for example, messages from POP and IMAP clients) in addition to messages that originate within your GroupWise system. This setting corresponds with the GWIA's `--relayaddsignature` switch.

Disable Mapping X-Priority Fields: Select this option to disable the function of mapping an x-priority MIME field to a GroupWise priority for the message. By default, the GWIA maps x-priority 1 and 2 messages as high priority, x-priority 3 messages as normal priority, and x-priority 4 and 5 as low priority in GroupWise. This setting corresponds with the GWIA's `--nomappriority` switch.

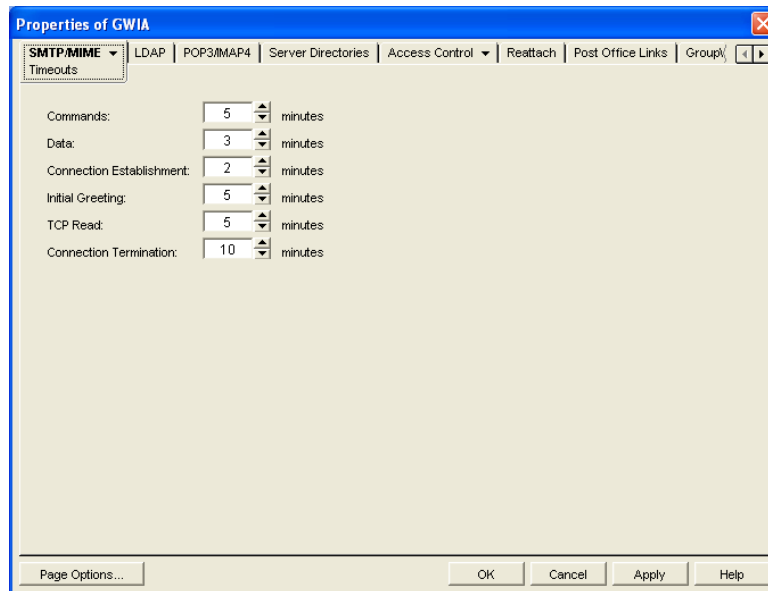
- 4 Click *OK* to save the changes.

53.1.5 Configuring the SMTP Timeout Settings

The SMTP Timeout settings specify how long the GWIA's SMTP service waits to receive data that it can process. After the allocated time expires, the GWIA might give a TCP read/write error.

To configure the SMTP timeout settings:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Timeouts*.



- 3 Fill in the fields:

Commands: The *Commands* setting lets you specify how long the GWIA waits for an SMTP command. The default is 5 minutes. This setting corresponds with the GWIA's `--tc` switch.

Data: The *Data* setting lets you specify how long the GWIA waits for data from the receiving host. The default is 3 minutes. This setting corresponds with the GWIA's `--td` switch.

Connection Establishment: The *Connection Establishment* setting lets you specify how long the GWIA waits for the receiving host to establish a connection. The default is 2 minutes. This setting corresponds with the GWIA's `--te` switch.

Initial Greeting: The *Initial Greeting* setting lets you specify how long the GWIA waits for the initial greeting from the receiving host. The default is 5 minutes. This setting corresponds with the GWIA's `--tg` switch.

TCP Read: The *TCP Read* setting lets you specify how long the GWIA waits for a TCP read. The default is 5 minutes. This setting corresponds with the GWIA's `--tr` switch.

Connection Termination: The *Connection Termination* setting lets you specify how long the GWIA waits for the receiving host to terminate the connection. The default is 10 minutes. This setting corresponds with the GWIA's `--tt` switch.

- 4 Click *OK* to save the changes.

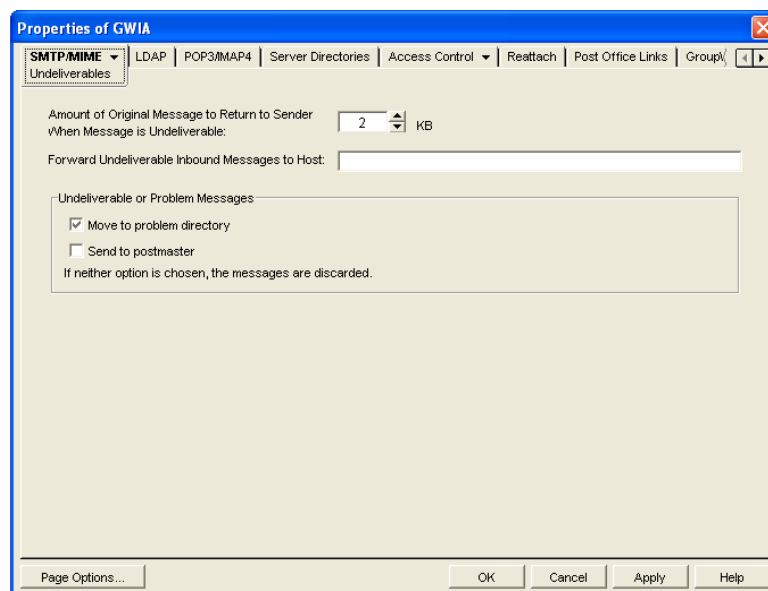
53.1.6 Determining What to Do with Undeliverable Messages

You can configure how the GWIA handles messages that it cannot deliver:

- How much of the message to return to the sender
- Another host to forward the message to (where it might be deliverable)
- Whether to move the message to the GroupWise problem directory or send it to the GroupWise administrator

To set the GWIA undeliverable message options:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Undeliverables*.



- 3 Fill in the fields:

Amount of Original Message to Return to Sender When Message is Undeliverable: This setting lets you specify how much of the original message is sent back to the sender when a message is undeliverable. By default, only 2 KB of the original message is sent back. This setting corresponds with the GWIA's `--mudas` switch.

Forward Undeliverable Inbound Messages to Host: This setting lets you specify a host to which undeliverable messages are forwarded.

When an IP address is specified rather than a DNS hostname, the IP address must be surrounded by square brackets []. For example, [172.16.5.18].

This setting corresponds with the GWIA's `--fut` switch.

Undeliverable or Problem Messages: This setting lets you specify what you want the GWIA to do with problem messages. A problem message is an inbound or outbound message that the GWIA cannot convert properly. By default, problem messages are discarded. If you want to save problem messages, specify whether to move the messages to the problem directory (`gwprob`), send them to the postmaster, or do both. This setting corresponds with the GWIA's `--badmsg` switch.

IMPORTANT: Despite the field name (*Undeliverable or Problem Messages*), this setting does not apply to undeliverable messages.

- 4 Click *OK* to save the changes.

53.1.7 Configuring SMTP Dial-Up Services

SMTP dial-up services can be used when you don't require a permanent connection to the Internet and want to periodically check for mail messages queued for processing. Perform the following tasks in order to use SMTP dial-up services:

- ♦ ["Setting up Internet Dial-Up Software" on page 767](#)
- ♦ ["Enabling Dial-Up Services" on page 767](#)
- ♦ ["Creating a Dial-Up Schedule" on page 768](#)

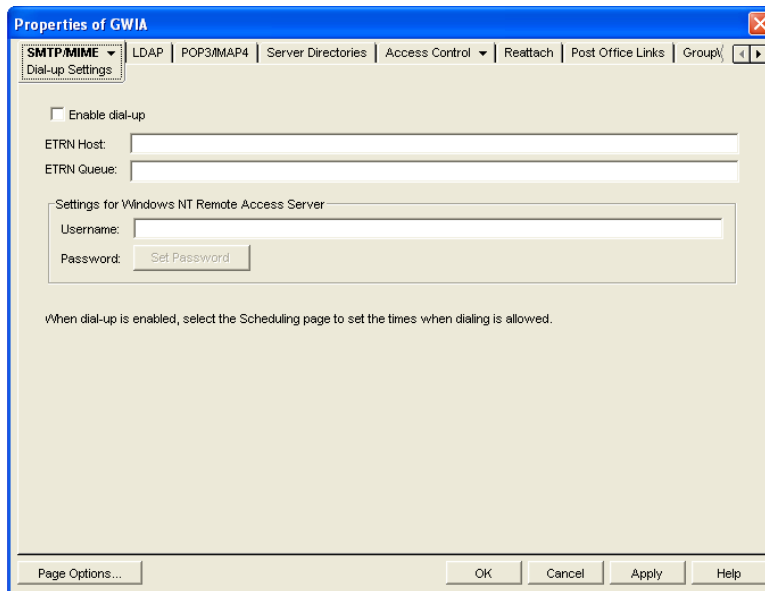
Setting up Internet Dial-Up Software

The GWIA requires routing software to make the dial-up connection to the Internet. The GWIA cannot make this connection itself; it simply creates packets to hand off to the routing software.

Enabling Dial-Up Services

After you have the appropriate routing software in place, you can enable and configure the GWIA's dial-up services.

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Dial-Up Settings*.



3 Fill in the fields:

Enable Dial-Up: Turn on this option to allow the GWIA to support SMTP dial-up service. This option is off by default. This setting corresponds with the GWIA's `--usedialup` switch.

ETRN Host: Specify the IP address, or DNS hostname, of the mail server (where your mail account resides) at your Internet Service Provider. You should obtain this address from your Internet Service Provider. This setting corresponds with the GWIA's `--etrnhost` switch.

ETRN Queue: Specify your email domain as provided by your Internet Service Provider (for example, novell.com). This setting corresponds with the GWIA's `--etrnqueue` switch.

Username: The *Username* setting applies only if you are using a Windows Remote Access Server (RAS) and the GWIA is not running on the same server as the RAS.

Specify the RAS Security user name. This setting corresponds with the GWIA's `--dialuser` switch.

Password: The *Password* setting applies only if you are using a Windows Remote Access Server (RAS) and the GWIA is not running on the same server as the RAS.

Specify the RAS Security user's password. This setting corresponds with the GWIA's `--dialpass` switch.

4 Click OK to save the changes.

Creating a Dial-Up Schedule

After you enable the GWIA to use a dial-up connection, you need to schedule the times when the GWIA initiates a connection.

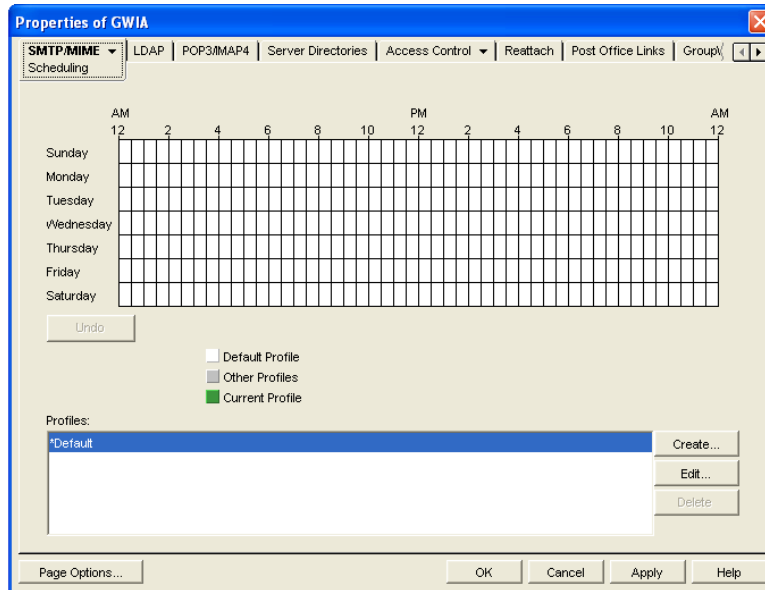
NOTE: When the GWIA initiates a connection, it simply passes TCP/IP packets to the routing service that makes the Internet connection. The routing software, not the GWIA, is responsible for the actual dial-up or timeout.

The GWIA uses profiles to enable you to assign different dial-up criteria to different times. For example, the default profile instructs the GWIA to initiate a dial-up connection whenever an outgoing message is placed in its send queue. However, during the night, you might want the GWIA

to initiate a connection only after 30 outgoing messages have been queued. In this case, you could create a profile that requires 30 messages to be queued and then apply the profile between the hours of 11 p.m. and 7 a.m. each day.

To create a dial-up schedule:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Scheduling*.



- 3 Continue with the desired task:
 - ◆ [“Applying a Profile” on page 769](#)
 - ◆ [“Creating a Profile” on page 769](#)
 - ◆ [“Editing a Profile” on page 770](#)
 - ◆ [“Deleting a Profile” on page 770](#)

Applying a Profile

- 1 Select the profile in the *Profiles* list.
- 2 Click the desired hour.
or
Drag to select multiple hours.
- 3 Click *Apply* to save the changes or click *OK* to save the changes and close the page.

Creating a Profile

- 1 Click *Create* to display the Create Profile dialog box.
- 2 Fill in the fields:
 - Name:** Specify a unique name for the profile. It must be different than any other name in the Profile list.
 - Description:** If desired, specify a description for the profile.

Queue Thresholds: The queue thresholds determine the criteria for the GWIA to initiate a dial-up connection to send messages. The settings do not apply to receiving messages (see [Dial Parameters](#) below).

You can base the criteria on the number of messages in the send queue, the total size of the messages in the send queue, or the number of minutes to wait between connections. If necessary, you can use a combination of the three criteria.

For example, if you set *Messages* to 20, *Kilobytes* to 100, and *Minutes* to 60, the GWIA instructs the routing service to initiate a dial-up connection when 20 messages have accumulated in the queue, when the total size of the messages in the queue reaches 100 K, or when 60 minutes have passed since the last connection.

Dial Parameters: The dial parameters serve two purposes: 1) the GWIA passes the Redial Interval and Idle Time Before Hangup parameters to the routing service to use when initiating a connection to send outbound messages, and 2) the GWIA uses the Polling Interval parameter to determine how often the routing service should initiate a connection to check for inbound messages. The Polling Interval parameter is required.

Specify the interval between redials (default is 30 seconds), the amount of time to wait before hanging up when there are no messages to process (default is 60 seconds), and the interval between polling for inbound messages (default is 0 minutes).

- 3 Click *OK* to add the profile to the Profiles list.
- 4 To apply the profile to a block of time, see [“Applying a Profile” on page 769](#).

Editing a Profile

- 1 Select the profile you want to edit, then click *Edit* to display the Edit Profile dialog box.
- 2 Modify the desired fields. For information about each of the fields, click the Help button in the Edit Profile dialog box or see [“Creating a Profile” on page 769](#).
- 3 Click *Apply* to save the changes or click *OK* to save the changes and close the page.

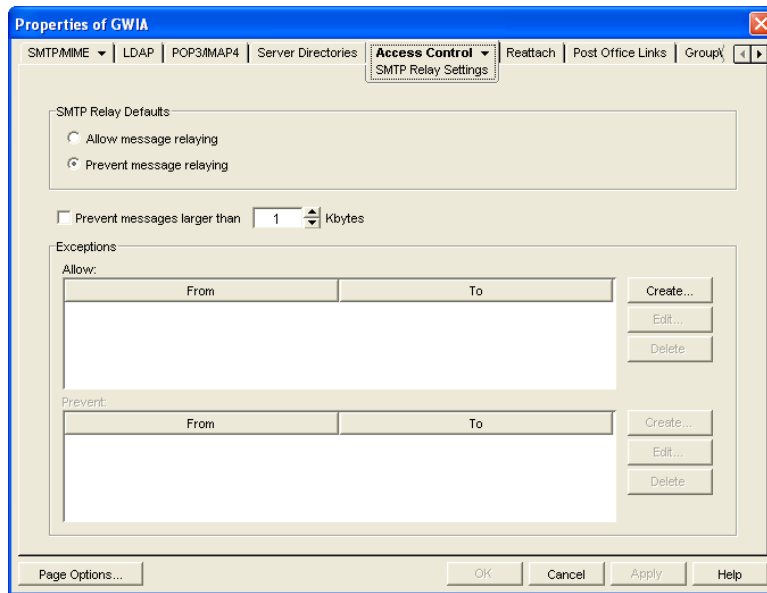
Deleting a Profile

- 1 Select the profile you want to remove from the list, then click *Delete*.
- 2 Click *Apply* to save the changes or click *OK* to save the changes and close the page.

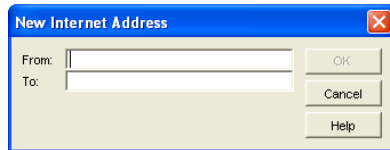
53.1.8 Enabling SMTP Relaying

You can enable the GWIA to function as a relay host for Internet messages. The GWIA can relay messages received from all Internet hosts, or you can select specific hosts for which you allow it to relay.

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *Access Control > SMTP Relay Settings*.



- 3 Under *SMTP Relay Defaults*, select whether you want to allow or prevent message relaying. If you prevent message relaying, you can define exceptions that allow message relaying for specific Internet hosts. This can also be done if you allow message relaying. We suggest that you select the option that enables you to define the fewest exceptions.
- 4 To prevent relaying of messages larger than a specific size (regardless of the *SMTP Relay Defaults* setting), enable the *Prevent Messages Larger Than* option and specify the size limitation.
- 5 To define an exception, click *Create* to display the New Internet Address dialog box.



- 6 Fill in the following fields:
 - From:** Specify the Internet address that must be in the message's *From* field for the exception to be applied.
 - To:** Specify the Internet address that must be in the message's *To* field for the exception to be applied. This is also the address that the message is relayed to (in the case of an Allow exception).
 In both the *From* and *To* fields, you can use either an IP address or a DNS hostname, as shown in the following examples:

novell.com
10.1.1.10

You can enter a specific address, as shown above, or you can use wildcards and IP address ranges to specify multiple addresses, as follows:

*.novell.com
10.1.1.*
10.1.1.10-15

NOTE: If the user for whom you want to define an exception has an alias, you must also define an exception for the user's alias. Ongoing use of aliases is not recommended. For more information, see [Section 5.14, "Gateway Alias Migration,"](#) on page 98.

- 7 Click *OK* to add the exception to the list.
- 8 When you are finished defining exceptions, click *OK* to save your changes.

53.1.9 Using a Route Configuration File

The GWIA supports the use of a route configuration file (`route.cfg`) to specify destination SMTP hosts. This can be useful in situations such as the following:

- ♦ You are using a relay host for outbound messages. However, you want some outbound messages sent directly to the destination host rather than the relay host. Whenever a message is addressed to a user at a host that is included in the `route.cfg` file, the GWIA sends the message directly to the destination host rather than the relay host.
- ♦ You need to send messages to SMTP hosts that are unknown to the public Domain Name Servers. The `route.cfg` file acts much like a hosts file to enable the GWIA to resolve addresses not listed in DNS.
- ♦ The GWIA uses external DNS servers but the server it is running on has an internal IP address. This prevents the GWIA from querying external DNS servers for its own internal domain names and receiving Host Down errors from the external DNS servers.
- ♦ You want to route messages through an SMTP host that checks for viruses (or performs some other task) before routing them to the destination host.

To set up a `route.cfg` file:

- 1 Create the `route.cfg` file as a text file in the `domain\wpgate\gwia` directory.
- 2 Add an entry for each SMTP host you want to send to directly. The entry format is:

```
hostname address
```

Replace *hostname* with a DNS hostname or an Internet domain name. Replace *address* with an alternative hostname or an IP address. For example:

```
novell.com gwia.novell.com  
unixbox [172.16.5.18]
```

If you use an IP address, it must be included in square brackets, as shown above.

To reference subdomains, place a period (.) in front of the domain name as a wildcard character. For example:

```
.novell.com gwia.novell.com
```

Make sure to include a hard return after the last entry.

- 3 Save the `route.cfg` file.
- 4 Restart the GWIA.

53.1.10 Customizing Delivery Status Notifications

The GWIA returns status messages for all outbound messages. For example, if a GroupWise user sends a message that the GWIA cannot deliver, the GWIA returns an undeliverable message to the GroupWise user.

By default, the GWIA uses internal status messages. However, you can override the internal status messages by using a `status.xml` file that includes the status messages you want to use.

- 1 Open the appropriate `statusxx.xml` file, located in the `domain\wpgate\gwia` directory.

The `domain\wpgate\gwia` directory includes a `statusxx.xml` file for each language included in the downloaded *GroupWise 2012* software image (for example, `statusus.xml`, `statusde.xml`, and `statusfr.xml`).

- 2 Make the modifications you want.

The following sample code shows the elements and default text of the Undeliverable Message status:

```
<STATUS_MESSAGE type="undeliverableMessage" xml:lang="en-US">
<SUBJECT>Message status - undeliverable</SUBJECT>
<MESSAGE_BODY>
<TEXT>\r\nThe attached file had the following undeliverable recipient(s):\r\n</
TEXT>
<RECIPIENT_LIST format="\t%s\r\n"
<SESSION_TRANSCRIPT>
<TEXT>\r\nTranscript of session follows:\r\n<TEXT>
</SESSION_TRANSCRIPT>
<ATTACH_ORIGINAL_MSG></ATTACH_ORIGINAL_MSG>
</MESSAGE_BODY>
</STATUS_MESSAGE>
```

You can modify text in the `<SUBJECT>` tag or in the `<TEXT>` tags.

You can add additional `<TEXT>` tags in the `<MESSAGE_BODY>`.

You can remove tags to keep an element from being displayed. For example, you could remove the `<ATTACH_ORIGINAL_MSG></ATTACH_ORIGINAL_MSG>` tags to keep the original message from displaying.

You can use the following format characters and variables:

- ◆ `\t`: tab
- ◆ `\r`: carriage return
- ◆ `\n`: line feed
- ◆ `%s`: recipient name variable

- 3 Save the file, renaming it from `statusxx.xml` to `status.xml`.

- 4 Restart the GWIA.

The GWIA now uses the status messages defined in the `status.xml` file rather than its internal status messages.

53.1.11 Managing MIME Messages

Multipurpose Internet Mail Extensions, or MIME, provides a means to interchange text in languages with different character sets. Multimedia email can be sent between different computer systems that use the SMTP protocol. MIME allows you to send and receive email messages containing:

- ◆ Images
- ◆ Sounds

- ♦ Linux Tar Files
- ♦ PostScript
- ♦ FTP-able File Pointers
- ♦ Non-ASCII Character Sets
- ♦ Enriched Text
- ♦ Nearly any other file

Because MIME handles such a variety of file types, you might need to customize aspects of MIME for your users.

- ♦ [“Customizing MIME Preamble Text” on page 774](#)
- ♦ [“Customizing MIME Content-Type Mappings” on page 774](#)

Customizing MIME Preamble Text

An ASCII file called `preamble.txt` is installed in the GWIA gateway directory (`domain\wpgate\gwia`). This file, which is included with any MIME multipart message, is displayed when the message recipient lacks a MIME-compliant mail reader.

The content of the `preamble.txt` file is a warning, in English, that the file is being sent in MIME format. If the recipient cannot read the message, he or she needs to either use a MIME-compliant mail reader or reply to the sender and request the message not be sent in MIME format.

We recommend that you use the `preamble.txt` file so that those who read MIME messages coming from your GroupWise system and who lack MIME-compliant mail readers can understand why they cannot read the message and can take corrective action.

If you choose to modify the `preamble.txt` file, be aware of the following considerations:

- ♦ The maximum file size is 1024 bytes (1 KB)
- ♦ This file is read by the GWIA when the GWIA starts, so if you change the file, you must restart the GWIA.

The GWIA's gateway directory also contains a `preamble.all` file. The `preamble.all` file includes the text of `preamble.txt` translated into several languages. If you anticipate that your users will be sending mail to non-English speaking users, you might want to copy the appropriate language sections from the `preamble.all` file to the `preamble.txt` file.

The 1024-byte limit on the size of the `preamble.txt` file still applies, so make sure that the file does not exceed 1024 bytes.

Customizing MIME Content-Type Mappings

By default, the GroupWise client determines the MIME content-type and encoding for message attachments. If, for some reason, the GroupWise client cannot determine the appropriate MIME content-type and encoding for an attachment, the GWIA must determine the content-type and encoding.

The GWIA uses a `mimetype.cfg` file to map attachments to the appropriate MIME content types. Based on an attachment's content type, the GWIA encodes the attachment using quoted-printable, Base64, or BinHex. Generally, quoted-printable is used for text-based files, Base64 for application files, and BinHex for Macintosh files.

The `mimetype.cfg` file includes mappings for many standard files. If necessary, you can modify the file to include additional mappings. If an attachment is sent that does not have a mapping in the file, the GWIA chooses quoted-printable, BinHex, or Base64 encoding.

The `mimetype.cfg` file is also used for RFC-822 attachments, but UUencode or BinHex encoding is used regardless of the mapped content type.

The `mimetype.cfg` file is located in the `domain\wpgate\gwia` directory. The following sections provide information you need to know to modify the file:

- ◆ “Mapping Format” on page 775
- ◆ “File Organization” on page 776

Mapping Format

Each mapping entry in the file uses the following format:

```
content-type .ext|dtk-code|mac-tttcccc [/parms] ["comment"]
```

Element	Description
content-type	The MIME content type to which the file type is being mapped (for example, text/plain). You can omit the content-type only if you use the /parms element to explicitly define the encoding scheme for the file type.
.ext dtk-code mac-tttcccc	The .ext element, dtk-code element, and mac-tttcccc element are mutually exclusive. Each entry contains only one of the elements. <ul style="list-style-type: none">◆ .ext: The file type extension being mapped to the content type (for example, .txt).◆ dtk-code: The detect code being mapped to the content type (for example, dtk-1126). GroupWise assigns a detect code to each attachment type.◆ mac-tttcccc: The Macintosh file type and creator application being mapped to the content type (for example, mac-textmswd). The first four characters (<i>ttt</i>) are used for the file type. The last four characters (<i>cccc</i>) are used for the creator application. You can use <i>????</i> for the creator portion (mac-text????) to indicate a certain file type created by any application. You can use <i>????</i> in both portions (mac-????????) to match any file type created by any application.

Element	Description
/parms	Optional parameters that can be used to override the default encoding assigned to the MIME content type. Possible parameters are: <ul style="list-style-type: none"> ◆ /alternate ◆ /parallel ◆ /base64 ◆ /quoted-printable ◆ /quoted-printable-safe ◆ /uuencode ◆ /plain ◆ /binhex ◆ /nofixeol ◆ /force-ext ◆ /noconvert ◆ /apple-single ◆ /apple-double
"comment"	Optional content description

File Organization

The `mimetype.cfg` file contains the following four sections:

- ◆ [Parameter-Override]
- ◆ [Mac-Mappings]
- ◆ [Detect-Mappings]
- ◆ [Extension-Mappings]

[Parameter-Override]

The `[Parameter-override]` section takes priority over other sections. You can use this section to force the encoding scheme for certain file types. This section also contains defaults for sending various kinds of multipart messages. This is how the GWIA knows to put attachments into MIME Alternate/Parallel multipart.

[Mac-Mappings]

The `[Mac-mappings]` section defines mappings for Macintosh file attachments. The following is a sample entry:

```
application/msword mac-wdbnmswd "Word for Macintosh"
```

Macintosh files have a type and creator associated with them. The first four characters are used for the type and the last four characters are used for the creator application.

In the above example, the type is `wdbn` and the creator application is `mswd`. When a user attaches a Macintosh file to a message, the GWIA uses the appropriate entry in the `[Map-mappings]` section to map the file to a MIME content type and then encode the file according to the assigned encoding

scheme. Unless otherwise specified by the /parms element, BinHex 4.0 is used for the encoding. The following example shows how you can use the /parms element to change the encoding from the default (BinHex) to Base64:

```
application/msword mac-wdbnmswd /base64 "Word for Macintosh"
```

If necessary, you can use `????` for the creator portion (`mac-text????`) to indicate a certain file type created by any application. Or, you can use `?????` in both portions (`mac-????????`) to match any file type created by any application. For example:

```
application/octet-stream mac-???????? /base64 "Mac Files"
```

This causes all Macintosh files to be encoded using Base64 rather than BinHex.

[Detect-Mappings]

GroupWise attempts to assign each attachment a detect code based on the attachment's file type. The [Detect-mappings] section defines the mappings based on these detect codes. The following is a sample entry:

```
application/msword dtk-1000 "Microsoft Word 4"
```

The GWIA uses the detect code to map to a MIME content type and then encode the file according to the assigned encoding scheme. If there is no mapping specified or if the file type cannot be determined, one of the other mapping methods, such as Extension-Mappings, are used. The detect codes associated with attachments are GroupWise internal codes and cannot be changed.

[Extension-Mappings]

If a mapping could not be made based on the entries in the [Mac-mappings] and [Detect-mappings] section, the GWIA uses the [Extension-mappings] section. The [Extension-mappings] section defines mappings based on the attachment's file extension. The following is a sample entry:

```
application/pdf .pdf
```

53.2 Configuring POP3/IMAP4 Services

The Post Office Protocol 3 (POP3) and the Internet Message Access Protocol 4 (IMAP4) are standard messaging protocols for the Internet. The GroupWise GWIA can function as a POP3 or an IMAP server, allowing access to the GroupWise domain database and message store. With POP3 or IMAP server functionality enabled, GroupWise users can download their messages from GroupWise to any POP3/IMAP4-compliant Internet email client. To send messages, POP3/IMAP4 clients can identify the GWIA as their SMTP server.

Complete the instructions in the following sections to set up POP3/IMAP4 service:

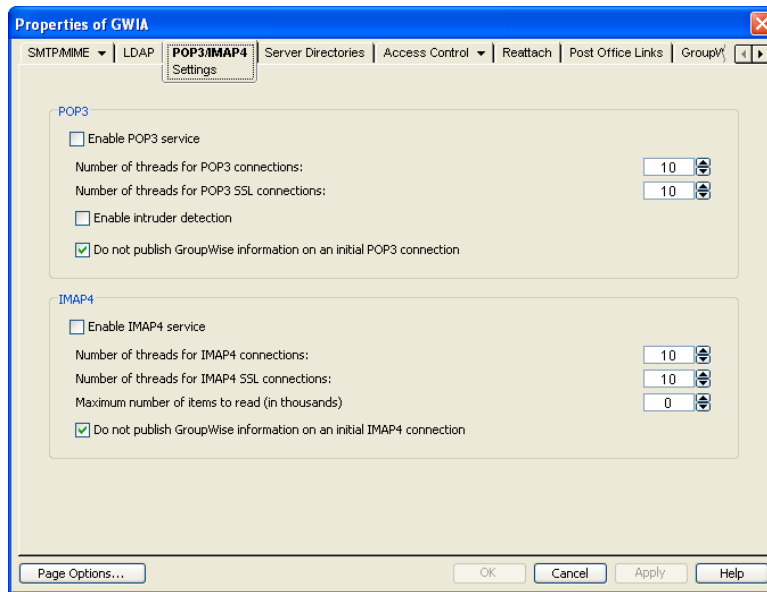
- ♦ [Section 53.2.1, "Enabling POP3/IMAP4 Services," on page 778](#)
- ♦ [Section 53.2.2, "Configuring Post Office Links," on page 779](#)
- ♦ [Section 53.2.3, "Giving POP3 or IMAP4 Access Rights to Users," on page 781](#)
- ♦ [Section 53.2.4, "Setting Up an Email Client for POP3/IMAP4 Services," on page 781](#)

NOTE: Internal IMAP clients can connect directly to the POA, rather than connecting through the GWIA, as described in [Section 36.2.3, "Supporting IMAP Clients," on page 498](#). Direct connection provides faster access for internal IMAP clients.

53.2.1 Enabling POP3/IMAP4 Services

By default, POP3 service and IMAP4 service are enabled. To verify that the services are enabled and configured appropriately:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *POP3/IMAP4 > Settings* to display the POP3/IMAP4 Settings page.



- 3 To enable POP3, fill in the following fields:

Enable POP3 Service: POP3 service is off by default. Select this option to allow POP3 downloads from a GroupWise mailbox. It corresponds with the GWIA's `--pop3` switch.

Number of Threads for POP3 Connections: The POP3 threads setting lets you specify the number of connections for POP3 download requests. The default is 10 threads. This setting corresponds with the GWIA's `--pt` switch.

Number of Threads for POP3 SSL Connections: Specify the maximum number of threads you want the GWIA to use for secure POP3 connections. This setting corresponds with the GWIA's `--sslpt` switch.

Enable Intruder Detection: Select this option to instruct the GWIA to log POP3 email clients in through the POA so that the POA's intruder detection can take effect, if it has been configured in ConsoleOne (POA object > *Client Access Settings > Intruder Detection*). This setting corresponds with the GWIA's `--popintruderdetect` switch.

Do Not Publish GroupWise Information on an Initial POP3 Connection: This option suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by a POP client. It is enabled by default. This setting corresponds with the GWIA's `--nopopversion` switch.

- 4 To enable IMAP4, fill in the following fields:

Enable IMAP4 Service: IMAP4 service is off by default. Select this option to allow IMAP4 downloads and management of GroupWise messages. It corresponds with the GWIA's `--imap4` switch.

Number of Threads for IMAP4 Connections: The IMAP4 threads setting lets you specify the number of connections for IMAP4 requests. The default is 10 threads. This setting corresponds with the GWIA's `--it` switch.

Number of Threads for IMAP4 SSL Connections: Specify the maximum number of threads you want the GWIA to use for secure IMAP4 connections. This setting corresponds with the GWIA's `--sslit` switch.

Maximum Number of Items to Read: Specify in thousands the maximum number of items that you want the GWIA to download at one time. By default, the GWIA downloads 20,000 items at a time. For example, specify 15 to download 15,000 items at a time. The higher the setting, the more memory the GWIA uses to process a single folder. This setting corresponds with the GWIA's `--imapreadlimit` switch. See also the `--imapreadnew` switch.

Do Not Publish GroupWise Information on an Initial IMAP4 Connection: This option suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by an IMAP client. It is enabled by default. This setting corresponds with the GWIA's `--noimapversion` switch.

- 5 Click *OK* to save the changes.

The Post Office Agent (POA) can also be configured to support IMAP connections. You could offer IMAP services internally through the POA to provide faster response time for internal users, as described in [Section 36.2.3, "Supporting IMAP Clients," on page 498](#). However, IMAP is primarily available on the POA to support several third-party applications that communicate with the POA using IMAP, while the IMAP services provided by the GWIA provide the standard IMAP access used by users across the Internet.

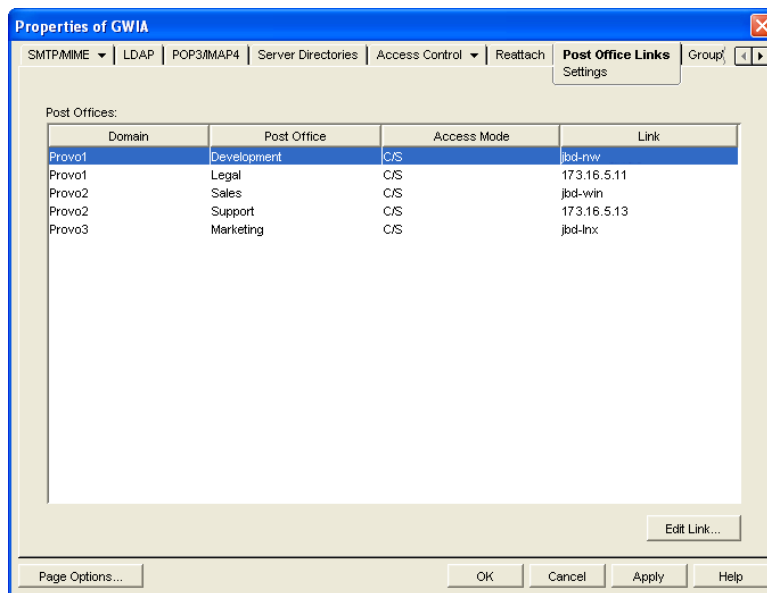
53.2.2 Configuring Post Office Links

To function as a POP3/IMAP4 server, the GWIA requires access to each post office that contains mailboxes that will be accessed by a POP3/IMAP4 client. The GWIA can connect directly to the post office directory through a UNC path or mapped drive, or it can use a TCP/IP connection to the Post Office Agent (POA). By default, the GWIA uses the access mode that has been defined for the post office (Post Office object > *GroupWise* > *Post Office Settings*). If necessary, you can change the way the GWIA links to a post office.

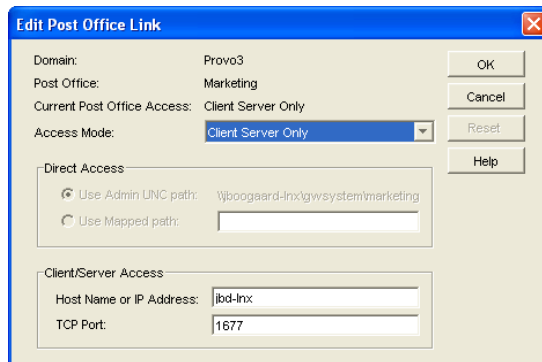
To change a post office link:

- 1 In *ConsoleOne*, right-click the GWIA object, then click *Properties*.
- 2 Click *Post Office Links* > *Settings*.

The Post Office list displays all post offices in your GroupWise system and how the GWIA connects to them



- 3 In the *Post Offices* list, select the post office whose link information you want to change, then click *Edit Link* to display the Edit Post Office Link dialog box.



- 4 Define the following properties:

Access Mode: The access mode determines whether the GWIA uses client/server access, direct access, or both client/server and direct access to connect to the post office. With client/server and direct, the GWIA first tries client/server access; if client/server access fails, it then tries direct access. You can also choose to use the same access mode currently defined for the post office (on the Post Office object's Post Office Settings). The current access mode is displayed in the *Current Post Office Access* field.

Direct Access: When connecting to the post office in direct mode, the GWIA can use the post office's UNC path (as defined on the Post Office object's Identification) or a mapped path that you enter.

Client/Server Access: When connecting to the post office in client/server mode, the GWIA must know the hostname (or IP address) and port number of the Post Office Agent running against the post office.

- 5 Click *OK*.
- 6 Repeat [Step 3](#) through [Step 5](#) for each post office whose link you want to change.

53.2.3 Giving POP3 or IMAP4 Access Rights to Users

Access to POP3/IMAP4 services is determined by the class of service in which they are a member. By default, all users are members of the default class of service, which gives them POP3 and IMAP4 access.

If you changed the default class of service to exclude POP3 or IMAP4 access rights, or if you defined additional classes of services that do not provide POP3 or IMAP4 access rights, you might want to evaluate your currently defined classes of service to ensure that they provide the appropriate POP3 or IMAP4 access. For details, see [Section 54.1, “Controlling User Access to the Internet,”](#) on page 787.

53.2.4 Setting Up an Email Client for POP3/IMAP4 Services

With the GWIA set up as a POP3 and/or IMAP4 server, you can configure users' email clients to download messages from GroupWise mailboxes.

Most email clients are configured differently. However, all Internet clients need to know the following information:

- ♦ **POP3/IMAP4 Server:** The DNS hostname or IP address of the GWIA.
- ♦ **Login Name:** The user's GroupWise user ID. For POP3 clients, there are several user ID login options you can use to control how the GWIA handles the user's messages. For example, you can limit how many messages are downloaded each session. For more information, see [“User ID Login Options”](#) on page 781.
- ♦ **Password:** The user's existing GroupWise mailbox password. POP3/IMAP4 services requires users to have passwords assigned to their mailboxes.

User ID Login Options

With POP3 clients, users can add the options listed in the table below to the login name (GroupWise user ID) to control management of their mailbox messages. If used, these options override the POP3 settings assigned through the user's class of service (see [Section 54.1.2, “Creating a Class of Service,”](#) on page 788).

Login options are appended to the user ID name with a colon character (:) between the user ID name and the switches:

Syntax: user_ID:switch

Example: User1:v=1

You can combine options by stringing them together after the user ID and the colon without any spaces between the options:

Syntax: user_ID:switch1switch2

Example: User1:v=1sdl=10

The syntax for the user ID options is not case sensitive. Login options are not required. If you do not want to include any login options, just enter the user ID name in the text box, or following the USER command if you are using a Telnet application as your POP3 client.

Option	Explanation	Example
<i>v=number between 1-31</i>	<p>The v option defines the POP3 client's view number. If multiple POP3 clients access the same GroupWise mailbox, each client must use a different view number in order to see a fresh mailbox.</p> <p>For example, if two POP3 clients access a mailbox and the first client downloads the unread messages, the second client cannot download the messages unless it is using a different view number than the first client.</p> <p>If this option is not used, the default value is 1.</p>	<i>User_ID:v=1</i>
d	The d option deletes the messages from the GroupWise mailbox after they have been downloaded to the POP3 client.	<i>User_ID:d</i>
p	The p option purges the messages from the GroupWise mailbox after they have been downloaded to the POP3 client.	<i>User_ID:p</i>
<i>t=1-1000</i>	The t option defines the download period, starting with the current day. For example, if you specify 14, then only messages that are 14 days old or newer are downloaded. If this option is not used, the default value is 30 days.	<i>User_ID:t=14</i>
n	The n option downloads messages in RFC-822 format rather than the default MIME format.	<i>User_ID:N</i>
m	The m option downloads messages in MIME format. This is the default.	<i>User_ID:M</i>
s	The s option presets the file size when the STAT command is executed. If the user mailbox contains a lot of messages or large messages, it can take a long time to calculate the file size. With this option, the STAT command always reports an artificial file size of 1, which can save time.	<i>User_ID:S</i>
<i>l=1-1000</i>	The l option limits the number of messages to download for each POP3 session. For example, if you want to limit the number of messages to 10, you enter l=10. If this option is not used, the default value is 100 messages.	<i>User_ID:l=10</i>

53.3 Configuring LDAP Services

The GWIA supports the Lightweight Directory Access Protocol (LDAP) standard. With LDAP enabled, the GroupWise GWIA functions as an LDAP server, allowing LDAP queries for GroupWise user information contained in the GroupWise Address Book. You can also configure which GroupWise fields (Given Name, Last Name, Phone, and E-Mail) are visible to an LDAP query.

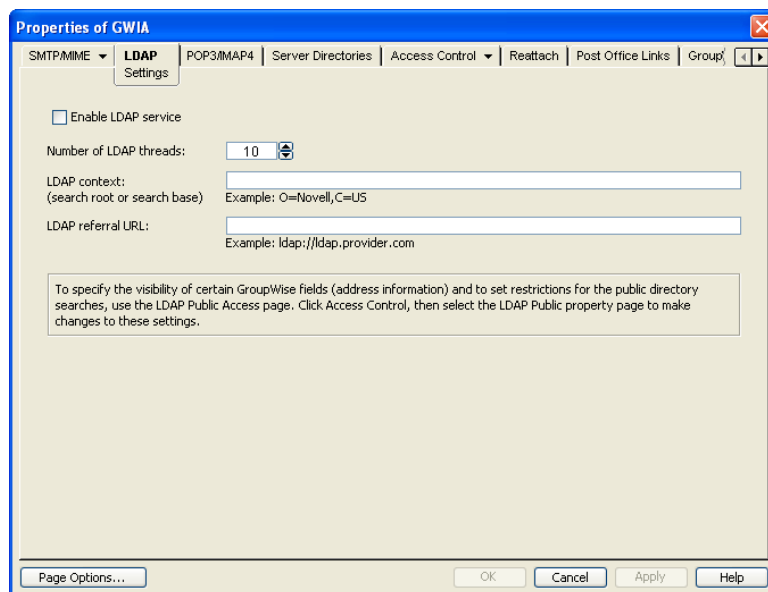
- ◆ [Section 53.3.1, “Enabling LDAP Services,” on page 783](#)
- ◆ [Section 53.3.2, “Configuring Public Access,” on page 784](#)

IMPORTANT: For users to perform LDAP searches for GroupWise user information, they need to define the GroupWise Address Book as an LDAP directory in their email client. When doing so, they use the GWIA's DNS hostname or IP address for the LDAP server address

53.3.1 Enabling LDAP Services

To enable and configure LDAP services for mail client access:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *LDAP > Settings* to display the LDAP Settings page.



- 3 Fill in the fields:

Enable LDAP Service: Turn on this option to allow LDAP queries. LDAP service is off by default. This setting corresponds to the GWIA's `--ldap` switch.

Number of LDAP Threads: The *LDAP Threads* setting lets you specify the maximum number of threads that process LDAP queries. The default is 10 threads. This setting corresponds with the GWIA's `--ldaphthr` switch.

LDAP Context: Use this option to limit the directory context in which the LDAP server searches. For example, if you want to limit LDAP searches to the Novell organization container located under the United States country container, enter `O=Novell,C=US`. This setting corresponds with the GWIA's `--ldapcntxt` switch.

If you enter an LDAP context, you must make sure that users, when defining the directory in their email client, enter the same context (using the identical text you did) in the Search Base or Search Root field.

You can leave the settings empty in both locations.

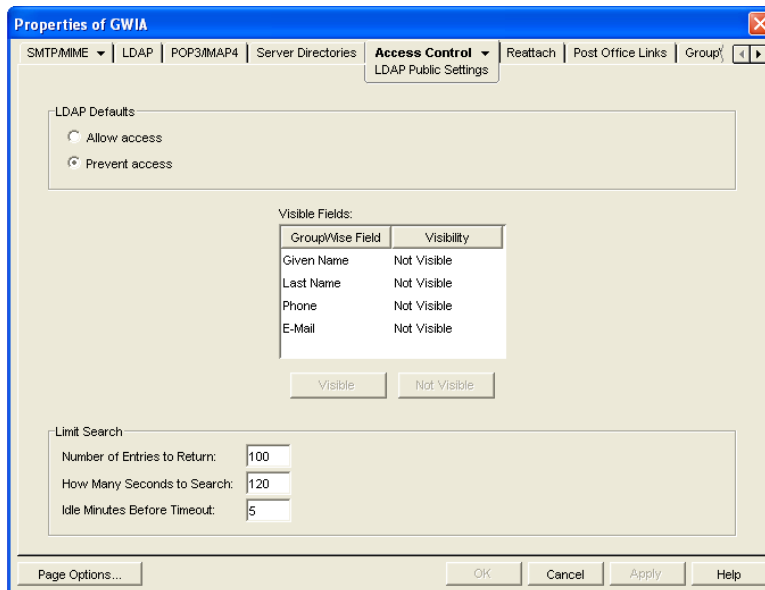
LDAP Referral URL: Use this option to define a secondary LDAP server to which you can refer an LDAP query if the query fails to find a user or address in your GroupWise system. For this option to work, the requesting Web browser must be able to track referral URLs. This setting corresponds with the GWIA's `--ldaprefurl` switch.

- 4 Continue with the next section, [Configuring Public Access](#).

53.3.2 Configuring Public Access

After you have enabled LDAP services, you can configure which GroupWise fields are visible to LDAP searches and also set search restrictions. By default, no fields are visible.

- 1 If the GWIA object's property page is not open, right-click the GWIA object, then click *Properties*.
- 2 Click *Access Control > LDAP Public Settings*.



- 3 Fill in the fields:

LDAP Defaults: Select one of the following defaults for public access: *Allow Access* or *Prevent Access*. If you select *Allow Access*, the GroupWise fields (in the *Visible Fields* lists) default to *Visible* for an LDAP search. If you select *Prevent Access*, the GroupWise fields default to *Not Visible*.

Visible Fields: You can override the default visibility for a GroupWise field (*Given Name*, *Last Name*, *Phone*, and *E-Mail*) by selecting the field and then clicking the appropriate visibility button (*Visible* or *Not Visible*). For example, if you have selected *Allow Access* as the LDAP default, but you don't want users' telephone numbers to be visible, you can mark the *Phone* field as *Not Visible*.

Number of Entries to Return: Select the maximum number of entries to return. The default is 100.

How Many Seconds to Search: Select the maximum amount of time (in seconds) you want the GWIA to spend searching. The default is 120 seconds.

Idle Minutes before Timeout: Specify the number of minutes to allow the search to continue without finding a matching address entry. The default is 5 minutes.

- 4 Click *OK* to save the changes.

53.4 Configuring Paging Services

The GroupWise GWIA includes the ability to send a GroupWise message to a pager through an Internet paging service provider. The GWIA's paging service includes the following features:

- ♦ **Smart forwarding:** If a message has been replied to or forwarded before being sent to a pager, the GWIA identifies the original message and sends only it.
- ♦ **Easy to read originator information:** The GWIA sends the original From, Subject, and Message information to the pager, rather than cryptic Header information.
- ♦ **User block control:** By using the `/l=length` and `/b=number` switches on the message's To line, the sender can control the block length and number of blocks to send to the pager. By default, the GWIA sends 255 bytes per block (`/l=255 /b=1`).

To set up and use paging services, complete the tasks in the following sections:

- ♦ [Section 53.4.1, "Setting Up Paging," on page 785](#)
- ♦ [Section 53.4.2, "Using Paging," on page 786](#)

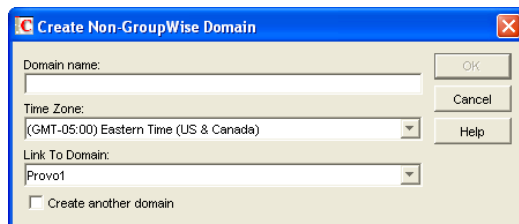
53.4.1 Setting Up Paging

To set up the GWIA's paging service, you need to create a non-GroupWise domain to represent the paging service and then use your GWIA to link your system to the non-GroupWise domain. The non-GroupWise domain enables GroupWise to correctly identify pager messages and route messages to the GWIA, which can then send the messages to the Internet.

- ♦ ["Creating a Non-GroupWise Domain" on page 785](#)
- ♦ ["Linking the GWIA to the Non-GroupWise Domain" on page 786](#)

Creating a Non-GroupWise Domain

- 1 In ConsoleOne, right-click the GroupWise System object, click *New*, then click *Non-GroupWise Domain* to display the Create Non-GroupWise Domain dialog box.



- 2 Fill in the following information:

Domain Name: Provide the domain with a name such as Page. Users need to know the name when addressing pager messages.

Time Zone: Select the time zone in which the GWIA is located.

Link to Domain: Select the domain in which the GWIA is located.

- 3 Click *OK* to create the domain.

Linking the GWIA to the Non-GroupWise Domain

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Link Configuration* to display the GroupWise Link Configuration tool.
- 2 In the drop-down list, select the domain that owns the GWIA that you are using for this paging service.
- 3 In the *Outbound Links* box, right-click the non-GroupWise domain, then click *Edit*.
- 4 Click *Yes* to accept the domain path as the mapped path and display the Edit Domain Link dialog box.
- 5 In the *Link Type* field, select *Gateway*.
- 6 In the *Gateway Link* field, select the *Internet Agent*.
- 7 In the *Gateway Access String* field, type `-page`.
- 8 Click *OK* to save the information.
- 9 Click *File > Exit > Yes* to save your changes and exit the Link Configuration tool.
- 10 Restart the GWIA.

53.4.2 Using Paging

To use paging, GroupWise users must address messages to the non-GroupWise domain, specifying the PIN number of the pager and the hostname of the paging service in the following format:

domain:pin@paging_service_provider

For example,

`page:123456789@skytel.com`

`page:123456789@epage.arch.com`

By using the `/l=length` and `/b=number` switches on the message's To line, the sender can control the block length and number of blocks to send to the pager. For example,

`page:123456789@epage.arch.com/l=128/b=4`

By default, the GWIA sends 255 bytes per block (`/l=255 /b=1`).

54 Managing Internet Access

After you have configured the Internet services that you want the GWIA to provide in your GroupWise system, you need to take control of the information that flows in and out between your GroupWise system and the Internet.

- ♦ [Section 54.1, “Controlling User Access to the Internet,” on page 787](#)
- ♦ [Section 54.2, “Blocking Unwanted Email from the Internet,” on page 798](#)
- ♦ [Section 54.3, “Tracking Internet Traffic with Accounting Data,” on page 805](#)

54.1 Controlling User Access to the Internet

You can use the GroupWise GWIA’s Access Control feature to configure a user’s ability to send and receive SMTP/MIME messages to and from Internet recipients and to access his or her mailbox from POP3 or IMAP4 email clients. In addition to enabling or disabling a user’s access to features, you can configure specific settings for the features. For example, for outgoing SMTP/MIME messages, you can limit the size of the messages or the sites to which they can be sent. By default, there are no limitations.

Access Control can be implemented at a user, distribution list, post office, or domain level.

Choose from the following information to learn how to set up and use Access Control.

- ♦ [Section 54.1.1, “Classes of Service,” on page 787](#)
- ♦ [Section 54.1.2, “Creating a Class of Service,” on page 788](#)
- ♦ [Section 54.1.3, “Testing Access Control Settings,” on page 794](#)
- ♦ [Section 54.1.4, “Maintaining the Access Control Database,” on page 796](#)

54.1.1 Classes of Service

A class of service is a specifically defined configuration of GWIA privileges. A class of service controls the following types of access activities:

- ♦ Whether SMTP/MIME messages are allowed to transfer to and from the Internet
- ♦ Whether SMTP/MIME messages are allowed to transfer to and from specific domains on the Internet
- ♦ The maximum size of SMTP/MIME messages that can transfer to and from the Internet
- ♦ Whether SMTP/MIME messages generated by GroupWise rules are allowed to transfer to the Internet
- ♦ Whether IMAP4 clients are allowed to access the GroupWise system
- ♦ Whether POP3 clients are allowed to access the GroupWise system, and if allowed, how messages to and from POP3 clients are managed by the GroupWise system

The default class of service, which all users belong to, allows incoming and outgoing SMTP/MIME messages, and allows POP3 and IMAP4 access. You can control user access, at an individual, distribution list, post office, or domain level, by creating different classes of service and adding the appropriate members to the classes. For example, you could create a class of service that limits the size of SMTP/MIME messages for a selected individual, distribution list, post office, or domain.

Because you can assign membership at the user, distribution list, post office, and domain level, it is possible that a single user can be a member of multiple classes of service. This conflict is resolved hierarchically, as shown in the following table:

Membership assigned to a user through a...	Overrides membership assigned to the user through the...
domain	♦ default class of service
post office	♦ default class of service ♦ domain
distribution list	♦ default class of service ♦ domain ♦ post office
user	♦ default class of service ♦ domain ♦ post office

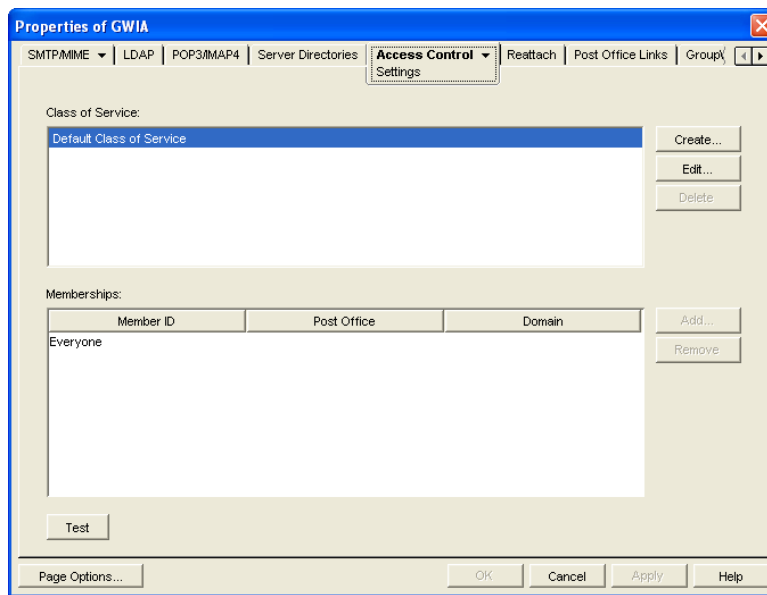
If a user's membership in two classes of service is based upon the same level of membership (for example, both through individual user membership), the class that applies is the one that allows the most privileges.

IMPORTANT: The GWIA uses the message size limit set for the default class of service as the maximum incoming message size for your GroupWise system. Therefore, you should set the message size for the default class of service to accommodate the largest message that you want to allow into your GroupWise system. As needed, you can then create other classes of service with smaller message size limits to restrict the size of incoming messages for selected users, distribution lists, post offices, or domains. Methods for restricting message size within your GroupWise system are described in [Section 12.3.5, "Restricting the Size of Messages That Users Can Send," on page 201](#).

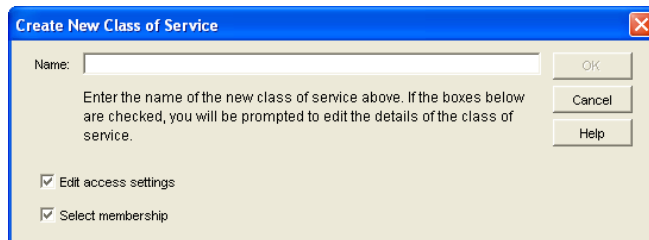
Attachments to incoming SMTP messages are included in the `mime.822` file, in addition to being attached to the message. Therefore, attachments contribute twice to the size of the overall message. Take this account when determining the maximum incoming message size for your GroupWise system.

54.1.2 Creating a Class of Service

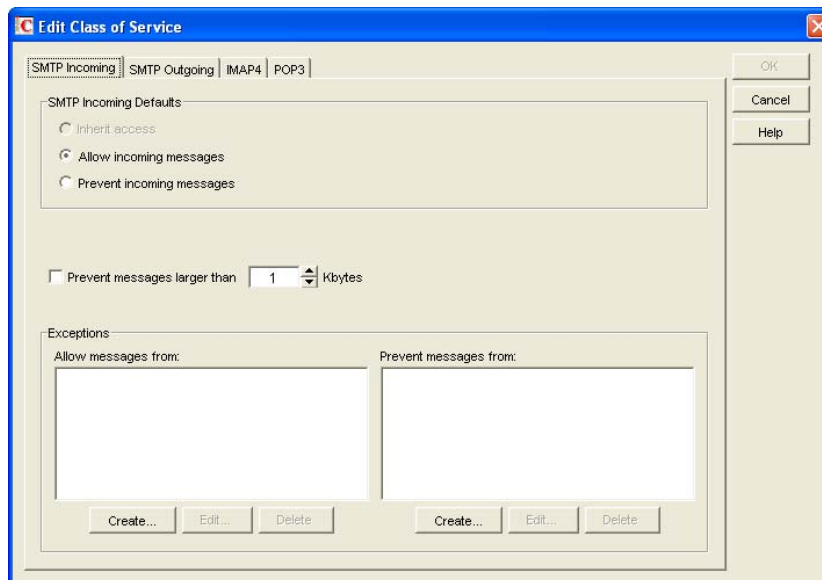
- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *Access Control > Settings* to display the Access Control Settings page.



3 Click *Create* to display the Create New Class of Service dialog box.



4 Type a name for the class, then click *OK* to display the Edit Class of Service dialog box.



5 On the *SMTP Incoming* tab, choose from the following options:

Inherit Access: Select this option if you want members of this class of service to inherit their SMTP Incoming access from a class of service assigned at a higher level. For example, a post office inherits the domain's access. If the domain is not a member of a class of service, the post office inherits the default class of service.

Allow Incoming Messages: Select this option to allow members of the class of service to receive email messages through the GWIA. You can use the *Exceptions* option to prevent messages from specific Internet sites.

Prevent Incoming Messages: Select this option to prevent email messages coming from the Internet. You can use the *Exceptions* option to allow messages from specific Internet sites.

NOTE: If a member of the class of service to allow or prevent has an alias, you must also add the member's alias to the class of service. Ongoing use of aliases is not recommended. For more information, see [Section 5.14, "Gateway Alias Migration," on page 98](#).

Prevent Messages Larger Than: This option is available only if you chose *Allow Incoming Messages* or *Prevent Incoming Messages*. In the case of *Prevent Incoming Messages*, this option only applies to messages received from Internet sites listed in the *Allow Messages From* list.

If you want to set a size limit on incoming messages, select the limit.

Internet messages that exceed the limit are not delivered. The sender receives an email message indicating that the message is undeliverable and including the following explanation:

Message exceeds maximum allowed size

IMPORTANT: If you have also set a message size limit for your MTAs, as described in [Section 42.2.1, "Restricting Message Size between Domains," on page 642](#), make sure that the MTA message size limit is equal to or greater than the GWIA message size limit.

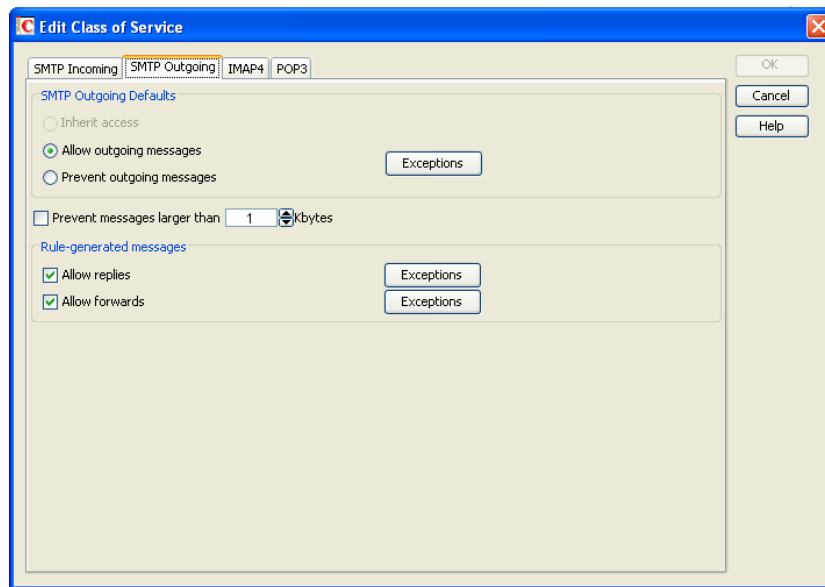
Exceptions: This option is available only if you chose *Allow Incoming Messages* or *Prevent Incoming Messages*.

Prevent Messages From: If you chose to allow incoming messages but you want to prevent messages from specific Internet sites (IP addresses or DNS hostnames), add the sites to the *Prevent Messages From* list.

Allow Messages From: Conversely, if you chose to prevent incoming messages but you want to allow messages from specific Internet sites (IP addresses or DNS hostnames), add the sites to the *Allow Messages From* list.

If you want to allow messages where the user name is blank, add Blank-Sender-User-ID to the *Allow Messages From* list.

- 6 Click *SMTP Outgoing*, then choose from the following options:



Inherit Access: Select this option if you want members of this class of service to inherit their *SMTP Outgoing* access from a class of service assigned at a higher level. For example, a post office inherits the domain's access. If the domain is not a member of a class of service, the post office inherits the default class of service.

Allow Outgoing Messages: Select this option to allow members of the class of service to send email messages over the Internet. You can use the *Exceptions* option to prevent messages from being sent to specific Internet sites.

Prevent Outgoing Messages: Select this option to prevent members of the class of service from sending email messages over the Internet. You can use the *Exceptions* option to allow messages to be sent to specific Internet sites.

Prevent Messages Larger Than: This option is available only if you chose *Allow Outgoing Messages* or *Prevent Outgoing Messages*.

If you want to set a size limit on outgoing messages, specify the limit.

Exceptions: This option is available only if you chose *Allow Outgoing Messages* or *Prevent Outgoing Messages*.

If you chose to allow outgoing messages but you want to prevent messages from being sent to specific Internet sites (IP addresses or DNS hostnames), add the sites to the *Prevent Messages To* list.

Conversely, if you chose to prevent outgoing messages but you want to allow messages to be sent to specific Internet sites (IP addresses or DNS hostnames), add the sites to the *Allow Messages To* list.

Allow Replies: This option is available only if you chose *Allow Outgoing Messages* or *Prevent Outgoing Messages*.

Turn on this option to allow the GWIA to send rule-generated replies to messages (such as vacation rule messages).

In addition, you can use the `/blockrulegenmsg` startup switch to allow some types of rule-generated messages while blocking others.

Exceptions: Click *Exceptions* to create a list of specific Internet addresses that are handled opposite to the *Allow Replies* setting.

Allow Forwards: This option is available only if you chose *Allow Outgoing Messages* or *Prevent Outgoing Messages*.

Turn on this option to allow the GWIA to forward rule-generated messages (which can be a security issue).

In addition, you can use the [/blockrulegenmsg](#) startup switch to allow some types of rule-generated messages while blocking others.

Exceptions: Click *Exceptions* to create a list of specific Internet addresses that are handled opposite to the *Allow Forwards* setting.

7 Click *IMAP4*, then choose from the following options:

Inherit Access: Select this option if you want members of this class of service to inherit their IMAP4 access from a class of service assigned at a higher level. For example, a post office inherits the domain's access. If the domain is not a member of a class of service, the post office inherits the default class of service.

Allow Access: Select this option to allow members of the class to send and receive messages with an IMAP4 client.

Prevent Access: Select this option to prevent members of the class from sending and receiving messages with an IMAP4 client.

8 Click *POP3*, then choose from the following options:

Inherit Access: Select this option if you want members of this class of service to inherit their POP3 access from a class of service assigned at a higher level. For example, a post office inherits the domain's access. If the domain is not a member of a class of service, the post office inherits the default class of service.

Allow Access: Select this option to allow members of the class to download their GroupWise messages to a POP3 client.

Prevent Access: Select this option to prevent downloading GroupWise messages to a POP3 client.

Delete Messages from GroupWise Mailbox after Download: This option applies only if you selected *Allow Access*.

If you turn on this option, messages downloaded from a GroupWise Mailbox to a POP3 client are moved to the Trash folder in the GroupWise Mailbox.

POP3 client users can enable this option by using the *userID:d* login option when initiating their POP session. For more information, see ["User ID Login Options" on page 781](#).

Purge Messages from GroupWise Mailbox after Download: This option applies only if you selected *Allow Access*.

If you turn on this option, messages downloaded from a GroupWise Mailbox are moved to the Mailbox's Trash folder and then emptied, completely removing the messages from the Mailbox.

POP3 client users can enable this option by using the *userID:p* login option when initiating their POP session. For more information, see ["User ID Login Options" on page 781](#).

Convert Messages to MIME Format When Downloading: This option applies only if you selected *Allow Access*.

If you turn on this option, messages downloaded to a POP3 client are converted to the MIME format.

POP3 client users can enable this option by using the *userID:m* login option when initiating their POP session. They can disable it by using the *userID:n* login option; this converts messages to RFC-822 format. For more information, see ["User ID Login Options" on page 781](#).

High Performance on File Size Calculations: This option applies only if you selected *Allow Access*.

POP3 clients calculate the size of each message file before downloading it. Turn on this option if you want to assign a size of 1 KB to each message file. This eliminates the time associated with calculating a file's actual size.

POP3 client users can enable this option by using the *userID:s* login option when initiating their POP session. For more information, see [“User ID Login Options” on page 781](#).

Number of Days Prior to Today to Get Messages From: This option applies only if you selected *Allow Access*.

Select the number of days to go back to look for GroupWise Mailbox messages to download to the POP3 client. The default is 30 days.

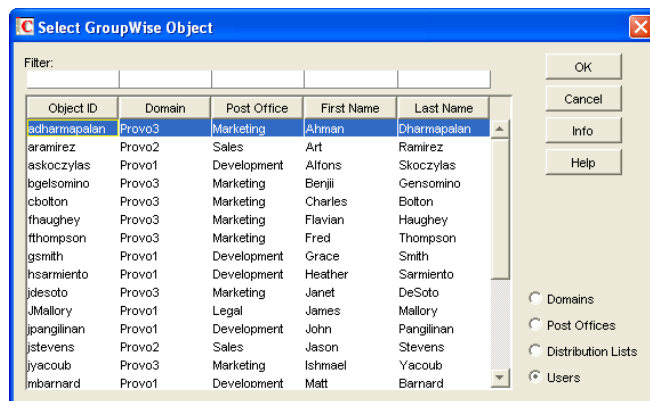
POP3 client users can override this option by using the *userID:t=x* login option when initiating their POP session. For more information, see [“User ID Login Options” on page 781](#).

Maximum Number of Messages to Download: This option applies only if you selected *Allow Access*.

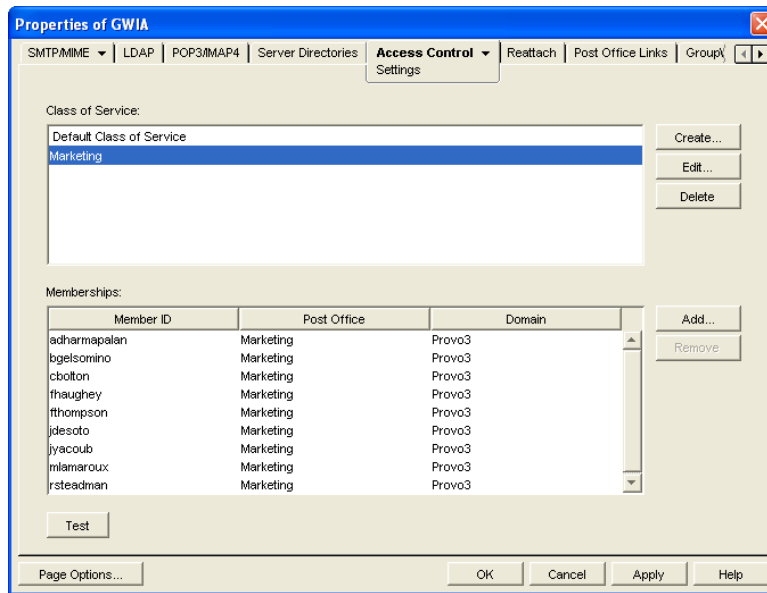
Select the maximum number of messages a user can download at one time from a GroupWise Mailbox to a POP3 client. The default is 100 messages.

POP3 client users can override this option by using the *userID:l=x* login option when initiating their POP session. For more information, see [“User ID Login Options” on page 781](#).

- 9 Click **OK** to display the Select GroupWise Object dialog box.



- 10 Select *Domains*, *Post Offices*, *Distribution Lists*, or *Users* to display the list you want.
- 11 In the list, select the domain, post office, distribution list, or user you want, then click *Add* to add the object as a member in the class. You can Control+click or Shift+click to select multiple users.

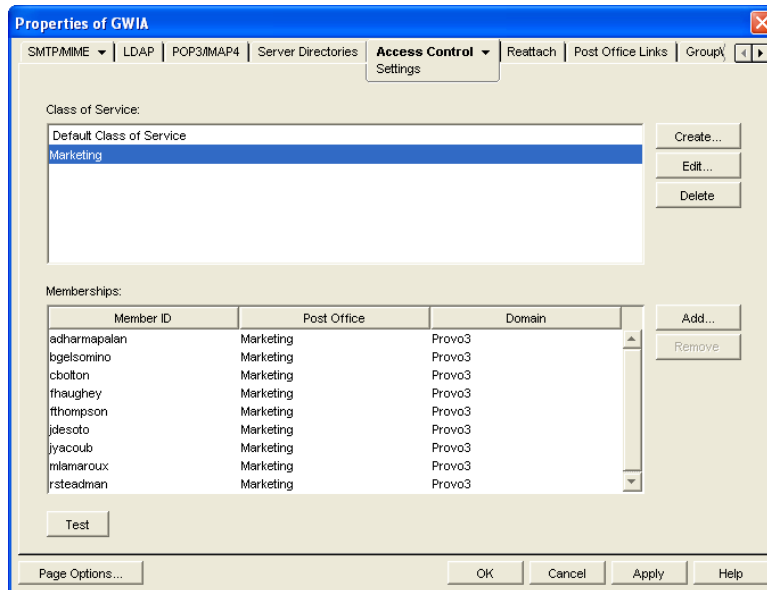


- 12 To add additional domains, post offices, distribution lists, or users as members of the class of service, select the class of server, then click *Add* to display the Select GroupWise Object dialog box.
- 13 Click *OK* (on the Settings page) when you are finished adding members.

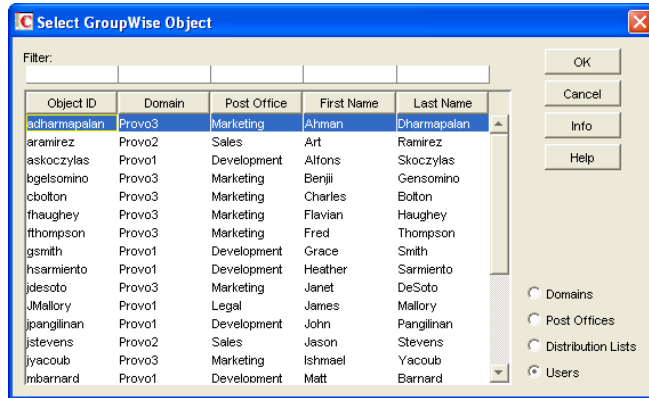
54.1.3 Testing Access Control Settings

If you created multiple classes of service, you might not know exactly which settings are being applied to a specific object (domain, post office, distribution list, or user) and which class of service the setting is coming from. To discover an object's settings, you can test the object's access.

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *Access Control > Settings* to display the Access Control Settings page.



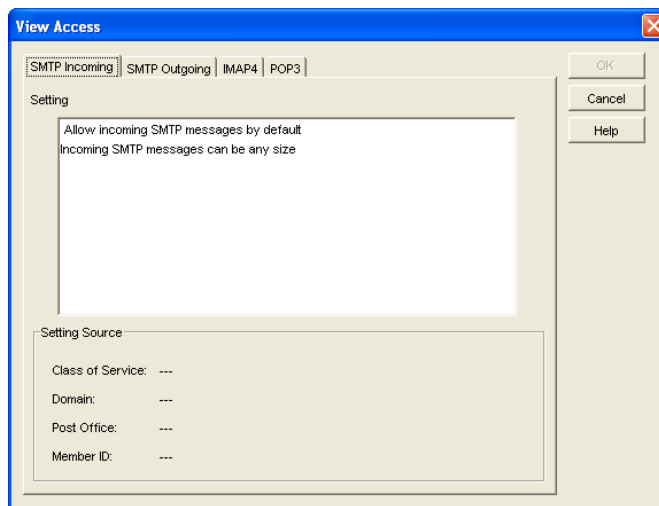
- 3 Click *Test* to display the Select GroupWise Object dialog box.



You use this dialog box to select the object (domain, post office, distribution list, or user) whose access you want to test.

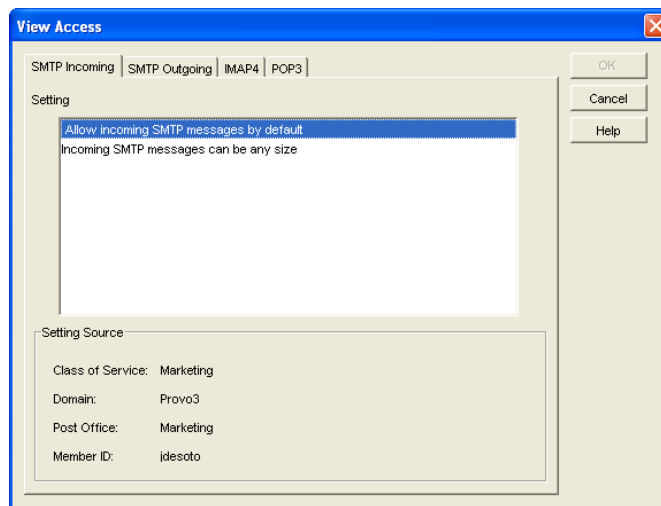
- 4 Select *Domains*, *Post Offices*, *Distribution Lists*, or *Users* to display the list you want. For example, if you want to see what access an individual user has, select *Users*.
- 5 In the list, select the object you want to view, then click *View Access*.

The tabbed pages show the access control settings for *SMTP Incoming*, *SMTP Outgoing*, *IMAP4*, and *POP3* as they are applied to that user, distribution list, post office, or domain.



- 6 To view the source for a specific setting, select the setting in the *Setting* box

The *Setting Source* fields display the class of service being applied to the object. It also displays the Member ID through which the class is being applied.



7 When you are finished, click *OK*.

54.1.4 Maintaining the Access Control Database

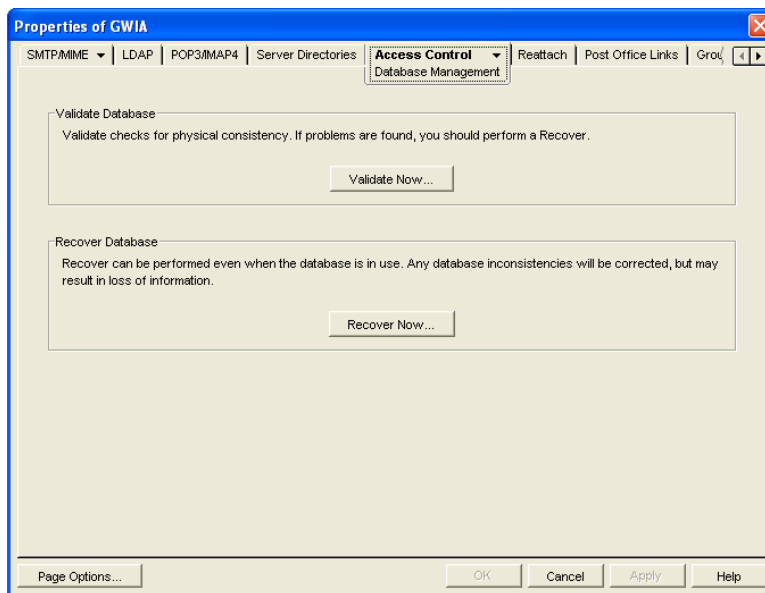
The Access Control database stores the information for the various classes of service you have created. If any problems occur with a class of service, you can validate the database to check for errors with the records and indexes contained in the database. If errors are found, you can recover the database.

The Access database, `gwac.db`, is located in the `domain\wpgate\gwia` directory.

- ♦ [“Validating the Database” on page 796](#)
- ♦ [“Recovering the Database” on page 797](#)

Validating the Database

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *Access Control > Database Management* to display the Database Management page.

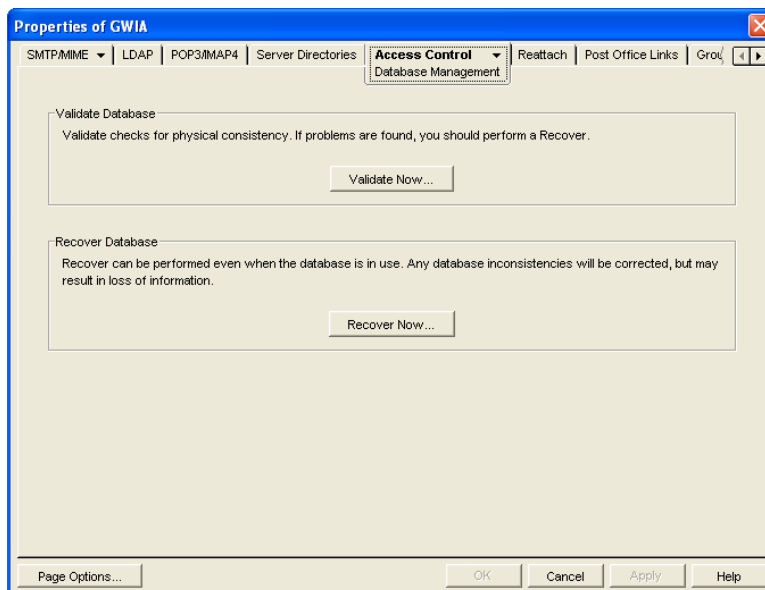


- 3 Click *Validate Now*.
- 4 After the database has been validated, click *OK*.
- 5 If errors were found, see [Recovering the Database](#) below.

Recovering the Database

If you encountered errors when validating the database, you must recover the database. During the recovery process a new database is created and all intact records are copied to the new database. Some records might not be intact, so you should check the classes of services to see if any information was lost.

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *Access Control > Database Management* to display the Database Management page.



- 3 Click *Recover Now*.
- 4 Click *OK*.
- 5 Check your class of service list to make sure that it is complete.

54.2 Blocking Unwanted Email from the Internet

The GWIA includes the following features to help you protect your GroupWise system and users from unwanted email:

- ♦ [Section 54.2.1, “Real-Time Blacklists,” on page 798](#)
- ♦ [Section 54.2.2, “Access Control Lists,” on page 800](#)
- ♦ [Section 54.2.3, “Blocked.txt File,” on page 800](#)
- ♦ [Section 54.2.4, “Mailbomb \(Spam\) Protection,” on page 801](#)
- ♦ [Section 54.2.5, “Customized Spam Identification,” on page 802](#)
- ♦ [Section 54.2.6, “SMTP Host Authentication,” on page 803](#)
- ♦ [Section 54.2.7, “Unidentified Host Rejection,” on page 804](#)

54.2.1 Real-Time Blacklists

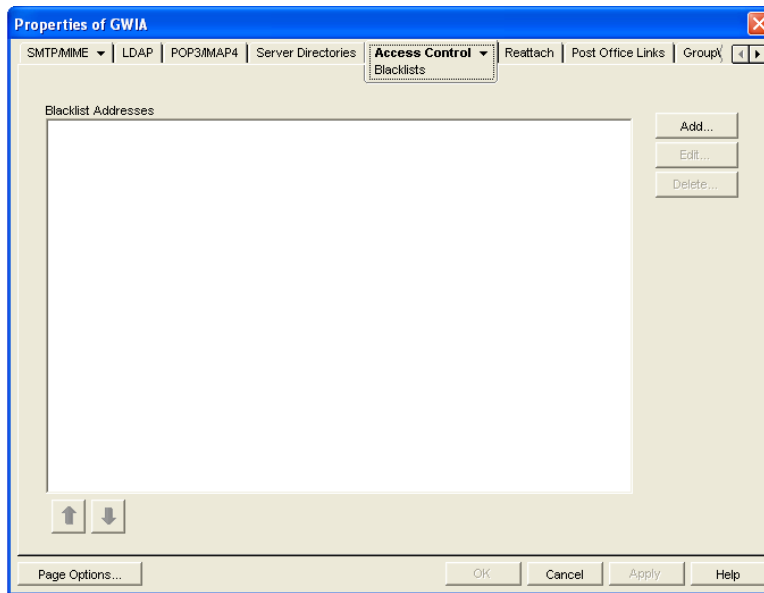
Organizations such as [SpamCop \(http://www.spamcop.net\)](http://www.spamcop.net) provide lists of IP addresses that are known to be open relay hosts or spam hosts. If you want to use free blacklist services such as these, or if you subscribe to fee-based services, you must define the blacklist addresses for these services. The GWIA then uses the defined services to ensure that no messages are received from blacklisted hosts. The following sections provide information to help you define blacklist addresses and, if necessary, override a host address included in a blacklist.

- ♦ [“Defining a Blacklist Address” on page 798](#)
- ♦ [“Overriding a Blacklist” on page 800](#)

NOTE: If you want to configure the GWIA to block a specific IP address or DNS hostname, add the address or hostname to a class of service, as described in [Section 54.1, “Controlling User Access to the Internet,” on page 787](#). The Blacklist feature configures the GWIA to use blacklist services that provide real-time lists of many sites that are known to be bad.

Defining a Blacklist Address

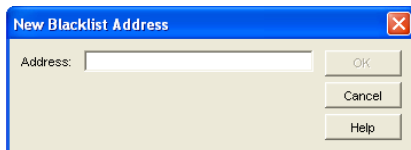
- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *Access Control > Blacklists* to display the Blacklists page.



The *Blacklist Addresses* list displays the addresses of all blacklists that the GWIA checks when it receives a message from another SMTP host. The GWIA checks the first blacklist and continues checking lists until the sending SMTP host's IP address is found or all lists have been checked. If the sending SMTP host's IP address is included on any of the blacklists, the message is rejected. If you have the GWIA's logging level set to *Verbose*, the log file includes information about the rejected message and the referring blacklist.

This list corresponds with the GWIA's */rbl* switch.

- 3 Click *Add* to display the New Blacklist Address dialog box.



For example, for [SpamCop](http://www.spamcop.net) (<http://www.spamcop.net>), you would use the following address:

```
b1.spamcop.net
```

- 4 Type the blacklist address in the *Address* box, then click *OK* to add the address to the *Blacklist Addresses* list.
- 5 If you have multiple blacklists in the *Blacklist Addresses* list, use the up-arrow and down-arrow to position the blacklists in the order you want them checked. The GWIA checks the blacklists in the order they are listed, from top to bottom.
- 6 Click *OK* to save your changes.

Overriding a Blacklist

In some cases, a blacklist might contain a host from which you still want to receive messages. For example, goodhost.com has been accidentally added to a blacklist but you still want to receive messages from that host.

You can use the *SMTP Incoming Exceptions* list on a class of service to override a blacklist. For information about editing or creating a class of service, see [Section 54.1.2, “Creating a Class of Service,”](#) on page 788.

54.2.2 Access Control Lists

If you want to block specific hosts yourself rather than use a blacklist (in other words, create your own blacklist), you can configure a class of service that prevents messages from those hosts. You do this on the GWIA object’s Access Control Settings page by editing the desired class of service to add the hosts to the *Prevent Messages From* exception list on the *SMTP Incoming* tab. For example, if you wanted to block all messages from badhost.com, you could edit the default class of service to add badhost.com to the list of prevented hosts.

You can also create a list of hosts that you always want to allow messages from, so you can create your own white list.

For information about editing or creating a class of service, see [Section 54.1.2, “Creating a Class of Service,”](#) on page 788.

54.2.3 Blocked.txt File

ConsoleOne creates a `blocked.txt` file that includes all the hosts that have been added to the *Prevent Messages From* exceptions list for the default class of service (see [Section 54.1, “Controlling User Access to the Internet,”](#) on page 787).

You can manually edit the `blocked.txt` file to add or remove hosts. To maintain consistency for your system, you can also copy the list to other GWIA installations.

To manually edit the `blocked.txt` file:

- 1 Open the `blocked.txt` file in a text editor.
- 2 Add the host addresses.

The entry format is:

```
address1  
address2  
address3
```

where *address* is either a hostname or an IP address. You can block on any octet. For example:

IP Address	Blocks
..*34	Any IP address ending with 34
172.16.*.34	Any IP address starting with 172.16 and ending with 34
172.16.10-34.*	Any IP address starting with 172.16 and any octet from 10 to 34

You can block on any segment of the hostname. For example:

Hostname	Blocks
provo*.novell.com	provo.novell.com provo1.novell.com provo2.novell.com
*.novell.com	gw.novell.com (but not novell.com itself)

There is no limit to the number of IP addresses and hostnames that you can block in the `blocked.txt` file

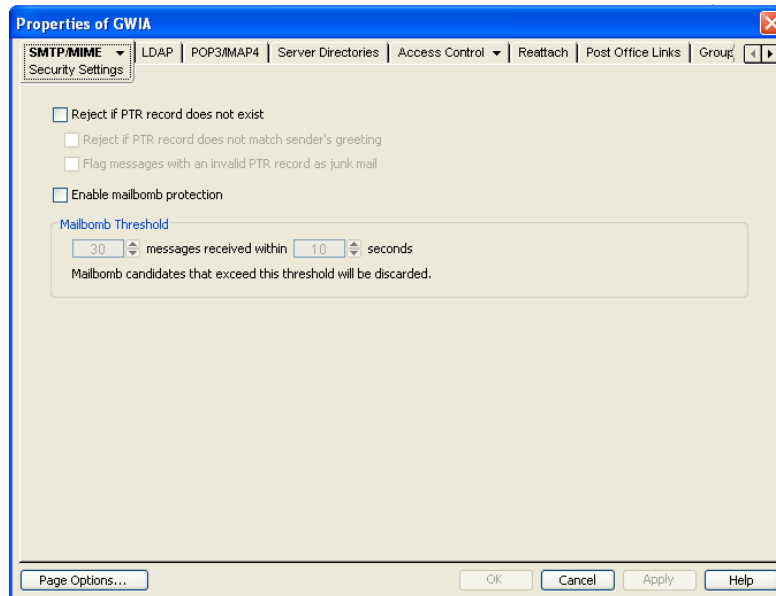
- 3 Save the file as `blocked.txt`.

54.2.4 Mailbomb (Spam) Protection

Multiple unsolicited messages (sometimes called a *mailbomb* or *spam*) from the Internet can potentially harm your GroupWise messaging environment. You can use the settings on the SMTP Security page to help protect your GroupWise system from malicious or accidental attacks.

To configure the SMTP security settings:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Security Settings*.



- 3 Fill in the fields:

Reject if PTR Record Does Not Exist: This setting lets you prevent messages if the sender's host is not authentic.

When this setting is turned on, the GWIA refuses messages from a smart host if a DNS reverse lookup shows that a PTR record does not exist for the IP address of the sender's host.

When this setting is turned off, the GWIA accepts messages from any host, but displays a warning if the initiating host is not authentic.

This setting corresponds with the GWIA's [/rejbs](#) switch.

- ♦ **Reject If PTR Record Does Not Match Sender's Greeting:** Select this option if you want the GWIA to reject messages from sending SMTP hosts where the sending host's PTR record does not match the information that the SMTP host sends out when it is initially contacted by another SMTP host. If the information does not match, the sending host might not be authentic.
- ♦ **Flag Messages with an Invalid PTR Record as Junk Mail:** Select this option to allow messages from unidentified sources to be handled by users' Junk Mail Handling settings in the GroupWise client rather than by being rejected by the GWIA. This gives users more control over what they consider to be junk mail.

Enable Mailbomb Protection: Mailbomb protection is turned off by default. You can turn it on by selecting this option.

Mailbomb Threshold: When you enable Mailbomb protection, default values are defined in the threshold settings. The default settings are 30 messages received within 10 seconds. You can change the settings to establish an acceptable security level.

Any group of messages that exceeds the specified threshold settings is entirely discarded. If you want to prevent future mailbombs from the mailbomb sender, identify the sender's IP address (by looking at the GWIA's console) and then modify the appropriate class of service to prevent mail being received from that IP address (*Access Control > Settings*). For more information, see [Section 54.1.2, "Creating a Class of Service," on page 788](#).

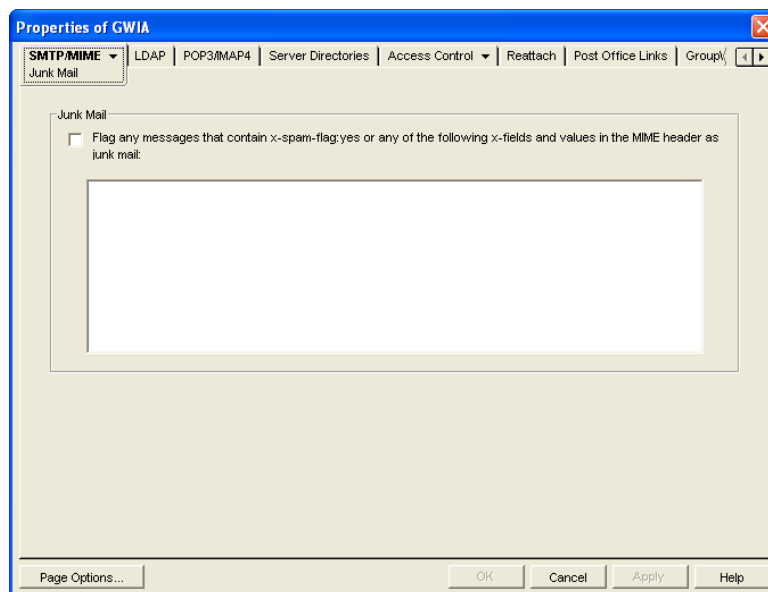
The time setting corresponds with the GWIA's [/mbtime](#) switch. The message count setting corresponds with the [/mbcount](#) switch.

- 4 Click *OK* to save the changes.

For additional protective startup switches, see [Section 59.6.13, "Mailbomb and Spam Security," on page 878](#).

54.2.5 Customized Spam Identification

- 1 In ConsoleOne, right-click the GWIA, then click *Properties*.
- 2 Click *SMTP/MIME > Junk Mail*.



- 3 Select *Flag Any Messages*, then specify the strings in the text box.

Anti-spam services use different indicators to mark potential spam. One might use a string of asterisks; the more asterisks, the greater the likelihood that the message is spam. Another might use a numerical value; the higher the number, the greater the likelihood that the message is spam. The following samples are taken from MIME headers of messages:

```
X-Spam-Results: ***** X-Spam-Status: score=9
```

Based on these samples, examples are provided below of lines that you could add to the list to handle the X-Spam tags found in the MIME headers of messages coming into your system.

Example: X-Spam-Results: *****

This line marks as spam any message whose MIME header contained an X-Spam-Results tag with five or more asterisks. Messages with X-Spam-Results tags with fewer than five asterisks are not marked as spam.

Example: X-Spam-Status: Yes

This line marks as spam any message whose MIME header contained the X-Spam-Status tag set to Yes, regardless of the score.

Example: X-Spam-Status: score=9 X-Spam-Status: score=10

These lines marks as spam any message whose MIME header has the X-Spam-Status tag set to Yes and had a score of 9 or 10. X-Spam-Status tags with scores less than 9 are not marked as spam.

You can add as many lines as necessary to the list to handle whatever message tagging your anti-spam service uses.

- 4 Click *OK* to save your list of strings.

The list is saved in the `xspam.cfg` file in the `domain\wpgate\gwia` directory. As described above, each line of the `xspam.cfg` file identifies an "X" header field that your anti-spam service is writing to the MIME header, along with the values that flag the message as spam. The GWIA examines the MIME header for any field listed in the `xspam.cfg` file. When a match occurs, the message is marked for handling by the GroupWise client Junk Mail Handling feature.

54.2.6 SMTP Host Authentication

The GWIA supports SMTP host authentication for both outbound and inbound message traffic.

- ♦ ["Outbound Authentication" on page 803](#)
- ♦ ["Inbound Authentication" on page 804](#)

Outbound Authentication

For outbound authentication to other SMTP hosts, the GWIA requires that the remote SMTP hosts support the AUTH LOGIN authentication method. To set up outbound authentication:

- 1 Include the remote SMTP host's domain name and authentication credentials in the `gwauth.cfg` file, located in the `domain\wpgate\gwia` directory. The format is:

```
domain_name authuser authpassword
```

For example:

```
smtp.novell.com remotehost novell
```

- 2 If you have multiple SMTP hosts that require authentication before they accept messages from your system, create an entry for each host. Make sure to include a hard return after the last entry.

- 3 If you want to allow the GWIA to send messages only to SMTP hosts listed in the `gwauth.cfg` file, use the following startup switch:

```
/forceoutboundauth
```

With the `--forceoutboundauth` switch enabled, if a message is sent to an SMTP host not listed in the `gwauth.cfg` file, the sender receives an Undeliverable message.

Inbound Authentication

For inbound authentication from other SMTP hosts, you can use the `--forceinboundauth` startup switch to ensure that the GWIA accepts messages only from SMTP hosts that use the AUTH LOGIN authentication method to provide a valid GroupWise user ID and password. The remote SMTP hosts can use any valid GroupWise user ID and password. However, for security reasons, we recommend that you create a dedicated GroupWise user account for remote SMTP host authentication.

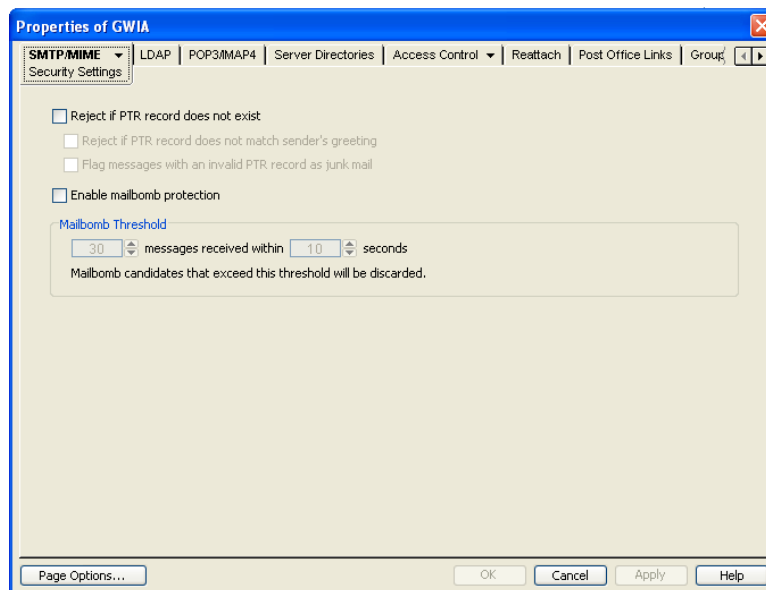
54.2.7 Unidentified Host Rejection

You can have the GWIA reject messages from unidentified sources. The GWIA refuses messages from a host if a DNS reverse lookup shows that a “PTR” record does not exist for the IP address of the sender’s host.

If you choose not to have the GWIA reject messages from unidentified hosts, it accepts messages from any host, but it displays a warning if the sender’s host is not authentic.

To configure the GWIA to reject messages from unidentified hosts:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *SMTP/MIME > Security Settings* to display the Security Settings page.



- 3 Turn on the *Reject Mail if Sender's Identity Cannot Be Verified* option. This setting corresponds with the GWIA's `--rejbs` switch.
- 4 Click *OK* to save your changes.

54.3 Tracking Internet Traffic with Accounting Data

The GWIA can supply accounting information for all messages, including information such as the message's source, priority, size, and destination.

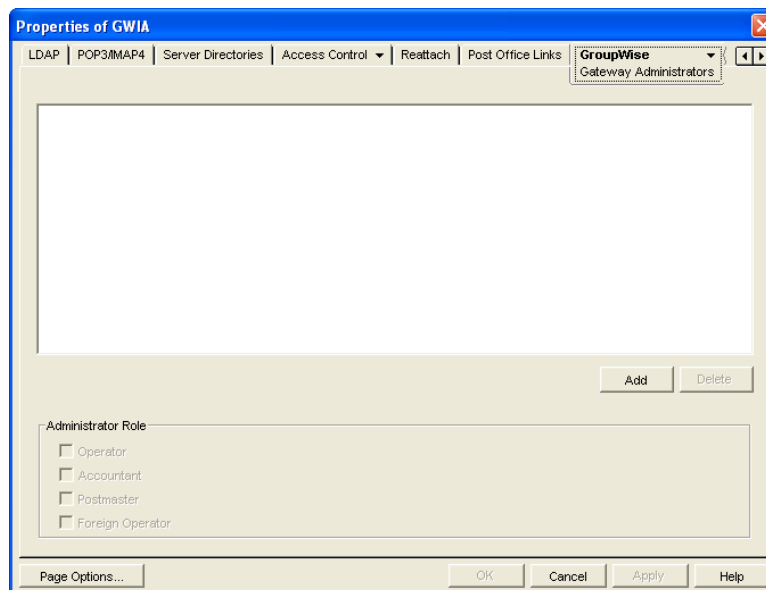
The accounting file is an ASCII-delimited text file that records the source, priority, message type, destination, and other information about each message sent through the gateway. The file, which is updated daily at midnight (and each time the GWIA restarts), is called `acct` and is located in the `xxx.prc` directory. If no accountant is specified for the gateway in ConsoleOne, the file is deleted and re-created each day. Follow the steps below to set up accounting.

- ♦ Section 54.3.1, "Selecting an Accountant," on page 805
- ♦ Section 54.3.2, "Enabling Accounting," on page 806
- ♦ Section 54.3.3, "Understanding the Accounting File," on page 807
- ♦ Section 54.3.4, "Generating an Accounting Report," on page 808

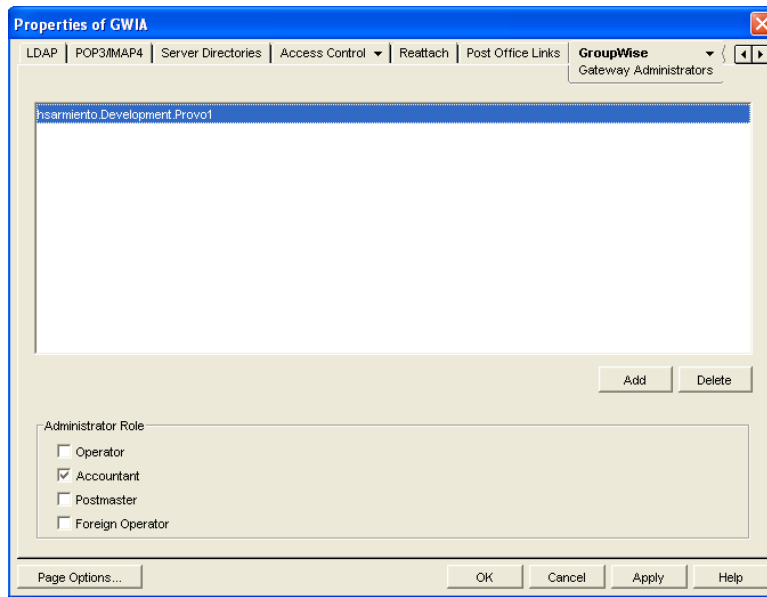
54.3.1 Selecting an Accountant

You can select one or more GroupWise users to be accountants. Every day at midnight, each accountant receives an accounting file (`acct`) that contains information about the messages the gateway sent that day.

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Gateway Administrators* to display the Gateway Administrators page.



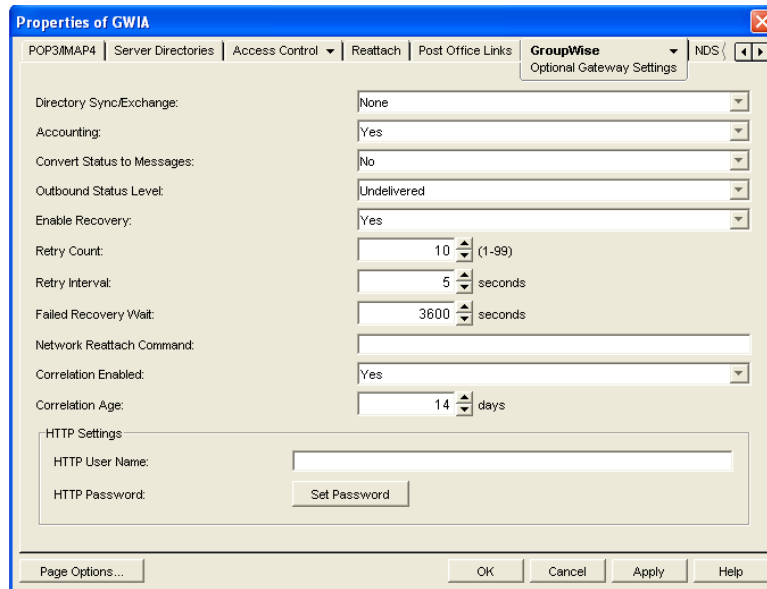
- 3 Click *Add*, browse for and select the user you want to add, then click *OK* to add the user to the list of administrators.
- 4 Select the user in the list of administrators, then click *Accountant*.



5 Click *OK* to save the changes.

54.3.2 Enabling Accounting

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Optional Gateway Settings* to display the Optional Gateway Settings page.



- 3 Set *Accounting* to *Yes*.
- 4 Set *Correlation Enabled* to *Yes*.
- 5 Click *OK*.

54.3.3 Understanding the Accounting File

The following is an Accounting file entry for a single event. Each field in the entry is described below.

```
O,1/25/2010,21:58:39,3DE29CD2.14E:7:6953,
Mail,2,Provo,Research,jsmith,48909,Meeting
Agenda,Provo,GWIA,sde23a9f.001,MIME,hjones@novell.com,1,2,11388,0
```

Field	Example	Description
<i>Inbound/Outbound</i>	O	Displays I for inbound messages and O for outbound messages
<i>Date</i>	1/25/2012	The date the message was processed.
<i>Time</i>	21:58:39	The time the message was processed.
<i>GroupWise message ID</i>	3DE29CD2.14E:7:6953	The unique GroupWise ID assigned to the message.
<i>GroupWise message type</i>	Mail	Mail message, appointment, task, note, or phone message for outbound messages. Unknown for inbound messages.
<i>GroupWise message priority</i>	2	High priority = 1 Normal priority = 2 Low priority = 3
<i>GroupWise user's domain</i>	Provo	The domain in which the GroupWise user resides.
<i>GroupWise user's post office</i>	Research	The post office where the GroupWise user's mailbox resides.
<i>GroupWise user's ID</i>	jsmith	The GroupWise user's ID. For outbound messages, the GroupWise user is the message sender. For inbound messages, the GroupWise user is the message recipient.
<i>GroupWise user's account ID</i>	48909	The GroupWise user's account ID. The account ID is assigned on the user's GroupWise Account page (<i>User object > GroupWise > Account</i>).
<i>Message subject</i>	Meeting Agenda	The message's Subject line. Only the first 32 characters are displayed.
<i>Gateway domain</i>	Provo	The domain where the GWIA resides.
<i>Gateway name</i>	GWIA	The GWIA's name.
<i>Foreign message ID</i>	sde23a9f.001	A unique ID for outbound messages. The identifier before the period (sde23a9f) uniquely identifies a message. The identifier after the period (001) is incremented by one for each message sent.
<i>Foreign message type</i>	MIME	The message type (MIME, etc.)
<i>Foreign user's address</i>	hjones@novell.com	The foreign user's email address. For inbound messages, the foreign user is the message sender. For outbound messages, the foreign user is the message recipient.

Field	Example	Description
<i>Recipient count</i>	1	The number of recipients.
<i>Attachment count</i>	2	The number of attached files. The total count includes the message.
<i>Message size</i>	11388	The total size, in bytes, of the message and its attachments.
<i>Other</i>	0	Not used.

54.3.4 Generating an Accounting Report

You can use the Monitor Agent to generate a report based on the contents of this file. For more information, see [Section 71.3.10, "Gateway Accounting Report," on page 988](#).

55 Configuring the GWIA

For GWIA system requirements, see “[Internet Agent System Requirements](#)” in the *GroupWise 2012 Installation Guide*. For detailed instructions about installing and starting the GWIA for the first time, see “[Installing the GroupWise Internet Agent](#)” in the *GroupWise 2012 Installation Guide*.

As your GroupWise system grows and evolves, you might need to modify your GWIA configuration to meet the changing needs of your system.

- ♦ [Section 55.1, “Changing the Link Protocol between the GWIA and the MTA,”](#) on page 809
- ♦ [Section 55.2, “Configuring an Alternate GWIA for a Domain,”](#) on page 810
- ♦ [Section 55.3, “Binding the GWIA to a Specific IP Address,”](#) on page 811
- ♦ [Section 55.4, “Securing GWIA Connections with SSL,”](#) on page 812

55.1 Changing the Link Protocol between the GWIA and the MTA

Originally, the GWIA and the MTA communicated by transferring message files through message queue directories, as shown in the following diagrams in *GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure*:

- ♦ “[Mapped/UNC Link Open: Outbound Transfer to the Internet Successful](#)”
- ♦ “[Mapped/UNC Link Open: Inbound Transfer from the Internet Successful](#)”

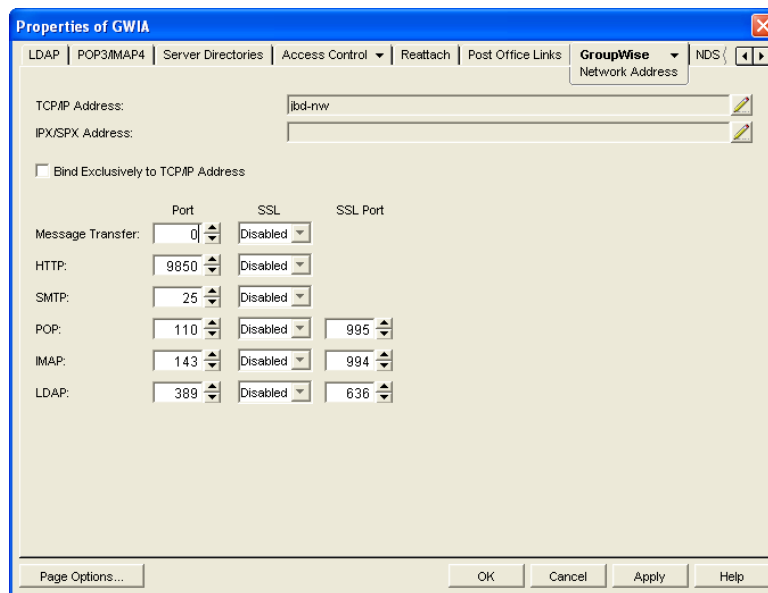
Currently, you can also configure the GWIA so that it uses TCP/IP to communicate with the MTA, instead of message files, as shown in the following diagrams:

- ♦ “[TCP/IP Link Open: Outbound Transfer to the Internet Successful](#)”
- ♦ “[TCP/IP Link Open: Inbound Transfer from the Internet Successful](#)”

During installation of the GWIA, you had the opportunity to choose between a direct link (message files) and a TCP/IP link. A direct link is appropriate when the GWIA and the MTA are on the same server. A TCP/IP link is preferable if they are on different servers. If you did not choose the TCP/IP link during installation, you can configure the GWIA to use TCP/IP at any time.

If you want to enable TCP/IP communication between the GWIA and the MTA, use port number 7102 or another available port number. If you do not want to enable TCP/IP communication, use 0 (zero) as the port number.

- 1 In ConsoleOne, right-click the GWIA, then click *Properties*.
- 2 Click *GroupWise > Network Address*.



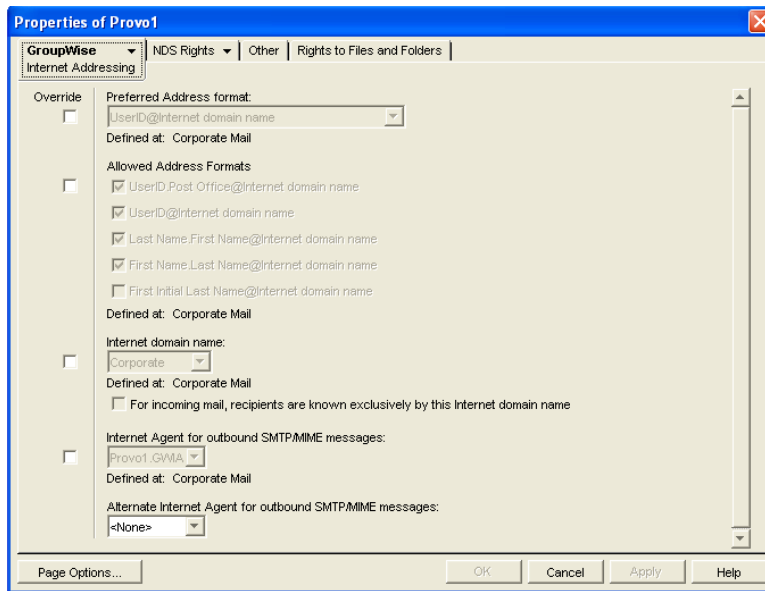
- 3 In the *TCP/IP Address* field, click *Edit*, specify the IP address of the server where the GWIA is running, then click *OK* to return to the Network Address page.
- 4 In the *Message Transfer Port* field, specify a unique port number; for example, 7102.
- 5 Click *OK* to save the new link configuration for the GWIA.

ConsoleOne then notifies the GWIA and MTA to restart using the new link protocol.

55.2 Configuring an Alternate GWIA for a Domain

By configuring the GWIA to communicate with the MTA by way of TCP/IP, you can configure an alternate GWIA for a domain, so that if the domain's primary GWIA goes down, the MTA can fail over to another GWIA in your GroupWise system until the primary GWIA is up and running again. This feature is especially useful in large GroupWise systems with multiple GWIAs that handle a lot of Internet messages.

- 1 Make sure that you have configured the GWIAs for TCP/IP, as described in [Changing the Link Protocol between the GWIA and the MTA](#).
- 2 In ConsoleOne, right-click the Domain object, then click *Properties*.
- 3 Click *GroupWise > Internet Addressing*.



- 4 In the *Alternate Internet Agent for Outbound SMTP/MIME Messages* field, select an GWIA as an alternate for this domain.
- 5 Click *OK* to save your changes.

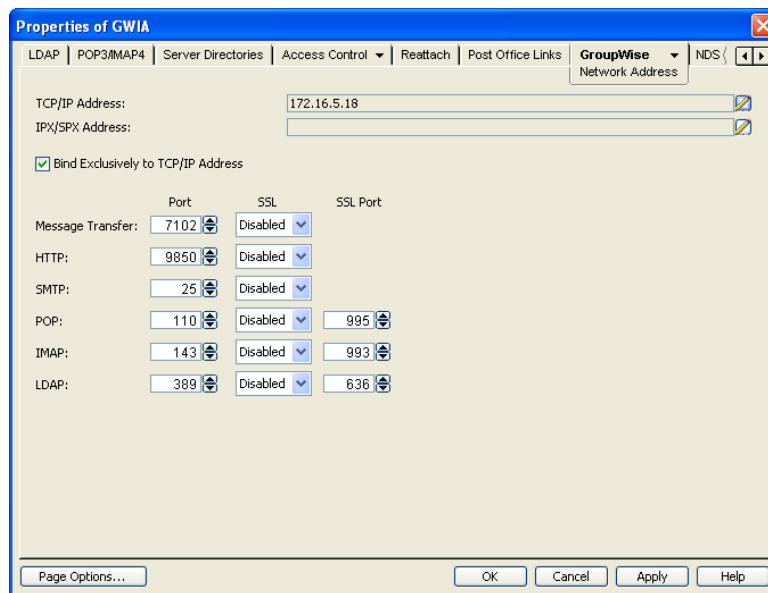
The MTA always tries to transfer outbound Internet messages to the primary GWIA first, so after an outage the primary GWIA automatically resumes its normal processing for the domain.

55.3 Binding the GWIA to a Specific IP Address

By default, the GWIA binds to a specified IP address when the server where it runs uses multiple IP addresses. The specified IP address is associated with all ports used by the agent. Without an exclusive bind, the GWIA binds to all IP addresses available on the server.

To turn off the exclusive bind:

- 1 In ConsoleOne, browse to and right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.



3 Deselect *Bind Exclusively to TCP/IP Address*, then click *OK* to save your change.

You can use the `/ip` startup switch in the GWIA startup file to establish an exclusive bind to the specified IP address. If you have used this switch in the GWIA startup file, remove it to turn off the exclusive bind.

55.4 Securing GWIA Connections with SSL

The GWIA can use the SSL (Secure Socket Layer) protocol to enable secure connections to other SMTP hosts, POP/IMAP clients, and the GWIA Web console. For the GWIA to do so, you must ensure that it has access to a server certificate file and that you have configured the connection types (SMTP, POP, IMAP, HTTP) you want secured through SSL. The following sections provide instructions:

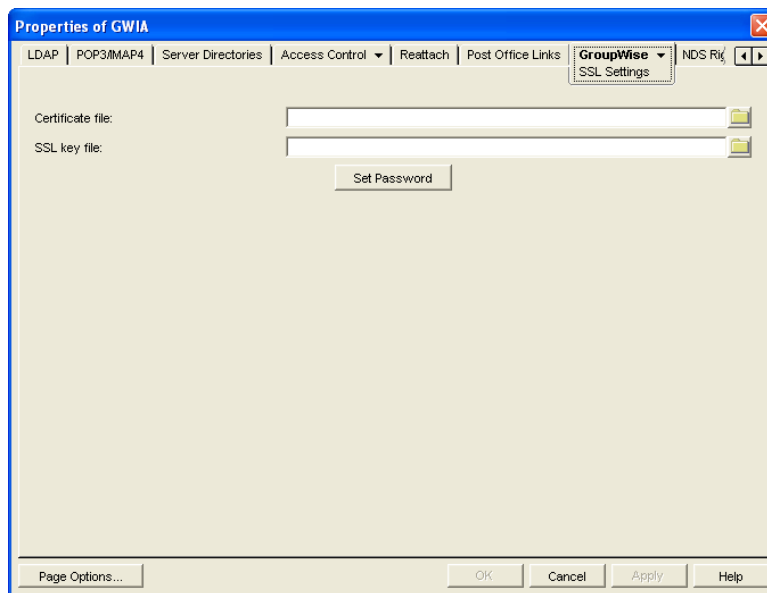
- ♦ [Section 55.4.1, “Defining the Certificate File,” on page 812](#)
- ♦ [Section 55.4.2, “Defining Which Connections Use SSL,” on page 813](#)

55.4.1 Defining the Certificate File

To use SSL, the GWIA requires access to a server certificate file and key file. The GWIA can use any Base64/PEM or PFX formatted certificate file located on its server. If the GWIA’s server does not have a server certificate file, you can use the GroupWise Generate CSR utility to help you obtain one. For information, see [Section 5.16.4, “GroupWise Generate CSR Utility \(GWCSRGEN\),” on page 104](#).

To define the certificate file and key file that the GWIA will use:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > SSL Settings* to display the SSL Settings page.



For background information about certificate files and SSL key files, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107.

By default, the GWIA looks for the certificate file and SSL key file in the same directory where the GWIA executable is located, unless you provide a full path name.

- 3 Fill in the *Certificate File*, *SSL Key File*, and *Set Password* fields:

Certificate File: Specify the server certificate file that the GWIA will use. The certificate file must be in Base64/PEM or PFX format. This setting corresponds to the GWIA’s `--certfile` switch.

SSL Key File: Specify the key file associated with the certificate. The key file must be password protected in order for SSL to function correctly. If the private key is included in the certificate file rather than in a separate key file, leave this field blank. This setting corresponds to the GWIA’s `--keyfile` switch.

Set Password: Click *Set Password* to specify the password for the key. If the key does not require a password, do not use this option. This setting corresponds to the `--keypasswd` switch.

- 4 If you want to define which connections (HTTP, SMTP, POP3, or IMAP4) use SSL, click *Apply* to save your changes, then continue with the next section, [Section 55.4.2, “Defining Which Connections Use SSL,”](#) on page 813.

or

Click *OK* to save your changes.

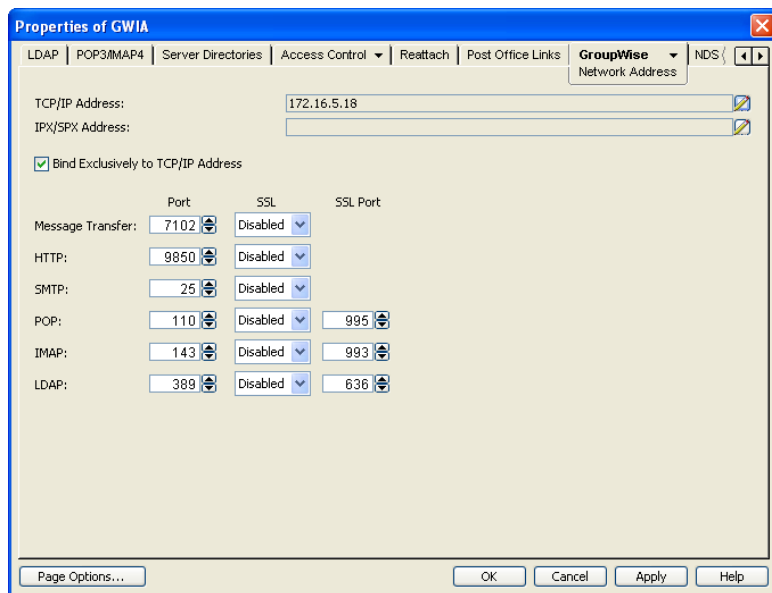
55.4.2 Defining Which Connections Use SSL

After you define the GWIA’s certificate and key file (see [Section 55.4.1, “Defining the Certificate File,”](#) on page 812), you can configure which connections you want to use SSL. You can enable SSL connections to other SMTP hosts and the GWIA Web console, which means that an SSL connection is used if the other SMTP host or the Web browser (running the Web console) supports SSL. You can also enable or require SSL connections to POP3, IMAP4, and LDAP clients. If SSL is enabled, an SSL connection is used if the client supports SSL; if SSL is required, only SSL connections are accepted.

For more information about POP3 and IMAP4 clients, see [Section 53.2, “Configuring POP3/IMAP4 Services,”](#) on page 777. For more information about LDAP clients, see [Section 53.3, “Configuring LDAP Services,”](#) on page 782.

To configure connections to use SSL:

- 1 In ConsoleOne, if the GWIA object's property pages are not already displayed, right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.



- 3 Configure the SSL settings for the following connections:

Message Transfer: Select *Required* if you want the GWIA to use a secure connection to the MTA. The MTA must also be enabled to use SSL.

HTTP: Select *Enabled* to enable the GWIA to use a secure connection when passing information to the GWIA Web console. The Web browser must also be enabled to use SSL; if it is not, a non-secure connection is used.

SMTP: Select from the following options to configure the GWIA's use of secure connections to other SMTP hosts. The SMTP host must also be enabled to use SSL or TLS (Transport Layer Security); if it is not, a non-secure connection is used. All connections are through port 25.

- ◆ **Disabled:** The GWIA does not support SSL connections.
- ◆ **Enabled:** The other SMTP host determines whether an SSL connection or non-SSL connection is used with an SSL-enabled GWIA.
- ◆ **Required:** The GWIA forces SSL connections. Non-SSL connections are denied.

POP: Select from the following options to configure the GWIA's use of secure connections to POP clients:

- ◆ **Disabled:** The GWIA does not support SSL connections. All connections are non-SSL through port 110.
- ◆ **Enabled:** The POP client determines whether an SSL connection or non-SSL connection is used with an SSL-enabled GWIA. An SSL-enabled GWIA allows SSL connections on port 995 and non-SSL connections on port 110.
- ◆ **Required:** The GWIA forces SSL connections on port 995 and port 110. Non-SSL connections are denied.

IMAP: Select from the following options to configure the GWIA's use of secure connections to IMAP clients:

- ◆ **Disabled:** The GWIA does not support SSL connections. All connections are non-SSL through port 143.
- ◆ **Enabled:** The IMAP client determines whether an SSL connection or non-SSL connection is used with an SSL-enabled GWIA. An SSL-enabled GWIA allows SSL connections on port 993 and non-SSL connections on port 143.
- ◆ **Required:** The GWIA forces SSL connections on port 993 and port 143. Non-SSL connections are denied.

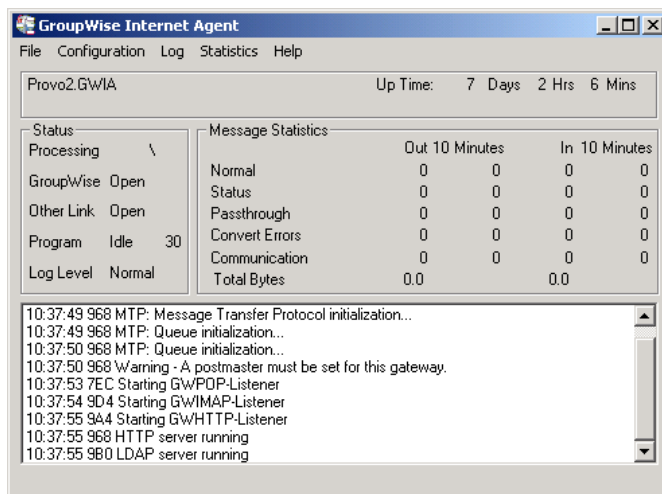
56 Monitoring the GWIA

You can monitor the operation of the GWIA by using several different diagnostic tools. Each provides important and helpful information about the status of the GWIA and how it is currently functioning. Choose from the titles listed below to learn more about how to monitor the operations of the GWIA.

- ◆ [Section 56.1, “Using the GWIA Server Console,” on page 817](#)
- ◆ [Section 56.2, “Using the GWIA Web Console,” on page 827](#)
- ◆ [Section 56.3, “Using Novell Remote Manager,” on page 829](#)
- ◆ [Section 56.4, “Using an SNMP Management Console,” on page 829](#)
- ◆ [Section 56.5, “Assigning Operators to Receive Warning and Error Messages,” on page 832](#)
- ◆ [Section 56.6, “Using GWIA Log Files,” on page 833](#)
- ◆ [Section 56.7, “Using GWIA Error Message Documentation,” on page 837](#)
- ◆ [Section 56.8, “Employing GWIA Troubleshooting Techniques,” on page 837](#)
- ◆ [Section 56.9, “Stopping the GWIA,” on page 838](#)

56.1 Using the GWIA Server Console

The GWIA console provides information, status, and message statistics about the GWIA to help you assess its current functioning.



Linux: You must use the `--show` startup switch in order to display the Linux GWIA server console.

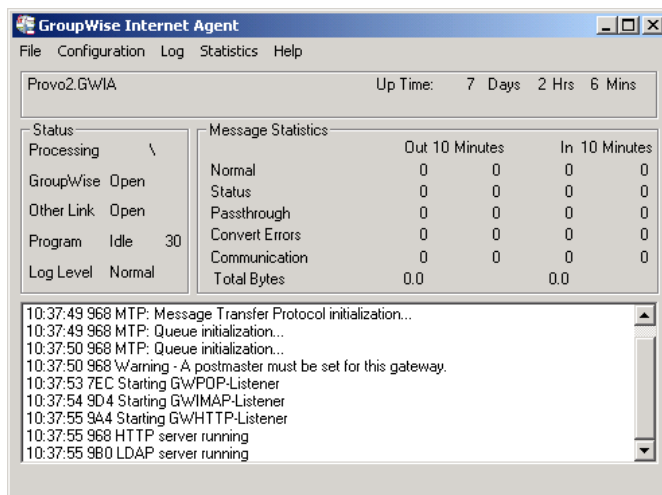
Windows: If the GWIA is running as a Windows service under the Local System User, it is displayed on the desktop only if the *Allow Service to Interact with Desktop* option was selected during installation or has been configured on the GWIA service's General property page.

Refer to the following sections for information about the specific sections and functionality included in the console:

- ◆ Section 56.1.1, “Description,” on page 818
- ◆ Section 56.1.2, “Status,” on page 818
- ◆ Section 56.1.3, “Statistics,” on page 819
- ◆ Section 56.1.4, “Logging,” on page 825
- ◆ Section 56.1.5, “Menu Functions,” on page 826

56.1.1 Description

The description section of the console identifies the GWIA and displays how long its has been running.



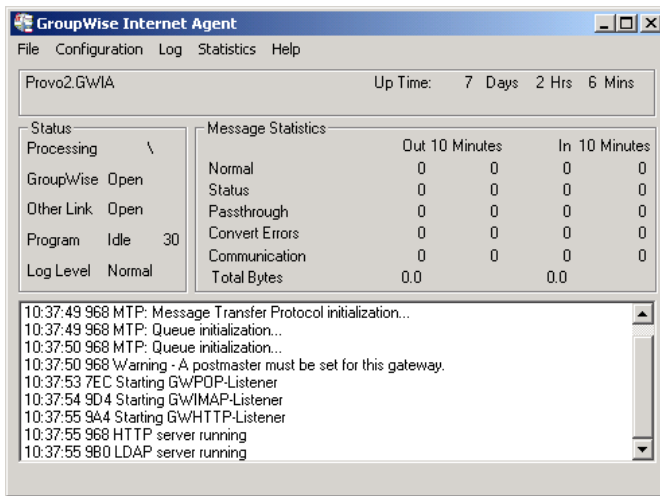
Domain.Gateway: Displays the domain and GWIA names.

Up Time: Displays the total length of time the GWIA has been running. If the GWIA terminates unexpectedly (such as in a power outage), the *Up Time* display does not reset to 0 (zero). It shows the total time elapsed since the GWIA was last loaded after a proper termination.

Description: Displays any descriptive information provided on the GWIA object’s Identification page (GWIA object > *GroupWise* > *Identification*).

56.1.2 Status

The *Status* section of the console provides a quick look at the GWIA’s current message processing activity, network connectivity, and information logging level.



Processing: Displays a rotating bar if the GWIA is running. If there is no bar, or if the bar is stationary for more than one minute, the GWIA is not running.

GroupWise: Displays whether the GWIA's network connection is OPEN or CLOSED. This network connection is the GWIA's only link to GroupWise. The status indicates whether or not the GWIA can write to the `wpcsin` directory and access the `wpcout` directory. The GWIA does a scan each cycle to see if these directories exist. If the status is CLOSED, the GWIA attempts to reattach to the network.

It is normal for this field to display the word CLOSED for a minute or so after you start the GWIA. However, if the connection remains CLOSED, look for the `wpcsin` and `wpcout` directories. If they are not created yet, start the Message Transfer Agent (MTA).

Other Link: This field does not apply to the GWIA. It always says OPEN.

Program: Displays the processing cycle. You can use the Gateway Time Settings page (GWIA object > *GroupWise* > *Gateway Time Settings*) to adjust the processing cycle.

Log Level: Displays the logging level the GWIA is currently using. The logging level determines how much data is displayed on the message portion of this screen and written to the log file. You can use the console menu options to override the default setting for the current session. For information, see

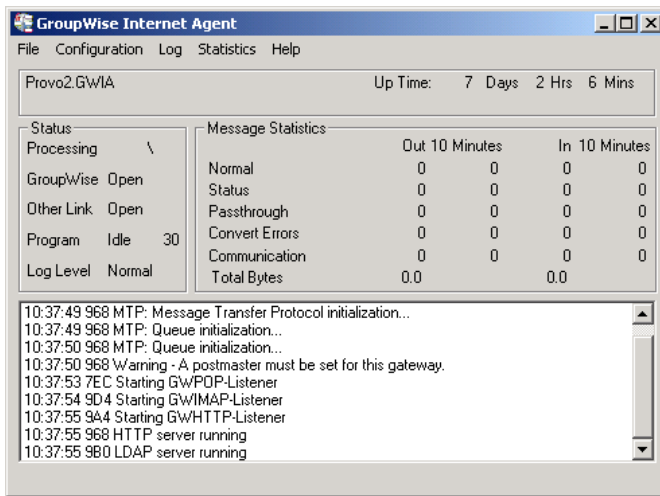
56.1.3 Statistics

The *Statistics* section of the console can display five different sets of information:

- ♦ ["Message Statistics" on page 819](#)
- ♦ ["SMTP Service Statistics" on page 820](#)
- ♦ ["POP Service Statistics" on page 822](#)
- ♦ ["IMAP Service Statistics" on page 823](#)
- ♦ ["LDAP Service Statistics" on page 825](#)

Message Statistics

The *Message Statistics* section of the console, shown below, is the default statistics section displayed by the GWIA console.



Message Statistics shows the number of inbound and outbound messages processed by the GWIA. The *Out* and *In* columns display the cumulative message totals and the *10 Minutes* column display snapshot totals for the last ten minutes. You change the time interval of the *10 Minutes* column in ConsoleOne. For instructions, see [Section 57.2.2, “Increasing Polling Time,”](#) on page 841.

Normal: Displays the number of inbound and outbound messages processed by the GWIA.

Status: Displays the number of inbound and outbound status messages processed by the GWIA. The amount of status message traffic depends on the Outbound Status level (GWIA object > *GroupWise* > *Optional Gateway Settings*). If the Outbound Status level is set to Full, more status messages are generated. If the Outbound Status level is set to Undelivered, fewer status messages are generated.

Passthrough: Displays the number of inbound and outbound passthrough messages the GWIA has processed.

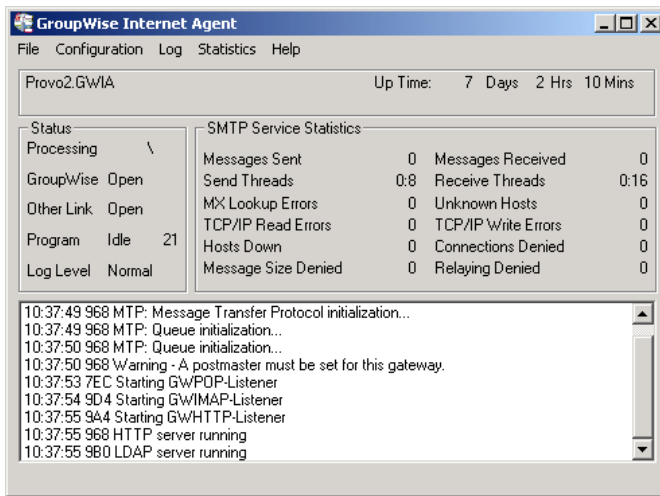
Convert Errors: Outbound messages are converted from GroupWise format to MIME or RFC-822 format. Inbound messages are converted to GroupWise format. This field displays the number of inbound and outbound messages that the GWIA could not convert.

Communication: Displays the number of communication errors encountered by the GWIA.

Total Bytes: Displays the total number of bytes of inbound and outbound messages processed by the GWIA.

SMTP Service Statistics

The *SMTP Service Statistics* section, shown below, includes only the information for messages processed by the GWIA’s SMTP daemon.



Messages Sent: Displays the total number of SMTP messages sent by the GWIA during its current up time.

Send Threads: The first number displays the number of threads currently being used to send SMTP messages. The second number displays the number of threads still available to the GWIA for sending SMTP messages. This is the total number of assigned send threads (by default, 8) minus the currently used threads. You can change the total number of assigned SMTP send threads in ConsoleOne (GWIA object > *SMTP/MIME* > *Settings*). For more information, see [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,”](#) on page 757.

Messages Received: Displays the total number of SMTP messages received by the GWIA during its current up time.

Receive Threads: The first number is the number of threads currently being used to receive SMTP messages. The second number is the number of threads still available to the GWIA for receiving SMTP messages. This is the total number of assigned receive threads (by default, 16) minus the currently used threads. You can change the total number of assigned SMTP receive threads in ConsoleOne (GWIA object > *SMTP/MIME* > *Settings*). For more information, see [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,”](#) on page 757.

MX Lookup Errors: To resolve hostnames to IP addresses, the GWIA performs MX record lookups in DNS. This field displays the number of MX record lookups that failed.

Unknown Hosts: Displays the number of SMTP hosts that the GWIA could not establish a connection with because the hostname could not be resolved to an IP address.

TCP/IP Read Errors: Displays the number of TCP read errors encountered by the GWIA. A TCP read error occurs if the GWIA connects successfully to another SMTP host but is unable to process a TCP read command during the message transfer.

TCP/IP Write Errors: Displays the number of TCP write errors encountered by the GWIA. A TCP write error occurs if the GWIA connects successfully to another SMTP host but is unable to process a TCP write command during the message transfer.

Hosts Down: Displays the number of SMTP hosts that the GWIA could not establish a connection with in order to send or receive messages. The GWIA was able to resolve the hostname to an IP address, but the connection could not be established.

Connections Denied: Displays the number of connections denied by the GWIA. A connection is denied if the host is blocked through:

- ♦ A Class of Service (GWIA object > *Access Control* > *Settings*). For more information, see [Chapter 54.1, “Controlling User Access to the Internet,”](#) on page 787.
- ♦ A blacklist (GWIA object > *Access Control* > *Blacklists*). For more information, see [Chapter 54.2, “Blocking Unwanted Email from the Internet,”](#) on page 798.
- ♦ The Reject Mail if Sender’s Identity Cannot Be Verified setting (GWIA object > *SMTP/MIME* > *Security Settings*), if it is enabled and the sender’s identity cannot be verified. For more information, see [Section 54.2.4, “Mailbomb \(Spam\) Protection,”](#) on page 801.

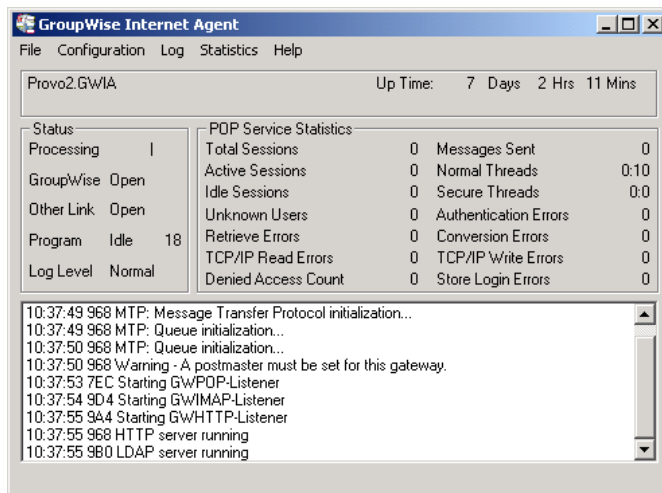
Message Size Denied: Displays the number of SMTP messages that the GWIA did not send or receive because they exceeded the maximum message size. You can change the maximum message size in ConsoleOne (GWIA object > *Access Control* > *Settings* > edit class of service > *SMTP Incoming* tab or *SMTP Outgoing* tab). For more information, see [Section 54.1, “Controlling User Access to the Internet,”](#) on page 787.

Relaying Denied: Displays the number of relay messages denied by the GWIA. A relay message is denied for the following reasons:

- ♦ The GWIA is not enabled as a relay host (GWIA object > *Access Control* > *SMTP Relay Settings*). For more information, see [Section 53.1.8, “Enabling SMTP Relaying,”](#) on page 770.
- ♦ The relay message could not be authenticated.

POP Service Statistics

The *POP Service Statistics* section, shown below, provides information about the POP activity handled by the GWIA.



Total Sessions: Displays the total number of POP3 sessions processed by the GWIA during its current up time.

Active Sessions: Displays the number of currently active POP3 sessions.

Idle Sessions: Displays the number of threads still available to the GWIA for POP3 sessions. This is the total number of assigned POP3 threads (by default, 10) minus the active sessions. You can change the total number of assigned POP3 threads in ConsoleOne (GWIA object > *POP3/IMAP4* > *Settings*). For more information, see [Section 53.2, “Configuring POP3/IMAP4 Services,”](#) on page 777.

Messages Sent: Displays the total number of GroupWise mailbox messages retrieved through POP3 sessions.

Normal Threads: Displays the number of POP threads that are busy and the number that are available.

Secure Threads: Displays the number of POP SSL threads that are busy and the number that are available.

Unknown Users: Displays the number of user logins that failed because the user does not exist in the GroupWise system.

Authentication Errors: Displays the number of GroupWise user logins that failed because the user supplied an incorrect password.

Retrieve Errors: Displays the number of errors generated because the GWIA could not transfer messages to the POP3 client.

Conversion Errors: Displays the number of errors generated because the GWIA could not convert retrieved GroupWise messages to MIME format.

TCP/IP Read Errors: Displays the number of TCP read errors encountered by the GWIA. A TCP read error occurs if the GWIA successfully opens a POP3 session but is unable to process a TCP read command during the session.

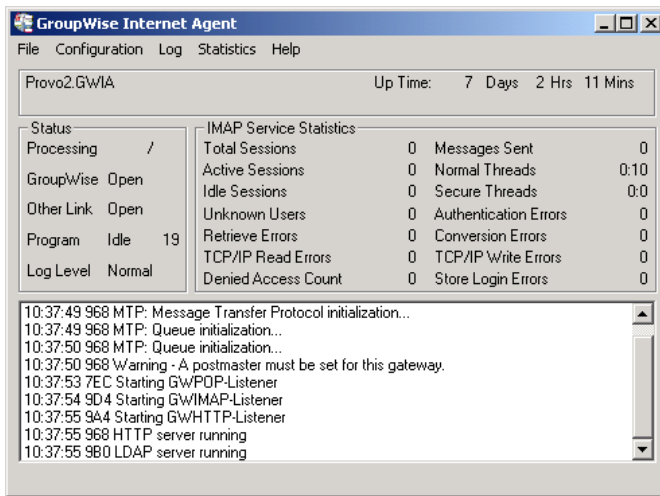
TCP/IP Write Errors: Displays the number of TCP write errors encountered by the GWIA. A TCP write error occurs if the GWIA successfully opens a POP3 session but is unable to process a TCP write command during the session.

Denied Access Count: Displays the number of POP3 sessions that were denied because the user does not have POP3 access. POP3 access is controlled through the user's Class of Service assignment (GWIA object > *Access Control* > *Settings*). For more information, see [Section 54.1, "Controlling User Access to the Internet,"](#) on page 787.

Store Login Errors: Displays the number of GroupWise user logins that failed because the users' GroupWise mailboxes were unavailable (for example, the post office is down or the GWIA link to the post office is down).

IMAP Service Statistics

The *IMAP Service Statistics* section, shown below, provides information about the IMAP activity handled by the GWIA.



Total Sessions: Displays the total number of IMAP4 sessions processed by the GWIA during its current up time.

Active Sessions: Displays the number of currently active IMAP4 sessions.

Sessions Available: Displays the number of threads still available to the GWIA for IMAP4 sessions. This is the total number of assigned IMAP4 threads (by default, 10) minus the active sessions. You can change the total number of assigned IMAP4 threads in ConsoleOne (GWIA object > POP3/IMAP4 > Settings). For more information, see [Section 53.2, “Configuring POP3/IMAP4 Services,” on page 777](#).

Messages Sent: Displays the total number of GroupWise mailbox messages retrieved through IMAP4 sessions.

Normal Threads: Displays the number of IMAP threads that are busy and the number that are available.

Secure Threads: Displays the number of IMAP SSL threads that are busy and the number that are available.

Unknown Users: Displays the number of user logins that failed because the user does not exist in the GroupWise system.

Authentication Errors: Displays the number of GroupWise user logins that failed because the user supplied an incorrect password.

Retrieve Errors: Displays the number of errors generated because the GWIA could not transfer messages to the IMAP4 client.

Conversion Errors: Displays the number of errors generated because the GWIA could not convert retrieved GroupWise messages to MIME format.

TCP/IP Read Errors: Displays the number of TCP read errors encountered by the GWIA. A TCP read error occurs if the GWIA successfully opens a IMAP4 session but is unable to process a TCP read command during the session.

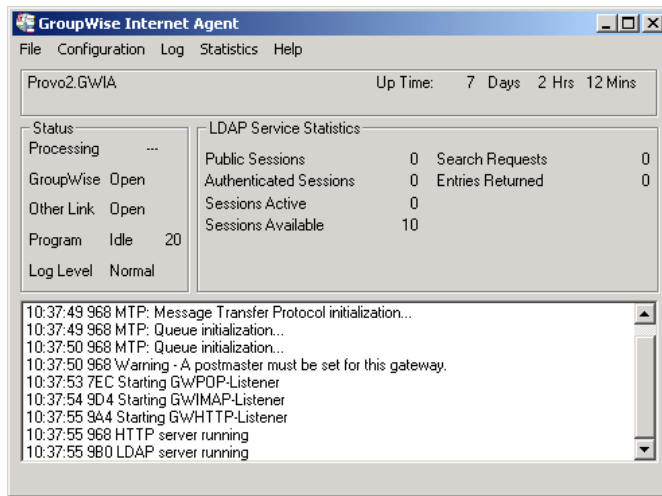
TCP/IP Write Errors: Displays the number of TCP write errors encountered by the GWIA. A TCP write error occurs if the GWIA successfully opens an IMAP4 session but is unable to process a TCP write command during the session.

Denied Access Count: Displays the number of IMAP4 sessions that were denied because the user does not have IMAP4 access. IMAP4 access is controlled through the user's Class of Service assignment (GWIA object > *Access Control* > *Settings*). For more information, see [Section 54.1, "Controlling User Access to the Internet,"](#) on page 787.

Store Login Errors: Displays the number of GroupWise user logins that failed because the users' GroupWise mailboxes were unavailable (for example, the post office is down or the GWIA link to the post office is down).

LDAP Service Statistics

The *LDAP Service Statistics* section, shown below, provides information about the LDAP activity handled by the GWIA.



Public Sessions: Displays the total number of LDAP sessions handled by the GWIA.

Authenticated Sessions: This field is not used.

Sessions Active: Displays the total number of LDAP sessions currently being processed by the GWIA.

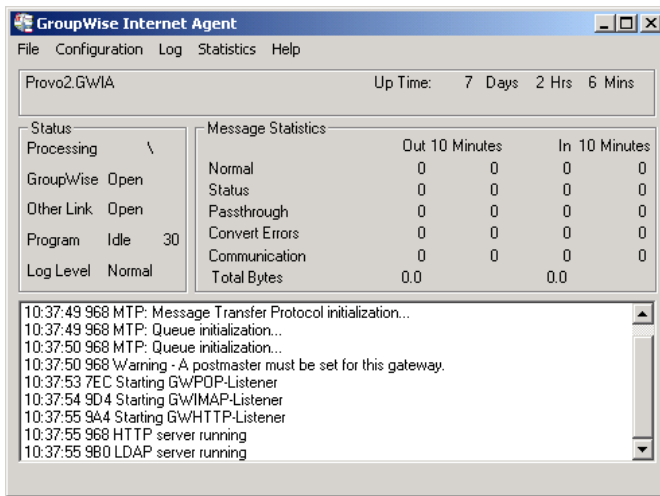
Sessions Available: Displays the number of threads still available to the GWIA for LDAP sessions. This is the total number of assigned LDAP threads (by default, 10) minus the active sessions. You can change the total number of assigned LDAP threads in ConsoleOne (GWIA object > *LDAP* > *Settings*). For more information, see [Section 53.3, "Configuring LDAP Services,"](#) on page 782.

Search Requests: Displays the total number of LDAP queries against the GroupWise Address Book.

Entries Returned: Displays the total number of Address Book entries returned for the search requests. For example, a single search request might return 25 entries.

56.1.4 Logging

The *Logging* section of the console, shown below, displays GWIA activity. The number and detail of these messages depend on the logging level you select. See [Chapter 56.6, "Using GWIA Log Files,"](#) on page 833 for more information.



56.1.5 Menu Functions

The menu functions on the Linux and Windows GWIA console provide you with the following options.

File > Restart (F6): Select this option to restart the GWIA. The GWIA rereads all of its configuration files ([gwia.cfg](#), [blocked.txt](#), [gwauth.cfg](#), [route.cfg](#) and so on).

File > Exit: Select this option to terminate the GWIA and return to the system prompt.

Configuration > Agent Settings: Select this option to display the GWIA configuration settings.

Configuration > Message Transfer Status: Select this option to display the status of the TCP/IP link between the GWIA and the MTA for the domain.

Configuration > Edit Startup File: Select this option to open the `gwia.cfg` file in the default text editor.

Log > Cycle Log: Select this option to close the current log file and start a new one.

Log > View Log: Select this option to view the log files.

Log > Log Settings: Select this option to set the logging level, turn on or off disk logging, and configure the maximum log file size and disk space. These changes apply only to the current session.

Statistics > Message: Select this option to display the Message statistics. For information about the Message statistics, see [“Message Statistics” on page 819](#).

Statistics > SMTP Service: Select this option to display the SMTP Service statistics. For information about the SMTP Service statistics, see [“SMTP Service Statistics” on page 820](#).

Statistics > POP Service: Select this option to display the POP Service statistics. For information about the POP Service statistics, see [“POP Service Statistics” on page 822](#).

Statistics > IMAP Service: Select this option to display the IMAP Service statistics. For information about the IMAP Service statistics, see [“IMAP Service Statistics” on page 823](#).

Statistics > LDAP Service: Select this option to display the LDAP Service statistics. For information about the LDAP Service statistics, see [“LDAP Service Statistics” on page 825](#).

Statistics > Zero Statistics: Select this option to reset the Message, SMTP, POP, IMAP, and LDAP statistics.

56.2 Using the GWIA Web Console

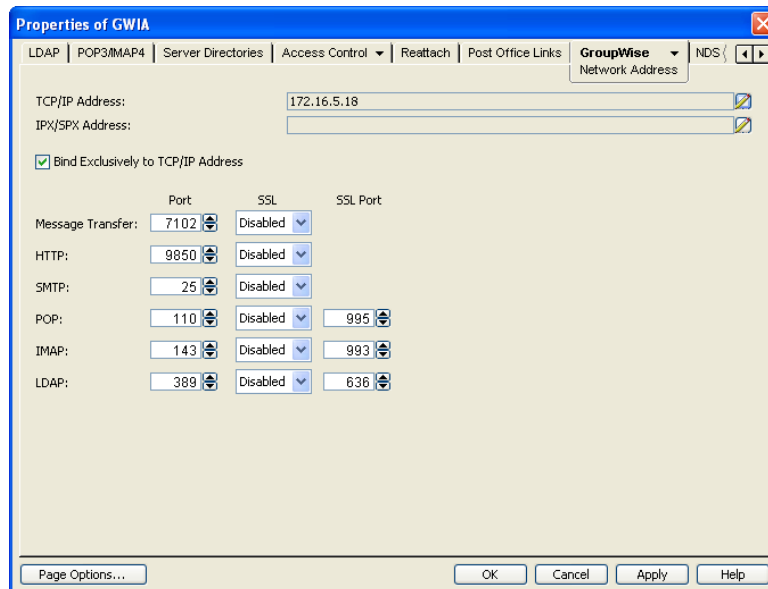
You can use a Web browser interface, referred to as the Web console, to monitor the GWIA. You cannot use the GWIA Web console to change any of the GWIA's settings. Changes must be made through ConsoleOne, the server console, or the startup file.

- ♦ [Section 56.2.1, “Setting Up the GWIA Web Console,” on page 827](#)
- ♦ [Section 56.2.2, “Monitoring the GWIA at the Web Console,” on page 828](#)

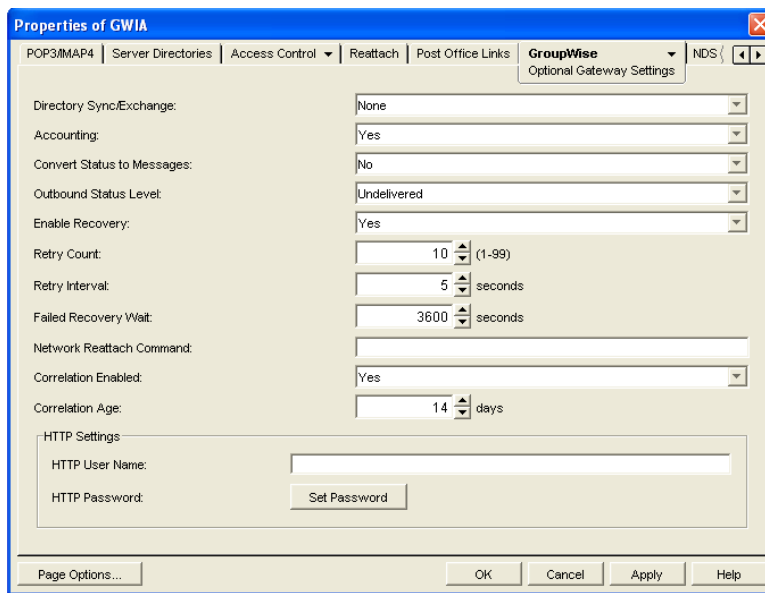
56.2.1 Setting Up the GWIA Web Console

The default HTTP port for the GWIA Web console is established during GWIA installation. You can change the port number and increase security after installation in ConsoleOne.

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.



- 3 Make a note of the TCP/IP address and the HTTP port number. You need this information to access the GWIA Web console.
- 4 If you want to use an SSL connection for the GWIA Web console, which provides optimum security, select *Enabled* in the *HTTP SSL* drop-down list.
For additional instructions about using SSL connections, see [Section 83.2, “Server Certificates and SSL Encryption,” on page 1107](#).
- 5 Click *Apply* to save your changes on the Network Address page.
If you want to limit access to the GWIA Web console, you can provide a user name and password.
- 6 Click *GroupWise > Optional Gateway Settings* to display the Optional Gateway Settings page.



- 7 In the *HTTP User Name* field, enter an arbitrary user name (for example, gwia).
- 8 Click *Set Password* to assign a password (for example, monitor).
- 9 Click *OK* to save your changes.

ConsoleOne then notifies the GWIA to restart to put the new settings into effect.

56.2.2 Monitoring the GWIA at the Web Console

- 1 In a Web browser, enter the following:

`http://IP_address:agent_port` (non-secure server)

or

`https://IP_address:agent_port` (secure server)

Replace *IP_address* with the IP address or hostname of the server where the GWIA is running, and *HTTP_port* is the port number assigned to the agent. If you used the default port during installation, the port number is 9850.

- 2 If prompted, enter the Web console user name and password.

The GWIA Web console is displayed.

GroupWise 2012 GWIA - GWIA.Provo1				
Status Configuration Environment Log Files MTP Status Help				
Restart Internet Agent				
UpTime: 0 Days 5 Hrs 41 Mins				
Thread Status				
	Busy	Idle		
Message Conversion Threads	0	0		
SMTP Threads	0	0		
Standard POP Threads	0	2		
Secure POP Threads	0	0		
Standard IMAP Threads	0	2		
Secure IMAP Threads	0	0		
Queue Information				
	Count	Oldest Message		
Outbound Message Queues	0			
Inbound Message Queues	0			
SMTP Send Queue	0			
SMTP Receive Queue	0			
Delayed Message Queue	0			
Statistics				
Message	Out	10 Minutes	In	10 Minutes
Normal	0	0	0	0
Status	0	0	0	0
Passthrough	0	0	0	0
Conversion Errors	0	0	0	0
Communication Errors	0	0	0	0
Total Bytes	0.0		0.0	

The Web console has five pages (Status, Configuration, Environment, and Log Files, and MTP Status). You can click *Help* on any page for information about the page.

56.3 Using Novell Remote Manager

If the GWIA is running on Novell Open Enterprise Server (OES), you can use Novell Remote Manager to monitor the GWIA. For more information, see the *Novell Remote Manager for Linux Administration Guide* for [your version of OES Linux \(http://www.novell.com/documentation/oes.html\)](http://www.novell.com/documentation/oes.html).

56.4 Using an SNMP Management Console

You can monitor the GWIA from SNMP management and monitoring programs. When properly configured, the GWIA sends SNMP traps to network management consoles for display along with other SNMP monitored programs.

Although the GWIA is SNMP-enabled by default, the server where the GWIA is installed must be properly configured to support SNMP, and the GWIA object in eDirectory must also be properly configured. To set up SNMP services for your server, complete the following tasks:

- ◆ [Section 56.4.1, “Setting Up SNMP Services for the GWIA,” on page 829](#)
- ◆ [Section 56.4.2, “Copying and Compiling the GWIA MIB File,” on page 831](#)
- ◆ [Section 56.4.3, “Configuring the GWIA for SNMP Monitoring,” on page 832](#)

56.4.1 Setting Up SNMP Services for the GWIA

Select the instructions for the platform where the GWIA runs:

- ◆ [“Linux: Setting Up SNMP Services for the GWIA” on page 830](#)
- ◆ [“Windows: Setting Up SNMP Services for the GWIA” on page 830](#)

Linux: Setting Up SNMP Services for the GWIA

The Linux GWIA is compatible with NET-SNMP. An older version of SNMP called UCD-SNMP cannot be used with the Linux GWIA. NET-SNMP comes with OES Linux, but it does not come with SLES. If you are using SLES, you must update to NET-SNMP in order to use SNMP to monitor the Linux GWIA.

- 1 Make sure you are logged in as `root`.
- 2 (Conditional) If NET-SNMP is not already set up on your Linux server, use the following command to configure SNMP:

```
snmpconf -g basic_setup
```

The `snmpconf` command creates the `snmpd.conf` file in one of the following directories, depending on your version of Linux:

```
/usr/share/snmp  
/usr/local/share/snmp  
~/.snmp
```

- 3 Locate the `snmpd.conf` file on your Linux server.
- 4 In a text editor, open the `snmpd.conf` file and add the following line:

```
dlmod Gwsnmp /opt/novell/groupwise/agents/lib/libgwsnmp.so
```
- 5 Save the `snmpd.conf` file and exit the text editor.
- 6 Restart the SNMP daemon (`snmpd`) to put the changes into effect.

IMPORTANT: Make sure that the SNMP daemon always starts before the GWIA starts.

- 7 Skip to [Section 37.6.2, “Copying and Compiling the POA MIB File,”](#) on page 555.

Windows: Setting Up SNMP Services for the GWIA

On Windows Server 2008, the SNMP Service is usually not included during the initial operating system installation. The SNMP Service can be easily added at any time. To add or configure the SNMP Service, you must be logged in as a member of the Administrator group.

To set up SNMP services for the Windows GWIA, complete the following tasks:

- ♦ [“Installing SNMP Support on Windows Server 2008”](#) on page 830
- ♦ [“Installing SNMP Support on Windows Server 2003”](#) on page 831
- ♦ [“Installing GroupWise Agent SNMP Support”](#) on page 831

Installing SNMP Support on Windows Server 2008

- 1 On the Control Panel, click *Programs and Features*.
- 2 Click *Turn Windows features on or off* to open the Server Manager.
- 3 Click *Features > Add Features*.
- 4 In the *Features* list, expand *SNMP Services*, then select *SNMP Service*.
- 5 Click *Next*, then click *Install*.
- 6 When the installation is finished, click *Close*, then exit the Server Manager.
- 7 Skip to [Installing GroupWise Agent SNMP Support](#).

Installing SNMP Support on Windows Server 2003

- 1 Click *Start > Control Panel > Add or Remove Programs*.
- 2 Click *Add/Remove Windows Components*.
- 3 Select *Management and Monitoring Tools*.
- 4 Click *Details*, then select *Simple Network Management Protocol*.
- 5 Follow the on-screen instructions to install the SNMP Service.
- 6 Continue with [Installing GroupWise Agent SNMP Support](#).

Installing GroupWise Agent SNMP Support

The GroupWise Agent Installation program includes an option for installing SNMP support. However, if the server where you installed the agents did not yet have SNMP set up, that installation option was not available. Now that you have set up SNMP, you can install GroupWise agent SNMP support.

At the Windows server where you want to install the GroupWise agent SNMP support:

- 1 Run `setup.exe` at the root of the downloaded *GroupWise 2012* software image.
- 2 Click *Install GroupWise System*, click *Yes* to accept the License Agreement, then click *Next* to perform a standard installation.
- 3 Select *Install individual components*, deselect *GroupWise Administration*, deselect *GroupWise Agents*, select *GroupWise Internet Agent*, then click *Next*.
- 4 On the Installation Path page, browse to and select the path where the Internet Agent software is installed, then select *Install and configure SNMP for Internet Agent*.
- 5 Continue through the rest of the installation process as prompted by the Agent Installation program.
The Agent Installation program copies the SNMP support files to the agent installation directory, makes the appropriate Windows registry entries, and restarts the Windows SNMP service.
- 6 Continue with [Copying and Compiling the POA MIB File](#).

56.4.2 Copying and Compiling the GWIA MIB File

An SNMP-enabled GWIA returns information contained in a Management Information Base (MIB). The MIB is an ASCII data structure that defines the information gathered. It also defines the properties that can be monitored and managed on the SNMP-enabled GWIA.

Before you can monitor an SNMP-enabled GWIA, you must compile the `gwia.mib` file using your SNMP management program. GroupWise agent MIB files are located in the `/agents/snmpmibs` directory of your GroupWise software distribution directory or the downloaded *GroupWise 2012* software image.

The MIB file contains all the Trap, Set, and Get variables used for communication between the GWIA and management console. The Trap variables provide warnings that point to current and potential problems. The Set variables allow you to configure portions of the application while it is still running. The Get variables display the current status of different processes of the application.

- 1 Copy the `gwia.mib` file to the location required by your SNMP management program.
- 2 Compile or import the `gwia.mib` file as required by your SNMP management program.
- 3 Continue with [Configuring the POA for SNMP Monitoring](#).

56.4.3 Configuring the GWIA for SNMP Monitoring

In order for SNMP monitoring programs to monitor the GWIA, the GWIA must be configured with a network address and SNMP community string.

- 1 In ConsoleOne, browse to and right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Network Address* to display the Network Address page.
- 3 Click the pencil icon to provide the TCP/IP address of the server where the POA runs, then click *Apply*.
- 4 Click *GroupWise > Agent Settings*, then scroll to the bottom of the settings list.
- 5 Provide your system SNMP community GET string, then click *OK*.
- 6 Configure the SNMP Service with the same community GET string:
 - 6a On the Windows desktop, click *Start > Administrator Tools > Services*.
 - 6b Right-click *SNMP Service*, then click *Properties*.
 - 6c Click *Security*, then click *Add* in the *Accepted community names* list.
 - 6d In the *Community Name* field, specify your system SNMP community GET string.
 - 6e In the *Community Rights* drop down list, select *READ WRITE*.
 - 6f Click *Add* to add the community string to the list, then click *OK* to close the SNMP Properties
- 7 Restart the GWIA.

The GWIA should now be visible to your SNMP monitoring program.

56.5 Assigning Operators to Receive Warning and Error Messages

You can select GroupWise users to receive warning and error messages issued by the GWIA. Whenever the agent issues a warning or error, these users, called operators, receive a message in their mailboxes. You can specify one or more operators.

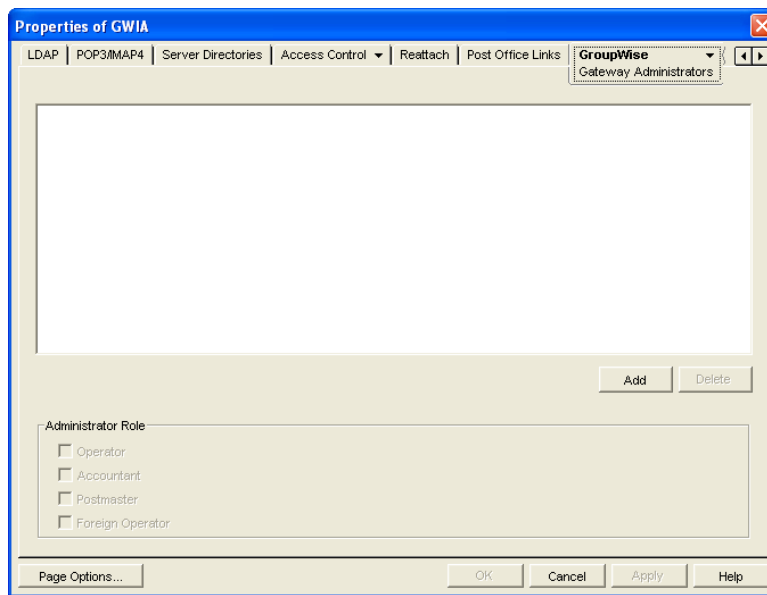
An operator can also shut down the GWIA by sending a mail message addressed as follows:

```
gwia:shutdown
```

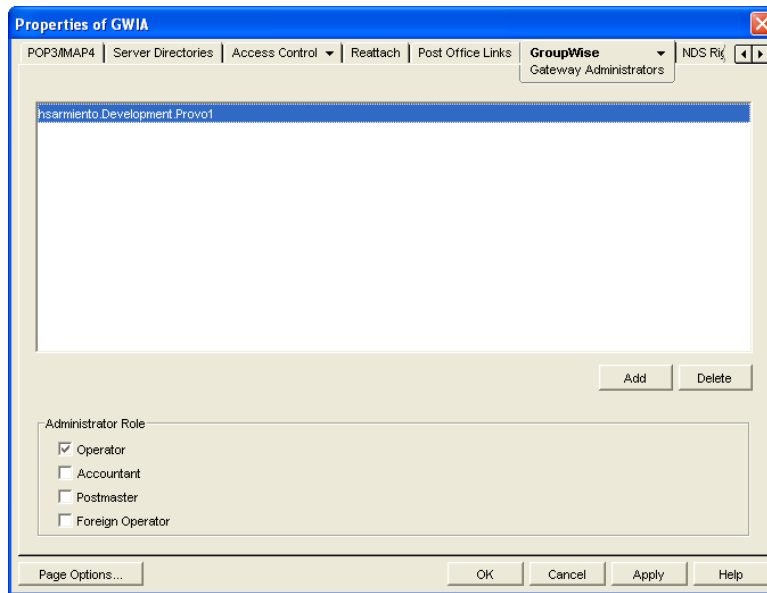
Replace *gwia* with your GWIA's name.

To assign an operator:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Gateway Administrators* to display the Gateway Administrators page.



- 3 Click *Add*, select a user, then click *OK* to add the user to the Gateway Administrators list.



- 4 Make sure *Operator* is selected as the Administrator Role.
- 5 If desired, add additional operators.
- 6 Click *OK*.

56.6 Using GWIA Log Files

You can use the GWIA logging options to help you monitor its operation. By default, the GWIA logs information to its server console, Web console, and to a log file on disk. You can control the following logging features:

- ♦ The type of information to log.

- ◆ Disabling disk logging (Windows GWIA only).
- ◆ How long to retain log files.
- ◆ The maximum amount of disk space to use for log files.
- ◆ Where to store log files.

You can control logging through ConsoleOne, GWIA startup switches, and the GWIA console. The following table shows which logging options you can control from each location.

	ConsoleOne	Startup Switches	Linux Console	Windows Console
Logging Level	Yes	Yes	Yes	Yes
Disk Logging	No	No	Yes	Yes
Maximum Log File Age	Yes	Yes	Yes	Yes
Maximum Disk Space	Yes	Yes	Yes	Yes
Log File Location	Yes	Yes	No	No

The log settings in ConsoleOne are used as the default settings. Startup switches override the ConsoleOne log settings, and console settings override startup switches.

- ◆ [Section 56.6.1, “Locating GWIA Log Files,” on page 834](#)
- ◆ [Section 56.6.2, “Modifying Log Settings in ConsoleOne,” on page 834](#)
- ◆ [Section 56.6.3, “Modifying Log Settings through Startup Switches,” on page 836](#)
- ◆ [Section 56.6.4, “Modifying Log Settings through the GWIA Server Console,” on page 836](#)
- ◆ [Section 56.6.5, “Viewing Log Files,” on page 837](#)

56.6.1 Locating GWIA Log Files

The default location of the GWIA log files varies by platform:

Windows: `domain\wpgate\gwia\000.prc`

Linux: `/var/log/novell/groupwise/domain_name.gwia`

You can change the location where the GWIA creates its log files in ConsoleOne, the GWIA configuration file (`gwia.cfg`), and the GWIA server console.

56.6.2 Modifying Log Settings in ConsoleOne

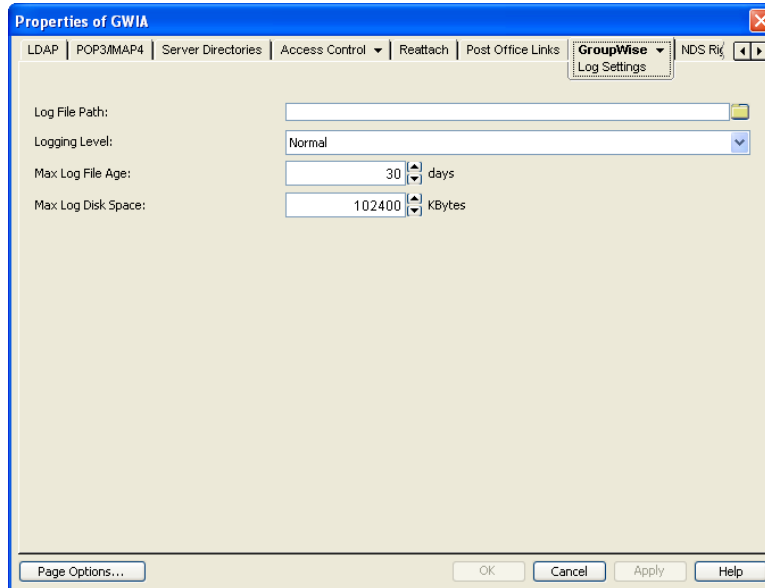
Through ConsoleOne, you can configure the following log settings:

- ◆ Log file location
- ◆ Logging level (applies to both console logging and disk logging)
- ◆ Maximum age for log files
- ◆ Maximum disk space used for log files

The ConsoleOne settings are the default settings. The GWIA uses these settings unless you override them with startup switches in the `gwia.cfg` startup file or at the server console.

To configure the default log settings in ConsoleOne:

- 1 Right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Log Settings* to display the Log Settings page.



- 3 Modify any of the following properties:

Log File Path: The GWIA creates a new log file each day and each time it is started. The log file is named *mmddgwia.nnn*, where *mm* is the month, *dd* is the day, and *nnn* is a sequenced number (001 for the first log file of the day, 002 for the second, and so on). The default location of the log files depends on the platform where the GWIA is running.

Windows: `domain\wpgate\gwia\000.prc`

Linux: `/var/log/novell/groupwise/domain_name.gwia`

If you want to specify a different location, enter the directory path or browse to and select the directory.

Logging Level: There are four logging levels:

- ◆ **Off:** Disables the logging function.
- ◆ **Normal:** Displays warnings and error messages. This is the preferred logging level.
- ◆ **Verbose:** Displays information about traffic, including non-delivery reports, in addition to warnings and error messages. Information includes the file name, path, message ID, and size of the message being processed; the IP address of any inbound SMTP connections; the GWIA-specific MSG number; and SMTP connection messages such as “Connect to novell.com” and “Accepted connection from 172.16.5.18 novell.com”.
- ◆ **Diagnostic:** Displays detailed function calls made by the GWIA. This level is not useful for most troubleshooting. Verbose is better for standard troubleshooting.

The Verbose and Diagnostic logging levels do not degrade GWIA performance, but log files saved to disk consume more disk space when Verbose or Diagnostic logging is in use.

Max Log File Age: Specify the number of days you want the GWIA to retain old log files. The GWIA retains the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 30 days.

Max Log Disk Space: Specify the maximum amount of disk space you want to use for log files. If the disk space limit is exceeded, the GWIA deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 102400 KB (100 MB).

- 4 Click *OK* to save the log settings.

56.6.3 Modifying Log Settings through Startup Switches

You can use startup switches to override any log settings you configured in ConsoleOne, as described in [Section 56.6.2, “Modifying Log Settings in ConsoleOne,” on page 834](#). Edit the `gwia.cfg` file to change switch settings, as described in [Section 59.1.2, “Modifying the gwia.cfg File,” on page 852](#).

For information about the startup switches that can be used to modify log settings, see [Section 59.12, “Log File Switches,” on page 890](#).

56.6.4 Modifying Log Settings through the GWIA Server Console

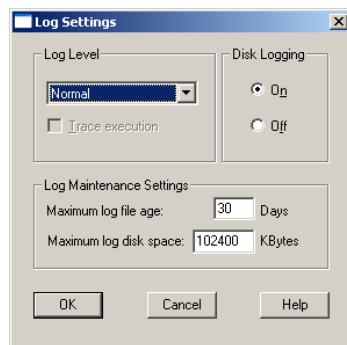
You can use the Windows GWIA console to override the following log settings for the current sessions:

- ♦ Disk logging on/off
- ♦ Log file location
- ♦ Logging level (applies to both console logging and disk logging)
- ♦ Maximum age for log files
- ♦ Maximum disk space used for log files

Changes you make to the log settings at the console apply only to the current session. When you restart the GWIA, the log level is reset to the level specified in ConsoleOne or the startup switches. See [Section 56.6.2, “Modifying Log Settings in ConsoleOne,” on page 834](#) and [Section 56.6.3, “Modifying Log Settings through Startup Switches,” on page 836](#).

To modify the log settings:

- 1 In the Windows GWIA console, click *Log > Log Settings* to display the Log Settings dialog box.



- 2 Change the desired settings:

Log Level: Select *Normal* to display warnings and error messages; this is the preferred logging level. Select *Verbose* to display information about traffic, including non-delivery reports, in addition to warnings and error messages. Information includes the file name, path, message ID, and size of the message being processed; the IP address of any inbound SMTP connections; the

GWIA-specific MSG number; and SMTP connection messages such as “Connect to novell.com” and “Accepted connection from 172.16.5.18 novell.com”. Select *Diagnostic* to display a detailed trace of gateway messages, errors, and operations that can be useful for troubleshooting.

Disk Logging: Select *On* or *Off* to enable or disable logging of information to log files.

Maximum Log File Age: Specify the number of days you want the GWIA to retain old log files. The GWIA retains the log file for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 30 days.

Maximum Log Disk Space: Specify the maximum amount of disk space you want to use for log files. If the disk space limit is exceeded, the GWIA deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 102400 KB (100 MB).

56.6.5 Viewing Log Files

You can view the log file for the current session, or you can view archived log files. The current log file is viewable through the GWIA console, as described in [Section 56.1, “Using the GWIA Server Console,” on page 817](#), or in the GWIA Web console, as described in [Section 56.2, “Using the GWIA Web Console,” on page 827](#). Archived files are viewable through the consoles or an ASCII text editor.

Current Log File

The current log file is displayed in the Logging window of the GWIA console, with only the most current operations visible. The log file is complete, and includes the gateway startup and configuration information and ongoing operations logged by time, including the shutdown operation. You can browse the file from top to bottom or perform a search for any text string you want. You can also view the current log file from the GWIA Web console.

Archived Log Files

The GWIA creates a new log file every day at midnight or every time it restarts. Older log files are not deleted for at least one day unless you have not allowed sufficient disk space for them to be archived.

Log files are named according to the date they were created. If the GWIA was restarted during the day, the file extension indicates which session is logged (for example 05181log.003 indicates the third session logged for May 18).

Archived log files are saved in ASCII. You can use any text editor to open a file or to print it. You can also view the log files from the GWIA console or the GWIA Web console.

56.7 Using GWIA Error Message Documentation

GWIA error messages are documented with the source and explanation of the error, possible causes of the error, and actions to take to resolve the error. See [“Internet Agent Error Messages”](#) in [GroupWise 2012 Troubleshooting 1: Error Messages](#).

56.8 Employing GWIA Troubleshooting Techniques

If you are having a problem with the GWIA but not receiving a specific error message, or if the suggested actions for the specific error did not resolve the problem, you can review more general troubleshooting strategies for dealing with GWIA problems. See [“Strategies for Agent Problems”](#) in [GroupWise 2012 Troubleshooting 2: Solutions to Common Problems](#).

56.9 Stopping the GWIA

The following sections describe the various methods you can use to shut down the GWIA:

- ♦ [Section 56.9.1, “Using the GWIA Server Console,” on page 838](#)
- ♦ [Section 56.9.2, “Using a Command at the Command Line,” on page 838](#)
- ♦ [Section 56.9.3, “Using a Mail Message,” on page 838](#)
- ♦ [Section 56.9.4, “Using a Shutdown File,” on page 838](#)

56.9.1 Using the GWIA Server Console

To stop the GWIA while at the server console, click *File > Exit*.

56.9.2 Using a Command at the Command Line

To stop the GWIA at the command line:

Linux: See [“Stopping the Linux GroupWise Agents”](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.

Windows: N/A

56.9.3 Using a Mail Message

The GWIA can be stopped by sending a shutdown message to the GWIA. In order to shut down the program with a message, the user sending the message must be defined as an operator for the GWIA. This prevents unauthorized users from shutting down the GWIA. For information about defining a user as an operator, see [Section 56.5, “Assigning Operators to Receive Warning and Error Messages,” on page 832](#).

The message to shut down the GWIA must be addressed to the GWIA, not a non-GroupWise domain. The syntax for the To line is:

```
gwia:shutdown
```

Replace *gwia* with the name of the GWIA object.

56.9.4 Using a Shutdown File

The GWIA can also be stopped by placing a file named `shutdown` in the `domain\wpgate\gwia\000.prc` directory. When the GWIA sees this file, it deletes the file and shuts down.

57 Optimizing the GWIA

The following sections provide information about some of the methods you can use to optimize the speed and reliability of the GroupWise GWIA:

- ♦ [Section 57.1, “Relocating the GWIA’s Processing Directories,”](#) on page 839
- ♦ [Section 57.2, “Increasing GWIA Speed,”](#) on page 840

57.1 Relocating the GWIA’s Processing Directories

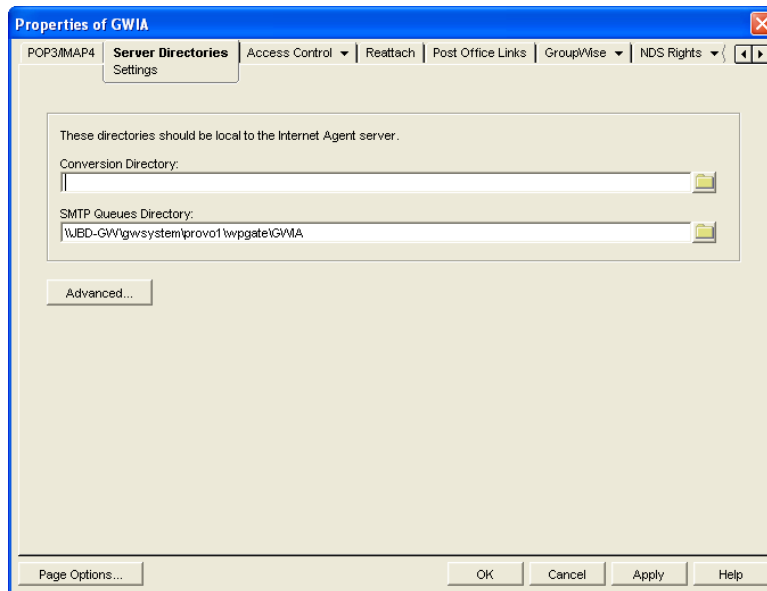
The GWIA uses several directories to process message files. For best performance, these directories should be located on the same server where the GWIA is running.

Linux: If you installed the GWIA on a different server from where the domain is located, you should move the GWIA’s processing directories to the server where the GWIA is running.

Windows: The GWIA Installation program creates the GWIA’s processing directories on the Windows server when it installs the Windows GWIA, so you typically don’t need to move them.

To define the location of the GWIA’s directories:

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *Server Directories > Settings* to display the server directories Settings page.



- 3 Fill in the fields:

Conversion Directory: Select the directory where the GWIA stores temporary files for message conversion. These files are automatically deleted after they are processed. The default conversion directory is under the GWIA queue directory:

`domain/wpgate/gwia/000.prc/gwork`

If you type a path to a Windows drive (rather than using the *Browse* button to select the directory), you must use UNC path syntax.

This setting corresponds with the GWIA's `--work` switch.

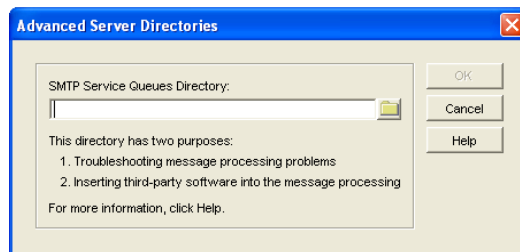
SMTP Queues Directory: Select the directory where the GWIA stores messages being routed to and from the Internet. The default directory is under the domain directory structure.

`domain\wpgate\gwia`

Four subdirectories are created under the SMTP queues directory: `defer`, `send`, `receive`, and `result`.

This setting corresponds with the GWIA's `--dhome` switch.

- 4 Click the *Advanced* button.



- 5 Fill in the field:

SMTP Service Queues Directory: If you want, specify a secondary SMTP queues directory for outbound messages. This secondary directory can be helpful for troubleshooting by providing a way to trap messages before they are routed to the Internet. You can also use the secondary directory to run third-party utilities such as a virus scanner on Internet-bound messages.

The GWIA places all outbound messages in this secondary directory. The messages must then be moved manually (or by another application) to the primary SMTP queues' `send` directory (see [Step 3](#)) before the GWIA routes them to the Internet.

This setting corresponds with the `--smtphome` switch.

If you type a directory path rather than using the *Browse* button to select a directory, make sure you use UNC path syntax.

- 6 Click *OK* to close the dialog box.
- 7 Click *OK* to save the changes to the directory locations.

57.2 Increasing GWIA Speed

You can implement the following procedures to help enhance the GWIA's processing speed:

- ♦ [Section 57.2.1, "Sending and Receiving Threads,"](#) on page 841
- ♦ [Section 57.2.2, "Increasing Polling Time,"](#) on page 841
- ♦ [Section 57.2.3, "Decreasing the Timeout Cycles,"](#) on page 842

57.2.1 Sending and Receiving Threads

The GWIA uses sending and receiving threads to process incoming and outgoing messages. The more threads you make available, the more messages the GWIA can process concurrently. However, threads place a demand on the server's resources. Too many threads can monopolize memory and CPU utilization.

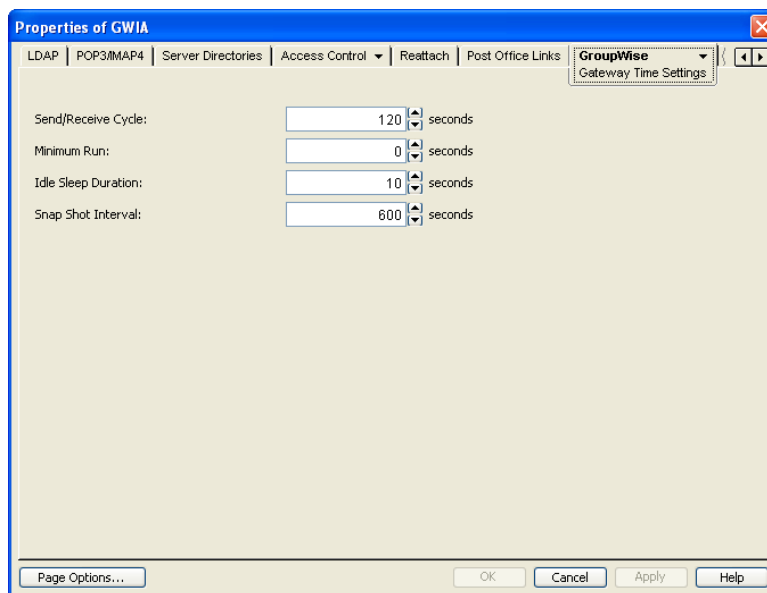
Make sure you balance your processing speed requirements with the other applications running on the same server as the GWIA.

For information about adjusting the SMTP sending and receiving threads, see [Section 53.1.1, "Configuring Basic SMTP/MIME Settings,"](#) on page 757.

57.2.2 Increasing Polling Time

Incoming and outgoing messages are stored in priority queues. The GWIA polls these queues and then forwards the messages for distribution. The *Time* option lets you control how often the GWIA polls these queuing directories. Make sure you balance polling time requirements with the other applications running on the same server as the GWIA.

- 1 In ConsoleOne, right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Gateway Time Settings* to display the Gateway Time Settings page.



- 3 Modify the following settings:

Idle Sleep Duration: Select the time, in seconds, you want the GWIA to idle after it has processed its queues. A low setting, such as 5 seconds, speeds up processing but requires more resources. A higher setting slows down the GWIA but requires fewer resources by reducing the number of network polling scans. The default is 10 seconds.

Snap Shot Interval: The *Snap Shot Interval* is a sliding interval you can use to monitor GWIA activity. For example, if the *Snap Shot Interval* remains at the default (10 minutes), the *Snap Shot* columns in the console display only the previous 10 minutes of activity.

- 4 Click *OK* to save the changes.

57.2.3 Decreasing the Timeout Cycles

The GWIA has a series of switches that control its timeout settings. By decreasing the default time of the timeout cycles you might be able to slightly increase the GWIA speed. However, the timeout cycles do not place an extremely significant burden on the overall performance of the GWIA so the effect might be minimal. You should consider this option only after you have tried everything else.

For information about configuring the timeout settings in ConsoleOne, see [Section 53.1.5, "Configuring the SMTP Timeout Settings,"](#) on page 765. For information about configuring the settings using startup switches, see [Section 59.6.9, "Timeouts,"](#) on page 875.

58 Connecting GroupWise Systems and Domains Using the GWIA

The GWIA can be used as a link between GroupWise systems and between domains in the same GroupWise system.

- ♦ [Section 58.1, “Connecting GroupWise Systems,” on page 843](#)
- ♦ [Section 58.2, “Linking Domains,” on page 848](#)

58.1 Connecting GroupWise Systems

If you have two independent GroupWise systems, you can use the GWIA to connect the two systems. This requires each GroupWise system to have the GWIA installed.

After the systems are connected, you can synchronize information between the two systems so that users from both systems appear in the GroupWise Address Book.

The following sections provide instructions:

- ♦ [Section 58.1.1, “Overview,” on page 843](#)
- ♦ [Section 58.1.2, “Creating an External Domain,” on page 844](#)
- ♦ [Section 58.1.3, “Linking to the External Domain,” on page 845](#)
- ♦ [Section 58.1.4, “Checking the Link Status of the External Domain,” on page 847](#)
- ♦ [Section 58.1.5, “Sending Messages Between Systems,” on page 848](#)
- ♦ [Section 58.1.6, “Exchanging Information Between Systems,” on page 848](#)

58.1.1 Overview

For the purpose of the following discussion, GWSys1 and GWSys2 represent two separate GroupWise systems.

When you connect the two systems, you connect the two domains where the GWIAs are located. To do so:

- ♦ In GWSys1, define the GWSys2 GWIA domain as an external domain. Configure a domain link from the GWSys1 GWIA domain to the external domain, defining the link type as a gateway link that uses the GWIA. This allows GWSys1 to deliver messages to GWSys2.
- ♦ In GWSys2, define the GWSys1 GWIA domain as an external domain. Configure a domain link from the GWSys2 GWIA domain to the external domain, defining the link type as a gateway link that uses the GWIA. This allows GWSys2 to deliver messages to GWSys1.

After you have connected the two systems, users can send messages between the two systems by entering the recipients' full addresses (*userID.post_office.domain* or *user@host*).

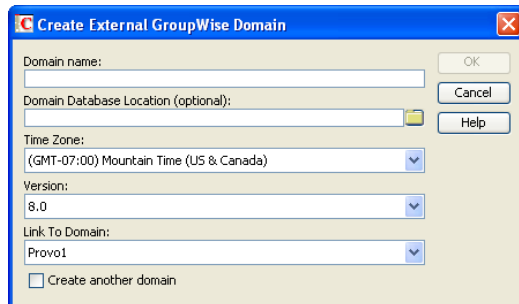
If desired, you can simplify addressing by exchanging information between systems, which causes user information to be displayed in the Address Book. The easiest way to exchange information is to enable the External System Synchronization feature in both systems. When enabled, this synchronization constantly updates the Address Books in both systems so that local users can more easily address messages to and access information about the users in the external system. If you don't want to enable the External System Synchronization feature, you can manually exchange information.

58.1.2 Creating an External Domain

The first step in connecting two GroupWise systems by way of GWIAs is to create an external domain in each GroupWise system. The external domain represents the GWIA domain in the other GroupWise system and provides the medium through which you define the link to the other system.

To create an external domain:

- 1 In ConsoleOne, right-click *GroupWise System*, then click *New > External Domain* to display the Create External GroupWise Domain dialog box.



- 2 Fill in the following fields:

Domain Name: Specify the name of the GWIA domain as it is defined in the external GroupWise system.

Domain Database Location (Optional): Leave this field empty.

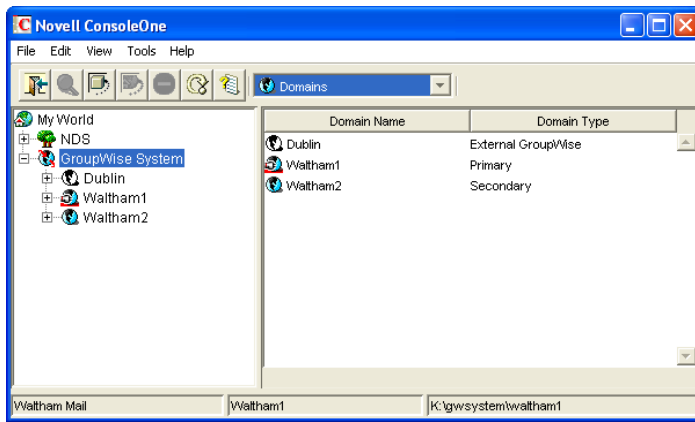
Time Zone: Select the time zone where the domain is physically located.

Version: Select the external domain's GroupWise version. The domain's version is determined by its MTA version. The options are 4.x, 5.x, 6, 6.5, 7, and 8.

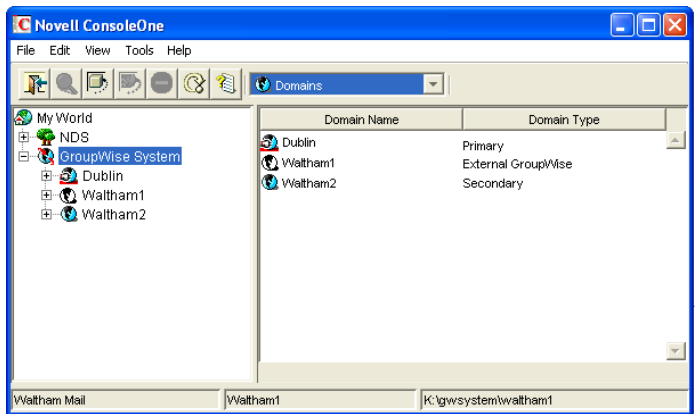
Link to Domain: Select the domain in your system that you want to link to the external domain. This must be your system's GWIA domain. By default, all messages sent to the external GroupWise system are routed to this domain. The domain's MTA then routes the messages to the GWIA, which connects to the GWIA in the other system.

- 3 Click *OK* to create the external domain.

The external domain is added to your GroupWise system and is visible in the GroupWise View. In the following example, Dublin is the external domain.



- Repeat [Step 1](#) through [Step 3](#) to define an external domain in the second GroupWise system. If you do not have administrative rights to that system, you must coordinate with that GroupWise system's administrator.



- Continue with [Linking to the External Domain](#).

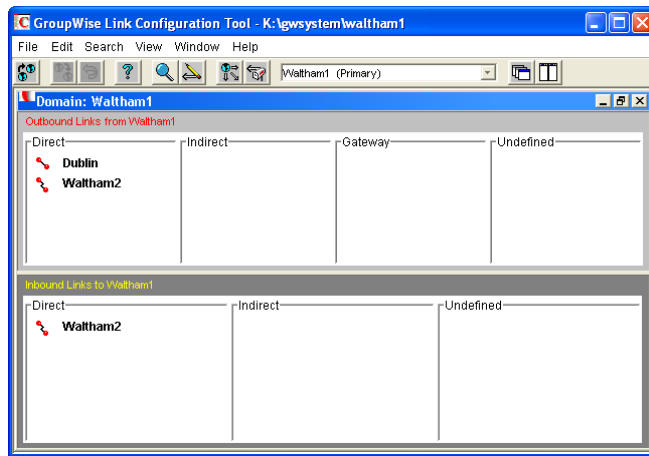
58.1.3 Linking to the External Domain

After you define a domain from the other GroupWise system as an external domain in your system, you need to make sure that your system's domains have the appropriate links to the external domain.

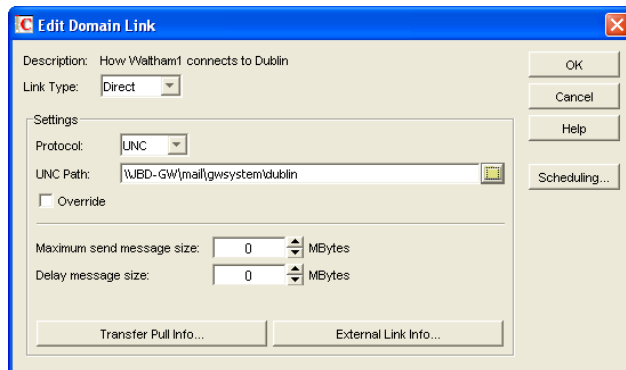
The GWIA domain in your system needs to have a gateway link to the external domain. All other domains in your system have indirect links (through the GWIA domain) to the external domain. These links are configured automatically when the external domain was created.

To configure the gateway link for your GWIA domain:

- In ConsoleOne, right-click the GWIA domain, then click *GroupWise Utilities > Link Configuration* to display the Link Configuration utility.



- In the *Outbound Links* list, double-click the external domain to display the Edit Domain Link dialog box.



- Modify the following fields:

Link Type: Select *Gateway*.

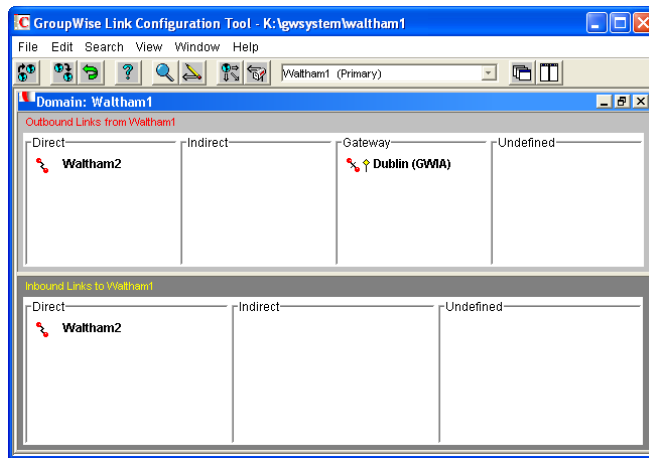
Gateway Link: Select the name of your GWIA.

Gateway Access String: Specify the hostname (GWIA object > *SMTP/MIME* > *Settings*) or foreign ID (GWIA object > *GroupWise* > *Identification*) assigned to the external domain's GWIA (for example, *gwia.ctp.com*).

Return Link: Leave this set to your GWIA domain.



- Click *OK* to save your changes.

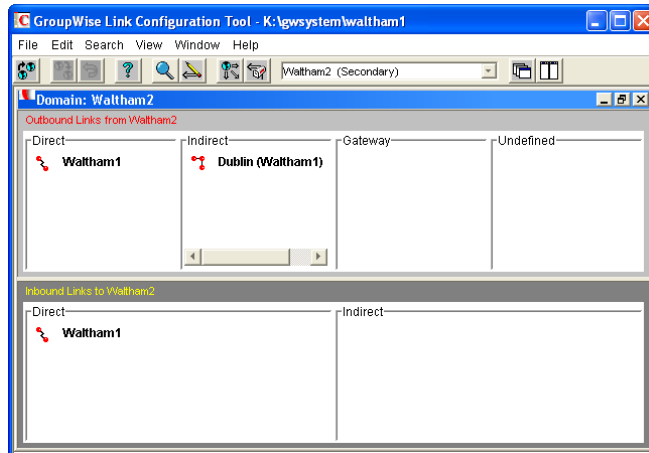
The external domain is displayed in the *Gateway* column of the *Outbound Links* list to show that the current domain is using a gateway link to the external domain. The ⚡ symbol indicates a gateway link. The ⚡ symbol indicates that the link configuration is not yet saved. To save the configuration information, click *Edit* > *Save*.



By default, the rest of the domains in your system should have an indirect link to the external domain. To verify this for a domain:

- 5 In the list of domains on the Link Configuration utility's toolbar, select the domain whose link you want to check, then verify that the external domain is displayed in the Indirect column of the *Outbound Links* list.

The  symbol indicates an indirect link. If the  symbol is displayed, the link modification has not yet been propagated to the domain.



- 6 After verifying your domain links, repeat [Step 1](#) through [Step 5](#) in the second GroupWise system to establish the links to the first GroupWise system. If you do not have administrative rights to that system, you must coordinate with that GroupWise system's administrator.
- 7 Continue with [Checking the Link Status of the External Domain](#).

58.1.4 Checking the Link Status of the External Domain

The GroupWise MTA has monitoring capabilities that let you determine whether the domains in your system are properly linked to the external domain. When you look at the MTA's operation screen, you should see the external domain added to the domain count in the Status box.

If the link to the external domain is closed, the MTA should be logging and displaying the reasons under its Configuration Status function.

For more information about link protocols, see [Chapter 10, “Managing the Links between Domains and Post Offices,”](#) on page 155.

58.1.5 Sending Messages Between Systems

After you have established links between the GWIA domains in the two GroupWise systems, users in one system can send message to recipients in the other system by including the recipients’ fully-qualified GroupWise addresses:

```
userID.post_office.domain or user@host
```

To simplify addressing for your GroupWise users, you can exchange information between the two systems. This enables users in your GroupWise system to use the Address Book when selecting recipients from the other system. For information, see the next section, [Exchanging Information Between Systems](#).

58.1.6 Exchanging Information Between Systems

Exchanging information between two GroupWise systems enables users in either system to use the Address Book when addressing messages to users in the other system. To exchange information, you can choose from the following methods:

External System Synchronization: You can use the External System Synchronization feature to automatically exchange domain, post office, user, resource, and distribution list information between the two systems. After the initial exchange of information, any information that changes in one system is automatically propagated to the other system in order to synchronize the information in that system. This is the recommended method for exchanging information between two systems. For information about setting up synchronization between two external systems, see [Section 4.8, “External System Synchronization,”](#) on page 84.

Manual Creation of Information: You can manually create the other systems’ objects (domains, post offices, users, resources, and distribution lists) as external objects in your GroupWise system. When doing so, the names of your external objects need to exactly match the names of the objects as defined in their system. Domains in your system link to the external domains indirectly through the first external domain you created (this is the external domain that one of your system’s domains has a direct link to). The advantage to this method is that you can choose which of the other system’s domains, post offices, users, resources, and distribution lists you want included in your system. The disadvantage is that there is a great amount of administrative overhead involved in creating all the objects and, after the objects are created, no automatic synchronization takes place so updates must be made manually.

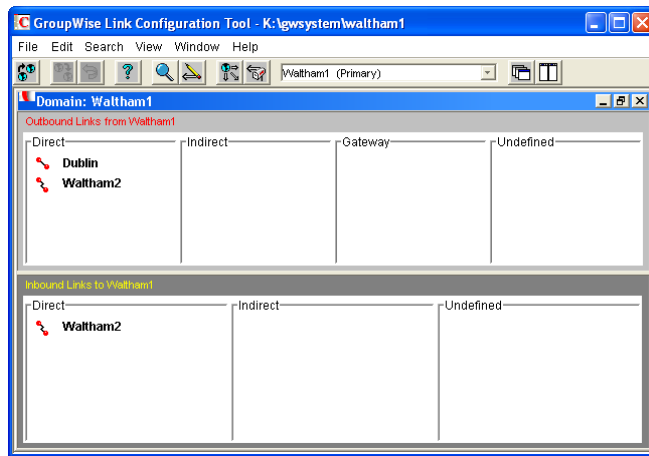
58.2 Linking Domains

If you have domains that cannot be linked by way of a mapped or TCP/IP connection, you can connect them by way of gateway links, with the GWIA defined as the gateway. Both domains being linked must have an GWIA installed.

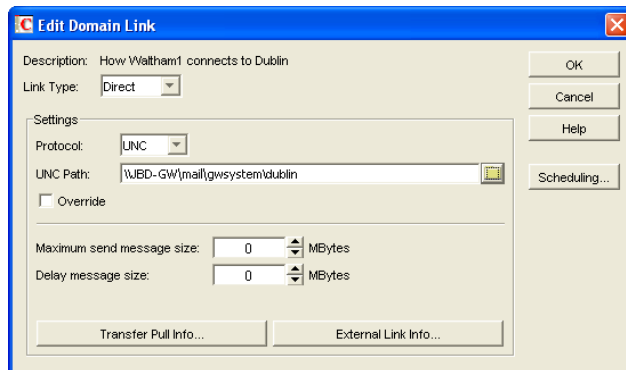
For purposes of reducing confusion in the following steps, the two domains being connected are referred to as Provo and Cambridge. You should substitute your domains appropriately.

To configure gateway links between two domains:

- 1 In ConsoleOne, right-click the Provo domain, then click *GroupWise Utilities > Link Configuration* to display the Link Configuration utility.



- In the *Outbound Links* list, double-click the *Cambridge* domain to display the Edit Domain Link dialog box.



- Modify the following fields:



Link Type: Select *Gateway*.

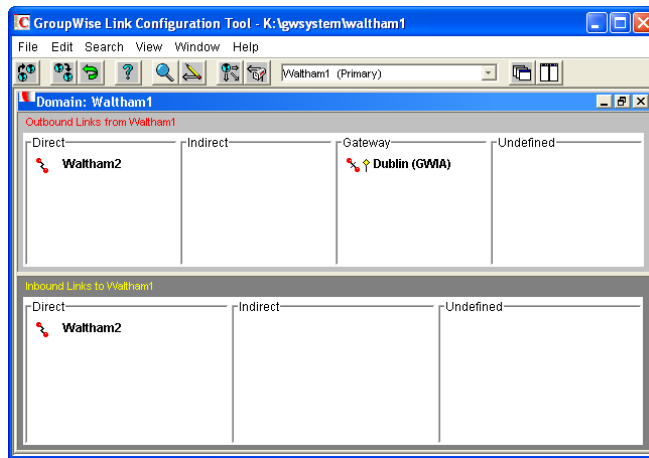
Gateway Link: Select the name of the Provo domain's GWIA.

Gateway Access String: Specify the hostname (GWIA object > *SMTP/MIME* > *Settings*) or foreign ID (GWIA object > *GroupWise* > *Identification*) of the Cambridge domain's GWIA (for example, *gwia.ctp.com*).

Return Link: Leave this set to the Provo domain.



- Click *OK* to save your changes.

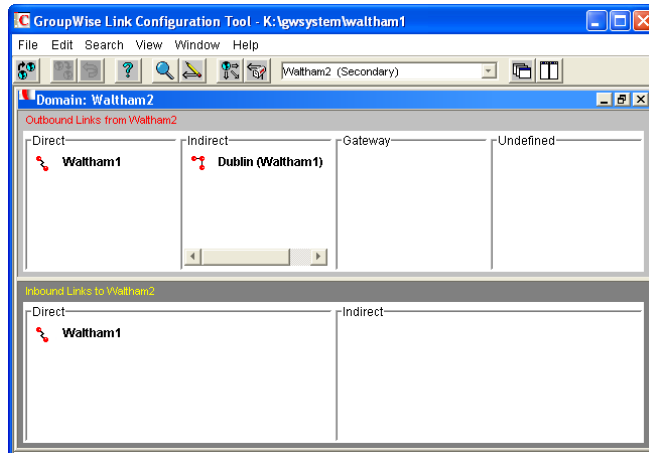
The Cambridge domain is displayed in the *Gateway* column of the *Outbound Links* list to show that the Provo domain is using a gateway link to it. The  symbol indicates a gateway link. The  symbol indicates that the link configuration is not yet saved. To save the configuration information, click *Edit* > *Save*.



By default, any domains that are already linked to your Provo domain should have an indirect link to the Cambridge domain through the Provo domain. To verify this for a domain:

- 5 In the list of domains on the Link Configuration utility's toolbar, select the domain whose link you want to check, then verify that the Cambridge domain is displayed in the Indirect column of the *Outbound Links* list.

The  symbol indicates an indirect link. If the  symbol is displayed, the link modification has not yet been propagated to the domain.



- 6 After verifying your domain links, repeat [Step 1](#) through [Step 5](#) in the second GroupWise system to establish the links to the first GroupWise system. If you do not have administrative rights to that system, you must coordinate with that GroupWise system's administrator.

The GroupWise MTA has monitoring capabilities that let you determine whether the domains in your system are properly linked. When you look at the MTA's operation screen, you should see all domains, regardless of link type, included in the domain count in the Status box.

If the link to a domain is closed, the MTA should be logging and displaying the reasons under its Configuration Status function.

For more information about link protocols, see [Chapter 10, "Managing the Links between Domains and Post Offices,"](#) on page 155.

59 Using GWIA Startup Switches

Choose from the following list to find out how to use GWIA startup switches, and for an explanation of the purpose for each of the switches. The switches are grouped into sections according to the features and functionality that they affect.

- ◆ [Section 59.1, “How to Use Startup Switches,” on page 851](#)
- ◆ [Section 59.2, “Alphabetical List of Switches,” on page 853](#)
- ◆ [Section 59.3, “Required Switches,” on page 858](#)
- ◆ [Section 59.4, “Console Switches,” on page 859](#)
- ◆ [Section 59.5, “Environment Switches,” on page 860](#)
- ◆ [Section 59.6, “SMTP/MIME Switches,” on page 862](#)
- ◆ [Section 59.7, “POP3 Switches,” on page 880](#)
- ◆ [Section 59.8, “IMAP4 Switches,” on page 882](#)
- ◆ [Section 59.9, “HTTP \(Web Console\) Switches,” on page 884](#)
- ◆ [Section 59.10, “SSL Switches,” on page 885](#)
- ◆ [Section 59.11, “LDAP Switches,” on page 887](#)
- ◆ [Section 59.12, “Log File Switches,” on page 890](#)

59.1 How to Use Startup Switches

The default location for the GWIA configuration file (`gwia.cfg`) file varies by platform.

Linux: `/opt/novell/groupwise/agents/share`

Windows: `c:\Program Files\Novell\GroupWise Server\GWIA`

The GWIA reads the `gwia.cfg` file at startup and restart. Only one switch is required in the `gwia.cfg` file. The `--home` switch points to the GWIA's gateway directory. This is always a subdirectory of `wpgate` in the domain directory structure.

NOTE: A boilerplate version of the `gwia.cfg` file is stored in the `domain/wpgate` directory, but the GWIA does not read it. Do not edit the switches in the `gwia.cfg` file in the `domain/wpgate` directory.

When you update the GWIA software, the existing `gwia.cfg` file can be retained or overwritten as needed.

Linux: When you use both the *Install* and *Configure* options in the Internet Agent Installation program, the existing `gwia.cfg` file is backed up and then overwritten. When you use only the *Install* option, the existing `gwia.cfg` file is retained.

Windows: When you select *Install the software files, but do not configure the Internet Agent* in the Internet Agent Installation program, the existing `gwia.cfg` file is retained. When you do not select this option, the existing `gwia.cfg` file is backed up and then overwritten.

You can use the `gwia.cfg` file to override primary configuration settings that are stored in the domain database (`wpdomain.db`) and modified in ConsoleOne. You can also use the `gwia.cfg` file to set secondary configuration settings that are not available in ConsoleOne. [Section 59.2, “Alphabetical List of Switches,” on page 853](#) indicates which settings are available in ConsoleOne and which settings are not. You can view the GWIA startup file from the Configuration page of the GWIA Web console.

- ♦ [Section 59.1.1, “Changing GWIA Settings in ConsoleOne,” on page 852](#)
- ♦ [Section 59.1.2, “Modifying the gwia.cfg File,” on page 852](#)
- ♦ [Section 59.1.3, “Editing Guidelines,” on page 852](#)

59.1.1 Changing GWIA Settings in ConsoleOne

We recommend that you modify configuration settings in ConsoleOne rather than using corresponding switches in the `gwia.cfg` file.

59.1.2 Modifying the gwia.cfg File

If you need to change the GWIA’s configuration and do not have access to ConsoleOne, you can manually edit the `gwia.cfg` file. Any changes you make to the `gwia.cfg` file override the primary settings in ConsoleOne so that the GWIA starts using the new settings. However, the primary settings are not changed in the domain database as a result of editing the `gwia.cfg` file. In order to specify secondary configuration settings that are not available in ConsoleOne, you must edit the `gwia.cfg` file.

The location of the `gwia.cfg` file used by the GWIA depends on the GWIA’s platform:

Linux: The `gwia.cfg` file used by the Linux GWIA is located in the `/opt/novell/groupwise/agents/share` directory.

Windows: The `gwia.cfg` file used by the Windows GWIA is located in the `domain\wpgate\gwia` directory. Do not edit the `gwia.cfg` file located in the same directory as the GWIA program. This `gwia.cfg` file is only used to redirect the GWIA to the `gwia.cfg` file in the `domain\wpgate\gwia` directory.

59.1.3 Editing Guidelines

If you decide to manually edit the `gwia.cfg` file, keep the following guidelines in mind:

- ♦ Archive a copy of the file in case you need to return to the original switch settings.
- ♦ Use a text editor to edit the file.

- ♦ The comment characters include the semicolon (;), pound sign (#), and asterisk (*), and are used to disable a switch or to add comments. The GWIA ignores any line that begins with a comment character.
- ♦ Changes made to the configuration file do not take effect until you restart the GWIA.
- ♦ On Linux, use a space to separate a switch from its value. On Windows, you can use a hyphen (-) or an equals sign (=) to separate a switch from its value. The equals sign is especially useful when the value includes a hyphen.
- ♦ None of the switches or switch values are case sensitive. For example, --sd 12 is the same as --SD 12.
- ♦ If a switch is specified more than once in the configuration file or on the command line, and if it has a value (such as --loglevel normal), only the last instance of the switch is used.
- ♦ The `gwia.cfg` file is used by default. However, you can also specify another configuration file or use startup switches on the command line when starting the GWIA program. If no other configuration file is specified on the command line (using the `gwia @file_name` syntax), the default `gwia.cfg` configuration file is read and processed before, and in addition to, any command line switches.
- ♦ If a configuration file other than `gwia.cfg` is specified on the command line, the default `gwia.cfg` file is not read.

59.2 Alphabetical List of Switches

Primary configuration settings are available in ConsoleOne. Secondary configuration settings are not available in ConsoleOne and can be set only using switches in the `gwia.cfg` file.

Switch starts with: [a](#) [b](#) [c](#) [d](#) [e](#) [f](#) [g](#) [h](#) [i](#) [j](#) [k](#) [l](#) [m](#) [n](#) [o](#) [p](#) [q](#) [r](#) [s](#) [t](#) [u](#) [v](#) [w](#) [x](#) [y](#) [z](#)

Linux GWIA	Windows GWIA	ConsoleOne Settings
--aqf	/aqf	<i>SMTP/MIME > Address Handling > Sender's Address Format</i>
--aqor	/aqor	<i>SMTP/MIME > Address Handling > Place Domain and Post Office Qualifiers on Right of Address</i>
--noaqor	/noaqor	
--ari	/ari	N/A
--attachmsg	/attachmsg	N/A
--noattachmsg	/noattachmsg	
--badmsg	/badmsg	<i>SMTP/MIME > Undeliverables > Undeliverable or Problem Message</i>
--blockrulegenmsg	/blockrulegenmsg	N/A
--certfile	/certfile	<i>GroupWise > SSL Settings > Certificate File</i>
--cluster	/cluster	N/A
--dbchar822	/dbchar822	N/A
--dhome	/dhome	<i>Server Directories > Settings > SMTP Queues Directory</i>
--defaultcharset	/defaultcharset	N/A

Linux GWIA	Windows GWIA	ConsoleOne Settings
--delayedmsgnotification	/delayedmsgnotification	SMTP/MIME > Settings
--nodelayedmsgnotification	/nodelayedmsgnotification	
--dia	/dia	SMTP/MIME > Address Handling > Ignore
--nodia	/nodia	GroupWise Internet Addressing
N/A	/dialpass	SMTP/MIME > Dial-Up Settings > Password
N/A	/dialuser	SMTP/MIME > Dial-Up Settings > Username
-disallowauthrelay	/disallowauthrelay	N/A
--displaylastfirst	/displaylastfirst	SMTP/MIME > Address Handling > Display
--nodisplaylastfirst	/nodisplaylastfirst	Fullname as Lastname, Firstname
--dontreplacedunderscore	/dontreplacedunderscore	SMTP/MIME > Address Handling > Do Not
--replaceunderscore	/replaceunderscore	Replace Underscores with Spaces
--dsn	/dsn	SMTP/MIME > ESMTP Settings > Enable
--nodsn	/nodsn	Delivery Status Notification (DSN)
--dsnage	/dsnage	SMTP/MIME > ESMTP Settings > DSN Hold Age
--etrnhost	/etrnhost	SMTP/MIME > Dial-Up Settings > ETRN Host
--etrnqueue	/etrnqueue	SMTP/MIME > Dial-Up Settings > ETRN Queue
--fd822	/fd822	SMTP/MIME > Address Handling > Non-
		GroupWise Domain for RFC-822 Replies
--fdmime	/fdmime	SMTP/MIME > Address Handling > Non-
		GroupWise Domain for MIME Replies
--flatfwd	/flatfwd	SMTP/MIME > Message Formatting > Enable
--noflatfwd	/noflatfwd	Flat Forwarding
--force7bitout	/force7bitout	SMTP/MIME > Settings > Use 7 Bit Encoding for
--noforce7bitout	/noforce7bitout	All Outbound Messages
--forceinboundauth	/forceinboundauth	N/A
--forceoutboundauth	/forceoutboundauth	N/A
--fut	/fut	SMTP/MIME > Undeliverables > Forward
		Undeliverable Inbound Messages
--group	/group	SMTP/MIME > Address Handling > Expand
--nogroup	/nogroup	Groups on Incoming Messages
--help	/help	N/A
--hn	/hn	SMTP/MIME > Settings > Hostname/DNS
		Record "A Record" Name
--home	/home	N/A
--httppassword	/httppassword	GroupWise > Optional Gateway Settings > HTTP
		Password
--httpport	/httpport	GroupWise > Network Address > HTTP Port
--httprefresh	/httprefresh	N/A

Linux GWIA	Windows GWIA	ConsoleOne Settings
--httpssl	/httpssl	GroupWise > Network Address > HTTP SSL
--httpuser	/httpuser	GroupWise > Optional Gateway Settings > HTTP User Name
--imap4	/imap4	POP3/IMAP4 > Settings > Enable IMAP4 Service
--imapport	/imapport	GroupWise > Network Address > IMAP Port
--imapreadlimit	/imapreadlimit	POP3/IMAP4 > Settings > Maximum Number of Items to Read
--imapreadnew	/imapreadnew	N/A
--imapsport	/imapsport	GroupWise > Network Address > IMAP SSL Port
--imapssl	/imapssl	GroupWise > Network Address > IMAP SSL
--imip--noimip	/imip /noimip	SMTP/MIME > Settings > Enable iCal Service
--ip	/ip	GroupWise > Network Address > Bind Exclusively to TCP/IP Address
--ipa	/ipa	N/A
--ipp	/ipp	N/A
--iso88591is	/iso88591is	N/A
--it	/it	POP3/IMAP4 > Settings > Number of Threads for IMAP4 Connections
--keepsendgroups	/keepsendgroups	SMTP/MIME > Address Handling > Retain Distribution Lists on Outgoing Messages
--nokeepsendgroups	/nokeepsendgroups	
--keyfile	/keyfile	GroupWise > SSL Settings > SSL Key File
--keypasswd	/keypasswd	GroupWise > SSL Settings > Password
--killthreads	/killthreads	SMTP/MIME > Settings > Kill Threads on Exit or Restart
--nokillthreads	/nokillthreads	
--koi8	/koi8	N/A
--ldap	/ldap	LDAP > Settings > Enable LDAP Service
--ldapcntxt	/ldapcntxt	LDAP > Settings > LDAP Context
--ldapipaddr	/ldapipaddr	N/A
--ldapport	/ldapport	GroupWise > Network Address > LDAP Port
--ldappwd	/ldappwd	N/A
--ldaprefcntxt	/ldaprefcntxt	LDAP > Settings > LDAP Context
--ldaprefurl	/ldaprefurl	LDAP > Settings > LDAP Referral URL
--ldapserversport	/ldapserversport	GroupWise > Network Address > LDAP Port
--ldapserverssllport	/ldapserverssllport	GroupWise > Network Address > LDAP SSL Port

Linux GWIA	Windows GWIA	ConsoleOne Settings
--ldapssl	/ldapssl	GroupWise > Network Address > LDAP SSL
--noldapssl	/noldapssl	
--ldapthrd	/ldapthrd	LDAP > Settings > Number of LDAP Threads
--ldapuser	/ldapuser	N/A
--log	/log	GroupWise > Log Settings > Log File Path
--logdays	/logdays	GroupWise > Log Settings > Max Log File Age
--loglevel	/loglevel	GroupWise > Log Settings > Log Level
--logmax	/logmax	GroupWise > Log Settings > Max Log Disk Space
--maxdeferhours	/maxdeferhours	SMTP/MIME > Settings > Maximum Number of Hours to Retry a Deferred Message
--mbcount	/mbcount	SMTP/MIME > Security Settings > Enable Mailbomb Protection and Mailbomb Threshold
--mbtime	/mbtime	SMTP/MIME > Security Settings > Enable Mailbomb Protection and Mailbomb Threshold
--mh	/mh	SMTP/MIME > Settings > Relay Host for Outbound Messages
--mime	/mime	SMTP/MIME > Message Formatting > Default Message Encoding: MIME
--msgdeferinterval	/msgdeferinterval	SMTP/MIME > Settings > Intervals to Retry a Deferred Message
--msstu	/msstu	N/A
--mudas	/mudas	SMTP/MIME > Undeliverables > Amount of Original Message to Return to Sender When Message Is Undeliverable
--nasoq	/nasoq	N/A
--nickgroup	/nickgroup	N/A
--noesmtplib	/noesmtplib	N/A
--noimapversion	/noimapversion	SMTP/MIME > POP3/IMAP4 > Settings > Do Not Publish GroupWise Information on an Initial IMAP4 Connection
--noiso2022	/noiso2022	N/A
--iso2022	/iso2022	
--nomappriority	/nomappriority	SMTP/MIME > Message Formatting > Disable Mapping X-Priority Fields
--mapriority	/mapriority	
--nopopversion	/nopopversion	SMTP/MIME > POP3/IMAP4 > Settings > Do Not Publish GroupWise Information on an Initial POP3 Connection
--nosmtplibversion	/nosmtplibversion	SMTP/MIME > Settings > Do Not Display GroupWise Information on an Initial SMTP Connection
--smtplibversion	/smtplibversion	

Linux GWIA	Windows GWIA	ConsoleOne Settings
--nosnmp	/nosnmp	N/A
--notfamiliar	/notfamiliar	N/A
--familiar	/familiar	
--nqpmt	/nqpmt	SMTP/MIME > Message Formatting > Enable Quoted Printed Message Text Line Wrapping
--p	/p	SMTP/MIME > Settings > Scan Cycle for Send Directory
--pop3	/pop3	POP3/IMAP4 > Settings > Enable POP3 Service
--noper3	/noper3	
--popintruderdetect	/popintruderdetect	POP3/IMAP4 > Settings > Enable Intruder Detection
--popport	/popport	GroupWise > Network Address > POP Port
--popsport	/popsport	GroupWise > Network Address > POP SSL Port
--popssl	/popssl	GroupWise > Network Address > POP SSL
--pt	--pt	POP3/IMAP4 > Settings > Number of Threads for POP3
--rbl	/rbl	Access Control > Blacklists > Blacklist Addresses
--rd	/rd	SMTP/MIME > Settings > Number of SMTP Receive Threads
--realmailfrom	/realmailfrom	SMTP/MIME > Address Handling > Use GroupWise User Address as Mail From: for Rule Generated Messages
--norealmailfrom	/norealmailfrom	
--rejbs	/rejbs	SMTP/MIME > Security Settings > Reject Mail If Sender's Identity Cannot Be Verified
--relayaddsignature	/relayaddsignature	SMTP/MIME > Message Formatting > Apply Global Signature to Relay Messages
--rt	/rt	SMTP/MIME > Message Formatting > Number of Inbound Conversion Threads
--sd	/sd	SMTP/MIME > Settings > Number of SMTP Send Threads
--show	N/A	N/A
--smtp	/smtp	SMTP-MIME > Settings > Enable SMTP
--smtpphone	/smtpphone	Server Directories > Settings > Advanced > SMTP Service Queues Directory
--smtpport	/smtpport	GroupWise > Network Address > SMTP Port
--smtpssl	/smtpssl	GroupWise > Network Address > SMTP SSL
--sslit	/sslit	POP3/IMAP4 > Settings > Number of Threads for IMAP4 SSL Connections

Linux GWIA	Windows GWIA	ConsoleOne Settings
<code>--sslpt</code>	<code>/sslpt</code>	POP3/IMAP4 > Settings > Number of Threads for POP3 SSL Connections
<code>--st</code>	<code>/st</code>	SMTP/MIME > Message Formatting > Number of Outbound Conversion Threads
<code>--tc</code>	<code>/tc</code>	SMTP/MIME > Timeouts > Commands
<code>--td</code>	<code>/td</code>	SMTP/MIME > Timeouts > Data
<code>--te</code>	<code>/te</code>	SMTP/MIME > Timeouts > Connection Establishment
<code>--tg</code>	<code>/tg</code>	SMTP/MIME > Timeouts > Greeting
<code>--tr</code>	<code>/tr</code>	SMTP/MIME > Timeouts > TCP Read
<code>--tt</code>	<code>/tt</code>	SMTP/MIME > Timeouts > Connection Termination
<code>--usedialup</code>	<code>/usedialup</code>	SMTP/MIME > Dial-Up Settings > Enable Dial-Up
<code>--ueea</code>	<code>/ueea</code>	SMTP/MIME > Message Formatting > UUEncode All Message Attachments
<code>--work</code>	<code>/work</code>	Server Directories > Settings > Conversion Directory
<code>--wrap</code>	<code>/wrap</code>	SMTP/MIME > Message Formatting > Line Wrap Length for Message Text on Outbound Mail
<code>--xspam</code>	<code>/xspam</code>	SMTP/MIME > Junk Mail

59.3 Required Switches

The following switches point the GWIA to the GWIA's directory. They are assigned their initial value during installation.

`--dhome`
`--hn`
`--home`

59.3.1 --dhome

Points to the SMTP service work area. This is normally the GWIA's gateway directory under the `domain\wpgate` directory. See [Section 57.1, "Relocating the GWIA's Processing Directories,"](#) on page 839.

Syntax: `--dhome path_name`

Linux Example: `--dhome /gwsystem/provo1/gwia`

Windows Example: `/dhome=c:\gwsystem\provo2\gwia`

59.3.2 --hn

Specifies the hostname that is displayed when someone connects to your GWIA using a Telnet session. You should enter the hostname assigned to you by your Internet service provider.

Syntax: `--hn host_name`

Example: `--hn gwia.novell.com`

This switch is required only under certain circumstances. Normally, the GWIA gets the information from another source and does not need this switch. If you receive a message that the `--hn` switch is required, you must use the switch.

59.3.3 --home

Points the GWIA to the GWIA's gateway directory. This is always a subdirectory of `wpgate` in the domain directory structure.

Syntax: `--home gateway_directory`

Linux Example: `--home /gwsystem/provo1/gwia`

Windows Example: `/home-j:\headq\wpgate\gwia`

If you specify a UNC path with the `--home` switch when you run the GWIA as a Windows service, you must configure the GWIA service to run under a specific Windows user account. If you specify a local directory or a mapped drive, you can configure the GWIA service to run under the local system account.

59.4 Console Switches

The following switches apply to the GWIA console:

`--color`
`--help`
`--mono`
`--show`

59.4.1 --color

Sets the default color of the GWIA console. The values range from 0-7.

Syntax: `color-0|1|2|3|4|5|6|7`

Example: `--color 3`

You can also change the color of the screen for an GWIA session. From the menu on the bottom of the console, select *Options*, then press the key for *Colors*.

59.4.2 --help

Displays the Help screen for the startup switches.

Syntax: `--help`

59.4.3 --mono

Runs the GWIA for a computer with a monochrome monitor.

Syntax: --mono

59.4.4 --show (Linux Only)

Starts the Linux GWIA with an agent console interface similar to that provided for the Windows GWIA. This user interface requires that the X Window System and Open Motif are running on the Linux server.

Syntax: --show

The --show switch cannot be used in the GWIA startup file (`gwia.cfg`). However, if you want the GWIA to start with a user interface when you run the `grpwise` script or when the server reboots, you can configure the GroupWise High Availability service (`gwha`) to accomplish this, as described in “[Configuring the GroupWise High Availability Service in the `gwha.conf` File](#)” in “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*.

59.5 Environment Switches

The following switches configure GWIA environment settings such as working directories, clustering support, and SNMP support.

--cluster
--ip
--ipa
--nosnmp
--smtpname
--work

59.5.1 --cluster

Informs the GWIA that it is running in a cluster. A clustered GWIA automatically binds to the IP address configured for the GWIA object even if the *Bind Exclusively to TCP/IP Address* option is not selected on the GWIA Network Address page in ConsoleOne. This prevents unintended connections to other IP addresses, such as the loopback address or the node’s physical IP address. For information about clustering the GWIA, see the *GroupWise 2012 Interoperability Guide*.

Syntax: --cluster

59.5.2 --ip

Binds the GWIA to the specified IP address so that, on a server with multiple IP addresses, the GWIA uses only the specified IP address.

Syntax: --ip *address*

Example: --ip 172.16.5.18

59.5.3 --ipa

Specifies the IP address (or hostname) of a GroupWise POA that the GWIA can use to resolve IP addresses of other POAs in the system. This replaces the need to configure post office links for the GWIA in ConsoleOne (GWIA object > *Post Office Links* > *Settings*).

If you have established a GroupWise name server (*ngwnameserver*), you can use it. See [Section 36.2.2, “Simplifying Client/Server Access with a GroupWise Name Server,”](#) on page 496.

Syntax: `--ipa address`

Example: `--ipa ngwnameserver`

59.5.4 --ipp

Specifies the port number of a GroupWise POA that the GWIA can use to resolve IP addresses of other POAs in the system. This replaces the need to configure post office links for the GWIA in ConsoleOne (GWIA object > *Post Office Links* > *Settings*).

If you have established a GroupWise name server (*ngwnameserver*), you can use it. See [Section 36.2.2, “Simplifying Client/Server Access with a GroupWise Name Server,”](#) on page 496.

Syntax: `--ipp port_number`

Example: `--ipp 678`

59.5.5 --nosnmp

Disables SNMP for the GWIA. The default is to have SNMP enabled. See [Section 37.6, “Using an SNMP Management Console,”](#) on page 553.

Syntax: `--nosnmp`

59.5.6 --smtphome

Specifies a secondary [SMTP queues directory](#) for inbound and outbound messages. This secondary directory can be helpful for troubleshooting by providing a way to trap messages before they are routed to the Internet. You can also use the secondary directory to run third-party utilities such as a virus scanner on Internet-bound messages. See [Section 57.1, “Relocating the GWIA’s Processing Directories,”](#) on page 839.

The GWIA places all outbound messages in this secondary directory. The messages must then be moved manually (or by another application) to the primary SMTP queue’s send directory (`--dhome` switch) before the GWIA routes them to the Internet.

Syntax: `--smtphome path`

Example: `--smtphome mail:\provo1\wpgate\gwia\smtp2`

59.5.7 --work

Sets the directory where the GWIA stores its temporary files. On Linux, the work directory is located in the domain by default. On Windows, it is not.

Linux: `domain/wpgate/gwia/000.prc/gwork`

Windows: `c:\grpwise\gwia`

Syntax: `--work path_name`

Linux Example: `--work /opt/novell/groupwise/tmp`

Windows Example: `/work -j:\tmp\work`

59.5.8 --nasoq

By default, the GWIA sends the accounting file (`acct`) to users specified as accountants in ConsoleOne (GWIA object > *GroupWise* > *Gateway Administrators*). The file is sent daily at midnight and any time the GWIA shuts down.

This switch instructs the GWIA to send the `acct` file once daily at midnight, not each time the GWIA quits or is shut down.

Syntax: `--nasoq`

59.6 SMTP/MIME Switches

The following sections categorize and describe the switches that you can use to configure the GWIA's SMTP/MIME settings:

- ♦ [Section 59.6.1, "SMTP Enabled," on page 862](#)
- ♦ [Section 59.6.2, "iCal Enabled," on page 863](#)
- ♦ [Section 59.6.3, "Address Handling," on page 863](#)
- ♦ [Section 59.6.4, "Message Formatting and Encoding," on page 868](#)
- ♦ [Section 59.6.5, "Forwarded and Deferred Messages," on page 871](#)
- ♦ [Section 59.6.6, "Extended SMTP," on page 872](#)
- ♦ [Section 59.6.7, "Send/Receive Cycle and Threads," on page 873](#)
- ♦ [Section 59.6.8, "Dial-Up Connections," on page 874](#)
- ♦ [Section 59.6.9, "Timeouts," on page 875](#)
- ♦ [Section 59.6.10, "Relay Host," on page 876](#)
- ♦ [Section 59.6.11, "Host Authentication," on page 877](#)
- ♦ [Section 59.6.12, "Undeliverable Message Handling," on page 878](#)
- ♦ [Section 59.6.13, "Mailbomb and Spam Security," on page 878](#)

59.6.1 SMTP Enabled

The following switches enable SMTP and suppress version information display.

`--smtp`

`--nosmtpversion`

--smtp

Enables the GWIA to process SMTP messages. See [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,”](#) on page 757.

Syntax: --smtp

--nosmtpversion

Suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by another SMTP host or a telnet session.

Syntax: --nosmtpversion

59.6.2 iCal Enabled

The following switch enables [iCal](#).

[--imip](#)

--imip

Converts outbound GroupWise Calendar items into MIME text/calendar iCal objects and converts incoming MIME text/calendar messages into GroupWise Calendar items.

Syntax: --imip

59.6.3 Address Handling

The following switches determine how the GWIA handles email addresses:

[--aql](#)

[--aqor](#)

[--ari](#)

[--blockrulegenmsg](#)

[--dia](#)

[--displaylastfirst](#)

[--dontreplaceunderscore](#)

[--fd822](#)

[--fdmime](#)

[--group](#)

[--keepsendgroups](#)

[--msstu](#)

[--nomappriority](#)

[--notfamiliar](#)

[--realmailfrom](#)

--aql

Allows you to determine the address qualification level. It specifies which GroupWise address components (*domain.post_office.user*) must be included as the user portion of a GroupWise user's outbound Internet address (*userhost*). Valid options are *auto*, *userid*, *po*, and *domain*.

This switch is valid only if your system is not configured to use Internet-style addressing, as described in [Section 52, "Configuring Internet Addressing," on page 743](#), or you have configured the GWIA to ignore Internet-style addressing, as described in [Section 53.1.3, "Configuring How the GWIA Handles Email Addresses," on page 761](#).

Syntax: `--aql option`

Example: `--aql po`

Option	Description
<code>auto</code>	This option causes the gateway to include the addressing components required to make the user's address unique. If a user ID is unique in a GroupWise system, the outbound address uses only the <i>user_ID</i> . If the <i>post_office</i> or <i>domain.post_office</i> components are required to make the address unique, these components are also included in the outbound address. The <code>auto</code> option is the default.
<code>userid</code>	This option requires the gateway to include only the <i>user_ID</i> in the outbound Internet address, even if the user ID is not unique in the system. If a recipient replies to a user whose user ID is not unique and no other qualifying information is provided, that reply cannot be delivered.
<code>po</code>	This option requires the gateway to include <i>post_office.user_ID</i> in every outbound address, regardless of the uniqueness or non-uniqueness of the user ID.
<code>domain</code>	This option requires the gateway to include the fully qualified GroupWise address (<i>domain.post_office.user_ID</i>) in every outbound address, regardless of the uniqueness or non-uniqueness of the user ID. This option guarantees the uniqueness of every outbound Internet address, and ensures that any replies are delivered.

--aqor

The user part of a GroupWise user's outbound Internet address (*user@host*) can and sometimes must include the full Groupwise address (*domain.post_office.user_ID@host*) in order to be unique. The `--aqor` switch instructs the GWIA to move any GroupWise address components, except the *user_ID* component, to the right side of the address following the at sign (@). In this way, GroupWise addressing components become part of the host portion of the outbound Internet address. The `--aql` switch specifies which components are included.

For example, if the `--aqor` switch is used (in conjunction with the `--aql-domain` switch), Bob Thompson's fully qualified Internet address (`headquarters.advertising.bob@novell.com`) is resolved to `bob@advertising.headquarters.novell.com` for all outbound messages.

If the `--aqor` switch is used with the `--aql-po` switch, Bob's Internet address is resolved to `bob@advertising.novell.com` for all outbound messages.

If you use the `--aqor` switch to move GroupWise domain or post office names to be part of the host portion on the right side of the address, you must provide a way for the DNS server to identify the GroupWise names. You must either explicitly name all GroupWise post offices and domains in your system as individual MX Records, or you can create an MX Record with wildcard characters to represent all GroupWise post offices and domains. For information about creating MX Records, see details found in RFC #974.

For details about this setting, see [Section 53.1.3, “Configuring How the GWIA Handles Email Addresses,”](#) on page 761.

--ari

Enables or disables additional routing information that is put in the SMTP return address to facilitate replies. This switch might be needed in large systems with external GroupWise domains in which the external GroupWise users have not been configured in your local domain. Options include *Never* and *Always*. Most sites do not need to use this switch.

Syntax: --ari *never|always*

Example: --ari never

--blockrulegenmsg

In ConsoleOne, you can control whether or not rule-generated messages are allowed to leave your GroupWise system by selecting or deselecting the *Rule-Generated Messages* options available in each class of service defined for the GWIA. This switch allows you to be specific in the types of rule-generated messages that are blocked.

Syntax: --blockrulegenmsg forward | reply | none | all

Example: --blockrulegenmsg forward

In order for this switch to take effect, senders must be in a class of service where rule-generated messages are allowed. For more information, see [Section 54.1.2, “Creating a Class of Service,”](#) on page 788.

--dia

GroupWise supports both Internet-style addressing (*user@host*) and GroupWise proprietary addressing (*user_ID.post_office.domain*). By default, the GWIA uses Internet-style addressing. See [Section 53.1.3, “Configuring How the GWIA Handles Email Addresses,”](#) on page 761.

You can use this switch to disable Internet-style addressing. With Internet-style addressing disabled, messages use the mail domain name in the *Foreign ID* field in ConsoleOne (GWIA object > *GroupWise* > *Identification*) for the domain portion of a user’s Internet address. The GWIA continues to support user and post office aliases in either mode.

Syntax: --dia

--displaylastfirst

By default, users’ display names are First Name Last Name. If you want users’ display names to be Last Name First Name, you can use the --displaylastfirst switch. This forces the display name format to be Last Name First Name, regardless of the preferred address format.

Syntax: --displaylastfirst

--dontreplacescore

By default, the GWIA accepts addresses of the format:

firstname_lastname@internet_domain_name

Even though this is not an address format included in the Allowed Address Formats list in ConsoleOne for configuring Internet addressing, as described in [Section 52.1.5, "Allowed Address Formats," on page 747](#), you can use this switch to prevent this address format from being accepted by the GWIA.

Syntax: `--dontreplaceunderscore`

--fd822

Specifies a return address for GroupWise replies. A message that has been received by a GroupWise user through the GWIA and is replied to has this return address form. These switches cause the GWIA to produce a return address of the form *foreign_domain.type:"user host."* *Foreign domain* can be any foreign domain you have configured and linked to the GWIA.

You can use the same foreign domain name for both the `--fd822` switch and the `--fdmime` switch. You can specify multiple foreign domain and kind pairs by placing them in quotes. If multiple foreign domain and kind pairs are used, the first domain/kind pair is the return address for replies to messages received through the GWIA. The second domain/kind pair is checked to see what message format is used for old replies in the system. Up to four pairs can be specified with an 80-character limit.

This switch lets you change your foreign domain names in your GroupWise system and still have replies work. For example, if your foreign domain is called *faraway* and you added a foreign domain called Internet, you could use `--fd822-"internet.nonmime smtp.nonmime."` This causes replies to have a return address of *internet.nonmime.:"user@host."* The GWIA would also recognize *faraway*. This switch also lets you migrate from one foreign domain to another.

Most administrators do not need to use this switch.

Syntax: `--fd822 foreign_domain.type`

Example: `--fd822 Internet.nonmime`

--fdmime

Specifies a return address for GroupWise replies. A message that has been received by a GroupWise user through the GWIA and is replied to has this return address form. These switches cause the GWIA to produce a return address of the form *foreign_domain.type:"user host."* *Foreign_domain* can be any foreign domain you have configured and linked to the GWIA. *Type* can be either *mime* or *nonmime*.

You can use the same foreign domain name for both the `--fd822` switch and the `--fdmime` switch.

You can specify multiple foreign domain and kind pairs by placing them in quotes. If multiple foreign domain and kind pairs are used, the first domain/kind pair is the return address for replies to messages received through the GWIA. The second domain/kind pair is checked to see what message format is used for old replies in the system. Up to four pairs can be specified with an 80-character limit.

This switch lets you change your foreign domain names in your GroupWise system and still have replies work. For example, if your foreign domain is called SMTP and you add a foreign domain called Internet, you can use `--fdmime-"internet.mime smtp.mime."` This causes replies to have a return address of *internet.mime:"user@host."* The GWIA also recognizes SMTP. This switch also lets you migrate from one foreign domain to another.

Most administrators do not need to use this switch.

Syntax: `--fdmime foreign_domain.type`

Example: --fdmime Internet.mime

--group

Turns on distribution list expansion. By default, the GWIA does not expand distribution lists, which means that recipients listed in distribution lists do not receive incoming Internet messages that are addressed to distribution lists.

Use this switch to expand distribution lists into individual email addresses of the distribution list members, so that the recipients in distribution lists do receive incoming Internet messages addressed to distribution lists. See [Section 53.1.3, “Configuring How the GWIA Handles Email Addresses,” on page 761](#).

Syntax: --group

See also [--nickgroup](#).

--keepsendgroups

Prevents the GWIA from expanding distribution lists on messages going to external Internet users so that the SMTP header does not become too large.

Syntax: --keepsendgroups

--msstu

Replaces spaces with underscores (_) in the email address of the sender for outbound messages. For example, john smith becomes john_smith.

It does not replace spaces in the addresses of recipients.

Syntax: --msstu

--nickgroup

Turns on distribution list expansion only for distribution lists that have nicknames. By default, the GWIA does not expand distribution lists, which means that recipients listed in distribution lists do not receive incoming Internet messages that are addressed to distribution lists. If you use the --group switch, the GWIA expands all distribution lists.

Use this switch to expand only nicknamed distribution lists. This means that recipients listed in nicknamed distribution lists do receive incoming Internet messages that are addressed to the nickname of the distribution list, but they do not receive incoming Internet messages that are addressed to distribution lists that do not have nicknames. For information about nicknames, see [Section 14.7, “Managing User Email Addresses,” on page 247](#). See also [Section 53.1.3, “Configuring How the GWIA Handles Email Addresses,” on page 761](#).

Syntax: --nickgroup

See also [--group](#).

--nomappriority

Disables the function of mapping an x-priority *MIME* field to a GroupWise priority for the message. By default, the GWIA maps x-priority 1 and 2 messages as high priority, x-priority 3 messages as normal priority, and x-priority 4 and 5 as low priority in GroupWise.

Syntax: --nomappriority

--notfamiliar

Instructs the GWIA to not include the user's familiar name, or display name, in the *From* field of the message's *MIME* header. In other words, the *From* field is *address* rather than "*familiar_name*" *address*.

Syntax: --notfamiliar

--realmailfrom

Instructs the GWIA to use the real user in the *Mail From* field instead of having auto-forwards come from Postmaster and auto-replies come from Mailer-Daemon.

Syntax: --realmailfrom

59.6.4 Message Formatting and Encoding

The following switches determine how the GWIA formats and encodes inbound and outbound email messages:

--attachmsg
--dbchar822
--charsetconfidencelevel
--defaultcharset
--defaultnonmimecharset
--force7bitout
--iso88591is
--koi8
--mime
--noiso2022
--noqpmt
--relayaddsignature
--rt
--st
--uueaa
--wrap

For more information, see [Section 7.4, "MIME Encoding,"](#) on page 125.

--attachmsg

Instructs the GWIA to maintain the original format of any file type attachment.

Syntax: --attachmsg

--charsetconfidencelevel

Sets the confidence level at which you want the GWIA to use the detected character set rather than the default character set when no character set is specified. The GWIA tries to detect the character set based on the presence or absence of certain characters in the text. The default confidence level is 25, meaning that if the detection process returns a confidence level of 25 or above, the GWIA uses the detected character set, but if the confidence level is less than 25, the GWIA uses the default character set. Valid values range from 0 to 100.

Syntax: `--charsetconfidencelevel number`

Example: `--charsetconfidencelevel 35`

--dbchar822

Instructs the GWIA to map inbound non-MIME messages to another character set that you specify. The mapped character set must be an Asian (double-byte) character set.

Syntax: `--dbchar822 charset`

Example: `--dbchar822 shift_jis`

--defaultcharset

Specifies what character set to use if no character set is specified in an incoming MIME-encoded message.

Syntax: `--defaultcharset charset`

Example: `--defaultcharset iso-8859-1`

--defaultnonmimecharset

Specifies what character set to use if no character set is specified in an incoming message that is not MIME encoded. The default is US_ASCII.

Syntax: `--defaultnonmimecharset charset`

Example: `--defaultnonmimecharset iso-8859-1`

--force7bitout

By default, the GWIA uses 8-bit MIME encoding for any outbound messages that are HTML-formatted or that contain 8-bit characters. If, after connecting with the receiving SMTP host, the GWIA discovers that the receiving SMTP host cannot handle 8-bit MIME encoded messages, the GWIA converts the messages to 7-bit encoding.

You can use the `--force7bitout` switch to force the GWIA to use 7-bit encoding and not attempt to use 8 bit MIME encoding. You should use this option if you are using a relay host that does not support 8-bit MIME encoding. See [Section 53.1.1, "Configuring Basic SMTP/MIME Settings," on page 757](#).

Syntax: `--force7bitout`

--iso88591is

Instructs the GWIA to map inbound MIME ISO-8859-1 messages to another character set that you specify.

Syntax: `--iso88591is charset`

Example: `--iso88591is big5`

--koi8

Instructs the GWIA to map all outbound MIME messages to the KOI8 (Russian) character set.

Syntax: `--koi8`

--mime

Instructs the GWIA to send outbound messages in MIME format rather than in RFC-822 format. If you've defined an RFC-822 non-GroupWise domain, as described in [Section 6.8, "Adding External Users to the GroupWise Address Book," on page 116](#), users can still send RFC-822 formatted messages by using the RFC-822 domain in the address string when sending messages. Removing the switch corresponds to enabling the Default Message Encoding: Basic RFC-822 switch in ConsoleOne. See [Section 53.1.4, "Determining Format Options for Messages," on page 763](#).

Syntax: `--mime`

--noiso2022

Instructs the GWIA to not use ISO-2022 character sets. ISO-2022 character sets provide 7-bit encoding for Asian character sets.

Syntax: `--noiso2022`

--nqpmt

Disables quoted printable message text for outbound messages. If this switch is turned on, messages are sent with Base64 MIME encoding, unless all the text is US-ASCII. If you use this switch you need to review the setting for the `--wrap` switch to ensure that message text wraps correctly. See [Section 53.1.4, "Determining Format Options for Messages," on page 763](#).

Syntax: `--nqpmt`

--relayaddsignature

Appends the global signature to messages that are relayed through your GroupWise system (for example, messages from POP and IMAP clients) in addition to messages that originate within your GroupWise system. See [Section 14.3, "Adding a Global Signature to Users' Messages," on page 231](#).

Syntax: `--relayaddsignature`

--rt

Specifies the maximum number of threads that the GWIA uses when converting inbound messages from MIME or RFC-822 format to the GroupWise message format. The default setting is 4. See [Section 53.1.4, “Determining Format Options for Messages,” on page 763](#).

Multiple threading allows for more than one receive process to be running concurrently. A receive request is assigned to a single thread and is processed by that thread. If you anticipate heavy inbound message traffic, you can increase the number of threads to enhance the speed and performance of the GWIA. The number of threads is limited only by the memory resources of your server.

Syntax: --rt

--st

Specifies the maximum number of threads that the GWIA uses when converting outbound messages from GroupWise message format to MIME or RFC-822 format. The default setting is 4. See [Section 53.1.4, “Determining Format Options for Messages,” on page 763](#).

Multiple threading allows for more than one send process to be running concurrently. A send request is assigned to a single thread and is processed by that thread. If you anticipate heavy outbound message traffic, you can increase the number of threads to enhance the speed and performance of the GWIA. The number of threads is limited only by the memory resources of your server.

Syntax: --st

--uueaa

Forces the GWIA to UUencode any ASCII text files attached to outbound RFC-822 formatted messages. This switch applies only if the `--mime` switch is not used. Without this switch, the GWIA includes the text as part of the message body. See [Section 53.1.4, “Determining Format Options for Messages,” on page 763](#).

Syntax: --uueaa

--wrap

Sets the line length for outbound messages that do not use quoted printable or Base64 MIME encoding. This is important if the recipient’s email system requires a certain line length. See [Section 53.1.4, “Determining Format Options for Messages,” on page 763](#).

Syntax: --wrap *line_length*

Example: --wrap 72

59.6.5 Forwarded and Deferred Messages

The following switches configure how the GWIA handles forwarded and deferred messages:

[--flatfwd](#)

[--delayedmsgnotification](#)

[--maxdeferhours](#)

[--msgdeferinterval](#)

--flatfwd

Automatically strips out the empty message that is created when a message is forwarded without adding text, and retains the original sender of the message, rather than showing the user who forwarded it. This facilitates users forwarding messages from GroupWise to other email accounts. Messages arrive in the other accounts showing the original senders, not the users who forwarded the messages from GroupWise.

Syntax: --flatfwd

--delayedmsgnotification

Provides a notification message to users whose email messages cannot be immediately sent out across the Internet. This provides more noticeable notification to users than manually checking the Properties page of the sent item to see whether it has been sent.

Syntax: --delayedmsgnotification

See [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,” on page 757](#).

--maxdeferhours

Specifies the number of hours after which the GWIA stops trying to send deferred messages. The default is 96 hours, or four days. A deferred message is any message that can't be sent because of a temporary problem (host down, MX record not found, and so on). See [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,” on page 757](#).

Syntax: --maxdeferhours *hours*

Example: --maxdeferhours 48

--msgdeferinterval

Specify in a comma-delimited list the number of minutes after which the GWIA retries sending deferred messages. The default is 20, 20, 20, 240. The GWIA interprets this list as follows: It retries 20 minutes after the initial send, 20 minutes after the first retry, 20 minutes after the second retry, and 240 minutes (4 hours) after the third retry. Thereafter, it retries every 240 minutes until the number of hours specified in the *Maximum Number of Hours to Retry a Deferred Message* field is reached. You can provide additional retry intervals as needed. It is the last retry interval that repeats until the maximum number of hours is reached. See [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,” on page 757](#).

Syntax: --msgdeferinterval *minutes,minutes...,minutes*

Example: --msgdeferinterval 10,10,10,120

59.6.6 Extended SMTP

The following switches configure the GWIA's Extended SMTP (ESMTP) settings:

[--noesmtplib](#)

[--dsn](#)

[--dsnage](#)

--noesmtplib

Disables ESMTP support in the GWIA.

Syntax: --noesmtplib

--dsn

Enables Delivery Status Notification (DSN). The GWIA requests status notifications for outgoing messages and supplies status notifications for incoming messages. This requires the external email system to also support Delivery Status Notification. Currently, notification consists of two delivery statuses: successful and unsuccessful. See [Section 53.1.2, “Using Extended SMTP \(ESMTP\) Options,” on page 760](#).

Syntax: --dsn

--dsnage

The --dsnage switch specifies the number of days that the GWIA retains information about the external sender so that status updates can be delivered to him or her. For example, the default DSN age causes the sender information to be retained for 4 days. If the GWIA does not receive delivery status notification from the GroupWise recipient’s Post Office Agent (POA) within that time period, it deletes the sender information and the sender does not receive any delivery status notification. See [Section 53.1.2, “Using Extended SMTP \(ESMTP\) Options,” on page 760](#).

Syntax: --dsnage

59.6.7 Send/Receive Cycle and Threads

The following switches configure the GWIA’s SMTP send/receive cycle and threads:

--p
--rd
--sd
--killthreads
--smtpport

--p

Specifies how often, in seconds, the GWIA polls for outbound messages. The default, 10 seconds, causes the GWIA to poll the outbound message directory every 10 seconds. See [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,” on page 757](#).

Syntax: --p *seconds*

Example: --p 5

--rd

Specifies the maximum number of threads used for processing SMTP receive requests (inbound messages). Each thread is equivalent to one connection. The default is 16 threads. See [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,” on page 757](#).

Syntax: --rd *number_of_threads*

Example: --rd 20

--sd

Specifies the maximum number of threads used for processing SMTP send requests (outbound messages). Each thread is equivalent to one connection. The default is 8 threads. See [Section 53.1.1, “Configuring Basic SMTP/MIME Settings,” on page 757](#).

Syntax: --sd *number_of_threads*

Example: --sd 12

--killthreads

Instructs the GWIA to quickly terminate any active send/receive threads when it restarts.

Syntax: --killthreads

--smtpport (Linux only)

Changes the SMTP listen port from the default of 25. Use this switch only if the GWIA is receiving messages only from SMTP hosts that can be configured to connect to GWIA on a specified port.

Syntax: --smtpport

Example: --smtpport 2525

59.6.8 Dial-Up Connections

SMTP dial-up services can be used when you don't require a permanent connection to the Internet and want to periodically check for mail messages queued for processing. The following switches can be used when configuring dial-up services. For more information about dial-up services, see [Section 53.1.7, “Configuring SMTP Dial-Up Services,” on page 767](#).

[--usedialup](#)

[--etrnhost](#)

[--etrnqueue](#)

[/dialuser](#) (Windows only)

[/dialpass](#) (Windows only)

--usedialup

Enables SMTP dial-up services. See [“Enabling Dial-Up Services” on page 767](#).

Syntax: --usedialup

--etrnhost

Specifies the IP address or DNS hostname of the mail server where your mail account resides at your Internet Service Provider. You should obtain this address from your Internet Service Provider. See [“Enabling Dial-Up Services” on page 767](#).

Syntax: --etrnhost *address*

Example: --etrnhost 172.16.5.18

--etrnqueue

Specifies your email domain as provided by your Internet Service Provider. See [“Enabling Dial-Up Services” on page 767](#).

Syntax: --etrnqueue *email_domain*

Example: --etrnqueue novell.com

/dialuser (Windows Only)

Specifies the RAS Security user if you are using a Windows Remote Access Server (RAS) and the GWIA is not running on the same server as the RAS.

Syntax: /dialuser-*user_name*

Example: /dialuser-rasuser

/dialpass (Windows Only)

Specifies the RAS Security user’s password if you are using a Windows Remote Access Server (RAS) and the GWIA is not running on the same server as the RAS.

Syntax: /dialpass-*password*

Example: /dialpass-raspassword

59.6.9 Timeouts

The following switches specify how long SMTP services waits to receive data that it can process. After the time expires, the GWIA might give a TCP read/write error. Leave these switches at the default setting unless you are experiencing a problem with communication.

--tc

--td

--te

--tg

--tr

--tt

--tc

Specifies how long the program waits for an SMTP command. The default is 2 minutes.

Syntax: --tc *minutes*

Example: --tc 3

--td

Specifies how long the program waits for data from the receiving host. The default is 5 minutes.

Syntax: `--td minutes`

Example: `--td 2`

--te

Specifies how long the program waits for the receiving host to establish a connection. The default is 5 minutes.

Syntax: `--te minutes`

Example: `--te 2`

--tg

Specifies how long the program waits for the initial greeting from the receiving host. The default is 3 minutes.

Syntax: `--tg minutes`

Example: `--tg 2`

--tr

Specifies how long the program waits for a TCP read. The default is 10 minutes.

Syntax: `--tr minutes`

Example: `--tr 2`

--tt

Specifies how long the program waits for the receiving host to terminate the connection. The default is 5 minutes.

Syntax: `--tt minutes`

Example: `--tt 2`

59.6.10 Relay Host

The following switch configures whether or not the GWIA uses a relay host.

`--mh`

--mh

Specifies the IP address or DNS hostname of one or more relay hosts that you want the GWIA to use for outbound messages. Use a space to separate multiple relay hosts in a list.

The relay host can be part of your network or can reside at the Internet service provider's site. This switch is typically used in firewall integration if you want one server, the specified relay host, to route all mail. See [Section 53.1.1, "Configuring Basic SMTP/MIME Settings," on page 757](#).

Syntax: --mh *address*

Example: --mh 172.16.5.18

59.6.11 Host Authentication

The GWIA supports SMTP host authentication for both inbound and outbound message traffic. The following switches are used with inbound and outbound authentication:

[--forceinboundauth](#)

[--forceoutboundauth](#)

--forceinboundauth

Ensures that the GWIA accepts messages only from remote SMTP hosts that use the AUTH LOGIN authentication method to provide a valid GroupWise user ID and password. The remote SMTP hosts can use any valid GroupWise user ID and password. However, for security reasons, we recommend that you create a dedicated GroupWise user account for remote SMTP host authentication.

Syntax: --forceinboundauth

NOTE: Using the --forceinboundauth switch overrides the Prevent Message Relaying setting for the GWIA in ConsoleOne for POP and IMAP users. To completely prevent message relaying when using the --forceinboundauth switch, you must also specify the [--disallowauthrelay](#) switch.

--forceoutboundauth

Ensures that the GWIA sends messages only to remote SMTP hosts that are included in a `gwauth.cfg` text file. The remote SMTP hosts must support the AUTH LOGIN authentication method.

The `gwauth.cfg` file must reside in the `domain\wpgate\gwia` directory and use the following format:

```
domain_name authuser authpassword
```

For example:

```
smtp.novell.com remotehost novell
```

You can define multiple hosts in the file. Make sure you include a hard return after the last entry.

If you use this switch, you need to include your GWIA as an entry in the `gwauth.cfg` file to enable status messages to be returned to GroupWise users. You can use any GroupWise user ID and password for your GWIA's authentication credentials. However, for security reasons, we recommend that you create a dedicated GroupWise user account for your GWIA.

Syntax: --forceoutboundauth

59.6.12 Undeliverable Message Handling

The following switches determine how the GWIA handles undeliverable messages:

--badmsg
--fut
--mudas

--badmsg

Specifies where to send problem messages. Problem messages can be placed in the GWIA problem directory (`gwprob`), they can be sent to the postmaster, or they can be sent to both or neither. The values for this switch are `move`, `send`, `both`, and `neither`.

The `move` option specifies to place problem messages in the `gwprob` directory for the GWIA. The `send` option specifies to send the message as an attachment to the GWIA postmaster defined in ConsoleOne (GWIA object > *GroupWise* > *Gateway Administrators*). The `both` option specifies to move the message to `gwprob` and send it to the postmaster. The `neither` option specifies to discard problem messages. The default when no switch is specified is `move`. See [Section 53.1.6, "Determining What to Do with Undeliverable Messages," on page 766](#).

Syntax: --badmsg `move|send|both|neither`

Example: --badmsg both

--fut

Forwards undeliverable messages to the specified host. See [Section 53.1.6, "Determining What to Do with Undeliverable Messages," on page 766](#).

Syntax: --fut *host*

Example: --fut novell.com

--mudas

Controls how much of the original message is sent back when a message is undeliverable. By default, only 2 KB of the original message is sent back. The value is specified in KB (8=8KB). See [Section 53.1.6, "Determining What to Do with Undeliverable Messages," on page 766](#).

Syntax: --mudas *KB*

Example: --mudas 16

59.6.13 Mailbomb and Spam Security

Multiple unsolicited messages (sometimes called a *mailbomb* or *spam*) from the Internet can potentially harm your GroupWise messaging environment. At the least, it can be annoying to your users. You can use the following switches to help protect your GroupWise system from malicious, accidental, and annoying attacks:

--disallowauthrelay
--mbcount
--mbtime
--rejbs

--xspam

--rbl

--disallowauthrelay

Prevents spammers from using GroupWise accounts to authenticate to the GWIA and using it as a relay host for their spam. It has no effect on normal GroupWise account usage in a GroupWise client or WebAccess. However, it does prevent users who access their GroupWise mailboxes from a POP or IMAP client from sending messages to users outside of the GroupWise system, because the GWIA identifies this activity as relaying.

Syntax: --disallowauthrelay

--mbcount

Sets the number of messages that can be received from a single IP address in a given number of seconds before the GWIA denies access to its GroupWise system. It provides a form of system security to protect your system from mailbombs.

For example, with --mbcount set to 25 and --mbtime set to 60 seconds, if these limits are exceeded the sender's IP address is blocked from sending any more messages. The IP address of the sender is also displayed in the GWIA console. You can permanently restrict access to your system by that IP address through settings on the Access Control page in ConsoleOne (GWIA object > *Access Control*). By default, the mailbomb feature is turned off. To enable this feature, you must specify a value for mailbomb count and mailbomb time. See [Section 54.2.4, "Mailbomb \(Spam\) Protection," on page 801](#).

Syntax: --mbcount-*number*

Example: --mbcount 25

--mbtime

Specifies the mailbomb time limit in seconds. This switch works with the --mbcount switch to block access to your GroupWise system from unsolicited inundations of email. The default value is 10 seconds. See [Section 54.2.4, "Mailbomb \(Spam\) Protection," on page 801](#).

Syntax: --mbtime *seconds*

Example: --mbtime 60

--rejbs

Prevents delivery of messages if the sender's host is not authentic. When this switch is used, the GWIA refuses messages from a host if a DNS reverse lookup shows that a PTR record does not exist for the IP address of the sender's host. See [Section 54.2.4, "Mailbomb \(Spam\) Protection," on page 801](#).

If this switch is not used, the GWIA accepts messages from any host, but displays a warning if the initiating host is not authentic.

Syntax: --rejbs

--xspam

Flags messages to be handled by the client Junk Mail Handling feature if they contain an x-spam-flag:yes in the MIME header. See [Section 54.2.5, “Customized Spam Identification,” on page 802](#).

Syntax: --xspam

--rbl

Lets you define the addresses of blacklist sites (free or fee-based) you want the GWIA to check for blacklisted hosts. If a host is included in a site’s blacklist, the GWIA does not accept messages from it.

Syntax: --rbl bl.spamcop.net

This switch corresponds to the Blacklist Addresses list (GWIA object > *Access Control* > *Blacklists*). For details about this setting, see [Section 54.2.1, “Real-Time Blacklists,” on page 798](#).

59.7 POP3 Switches

The following optional startup switches that can be used to configure the GWIA’s POP3 service:

- noproversion
- pop3
- popintruderdetect
- popport
- popsport
- popssl
- pt
- sslpt

59.7.1 --noproversion

Suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by a POP client.

Syntax: --noproversion

59.7.2 --pop3

Enables POP3 client access to GroupWise mailboxes through the GWIA. See [Section 53.2.1, “Enabling POP3/IMAP4 Services,” on page 778](#).

Syntax: --pop3

59.7.3 --popintruderdetect

Instructs the GWIA to log POP email clients in through the POA so that the POA’s intruder detection can take effect, if intruder has been configured in ConsoleOne (POA object > *Client Access Settings* > *Intruder Detection*). This switch cannot be used with older POAs that do not support intruder detection.

Syntax: --popintruderdetect

59.7.4 --popport

By default, the GWIA listens for POP3 connections on port 110. This switch allows you to change the POP3 listen port.

Syntax: `--popport port_number`

Example: `--popport 111`

59.7.5 --popsport

By default, the GWIA listens for secure (SSL) POP3 connections on port 995. This switch allows you to change the POP3 SSL listen port.

Syntax: `--popsport port_number`

Example: `--popsport 996`

59.7.6 --popssl

Disables, enables, or requires secure (SSL) connections between POP3 clients and the GWIA. See [Section 55.4, “Securing GWIA Connections with SSL,”](#) on page 812.

Syntax: `--popssl enabled | disabled | required`

Example: `--popssl required`

Option	Description
enabled	The POP3 client determines whether an SSL connection or non-SSL connection is used. By default, the GWIA listens for SSL connections on port 995 and non-SSL connections on port 110. You can use the <code>--popsport</code> and <code>--popport</code> switches to change these ports.
required	The GWIA forces SSL connections on port 995 and port 110. Non-SSL connections are denied. You can use the <code>--popsport</code> and <code>--popport</code> switches to change these ports.
disabled	The GWIA listens for connections only on port 110, and the connections are not secure. You can use the <code>--popport</code> switch to change this port.

59.7.7 --pt

Specifies the maximum number of threads to be used for POP3 connections. The default number is 10. You are limited only by the memory resources of your server. See [Section 53.2.1, “Enabling POP3/IMAP4 Services,”](#) on page 778.

Syntax: `--pt number_of_threads`

Example: `--pt 15`

59.7.8 --sslpt

Specify the maximum number of threads you want the GWIA to use for secure POP3 connections. You are limited only by the memory resources of your server. See [Section 53.2.1, “Enabling POP3/IMAP4 Services,”](#) on page 778.

Syntax: `--sslpt number_of_threads`

Example: --sslpt 15

59.8 IMAP4 Switches

The following optional startup switches that can be used to configure the GWIA's IMAP4 service:

--imap4
--imapport
--imapreadlimit
--imapreadnew
--imapsport
--imapssl
--it
--noimapversion
--sslit

59.8.1 --imap4

Enables IMAP4 client access to GroupWise mailboxes through the GWIA. See [Section 53.2.1, "Enabling POP3/IMAP4 Services,"](#) on page 778.

Syntax: --imap4

59.8.2 --imapport

By default, the GWIA listens for IMAP4 connections on port 143. This switch allows you to change the IMAP4 listen port.

Syntax: --imapport *port_number*

Example: --imapport 144

59.8.3 --imapreadlimit

By default, the GWIA downloads a maximum of 20,000 items at a time. This switch allows you to specify, in thousands, the maximum number of items you want the GWIA to download. For example, specifying 30 indicates 30,000.

Syntax: --imapreadlimit *number_of_items*

Example: --imapreadlimit 30

59.8.4 --imapreadnew

By default, the GWIA reads items in a folder from the oldest to the newest. As a result, if a folder contains more items than are allowed by the [/imapreadlimit](#) setting, users receive the older items but not the newer items. Enable this switch so that the GWIA reads items from the newest to the oldest. This ensures that users receive all their new items in a timely manner.

Syntax: --imapreadnew

59.8.5 --imapport

By default, the GWIA listens for secure (SSL) IMAP4 connections on port 993. This switch allows you to change the IMAP4 SSL listen port.

Syntax: `--imapport port_number`

Example: `--imapport 994`

59.8.6 --imapssl

Disables, enables, or requires secure (SSL) connections between IMAP4 clients and the GWIA. See [Section 55.4, “Securing GWIA Connections with SSL,” on page 812.](#)

Syntax: `--IMAP4ssl enabled|disabled|required`

Example: `--popssl required`

Option	Description
enabled	The IMAP4 client determines whether an SSL connection or non-SSL connection is used. By default, the GWIA listens for SSL connections on port 993 and non-SSL connections on port 143. You can use the <code>--imapport</code> and <code>--imapport</code> switches to change these ports.
required	The GWIA forces SSL connections on port 993 and port 143. Non-SSL connections are denied. You can use the <code>--imapport</code> and <code>--imapport</code> switches to change these ports.
disabled	The GWIA listens for connections only on port 143, and the connections are not secure. You can use the <code>--imapport</code> switch to change this port.

59.8.7 --it

Specifies the maximum number of threads to be used for IMAP4 connections. The default number is 10. You are limited only by the memory resources of your server. See [Section 53.2.1, “Enabling POP3/IMAP4 Services,” on page 778.](#)

Syntax: `--it number_of_threads`

Example: `--it 15`

59.8.8 --noimapversion

Suppresses the GroupWise version and copyright date information that the GWIA typically responds with when contacted by an IMAP client.

Syntax: `--noimapversion`

59.8.9 --sslit

Specify the maximum number of threads you want the GWIA to use for secure IMAP4 connections. You are limited only by the memory resources of your server. See [Section 53.2.1, “Enabling POP3/IMAP4 Services,” on page 778.](#)

Syntax: `--sslit number_of_threads`

Example: `--sslit 15`

59.9 HTTP (Web Console) Switches

The following switches enable the HTTP Web console and control its configuration settings. The Web console enables you to monitor the GWIA through a Web browser. For more information, see [Section 56.2, “Using the GWIA Web Console,” on page 827](#).

`--httpport`
`--httpuser`
`--httppassword`
`--httprefresh`
`--httpsl`

59.9.1 `--httpport`

Specifies the port where the GWIA listens for the Web console. The default port established during installation is 9850.

Syntax: `--httpport` *port_number*

Example: `--httpport 9851`

59.9.2 `--httpuser`

By default, any user who knows the GWIA’s address and port (`--httpport`) can use the Web console. This switch adds security to the Web console by forcing users to log into the Web console using the specified user name. The `--httppassword` switch must also be used to establish the user password.

Syntax: `--httpuser` *user_name*

Example: `--httpuser gwia`

The *user_name* can be any arbitrary name.

59.9.3 `--httppassword`

Specifies the password that must be supplied along with the user name provided by `--httpuser`.

Syntax: `--httppassword` *password*

Example: `--httppassword monitor`

59.9.4 `--httprefresh`

By default, the GWIA refreshes the Web console information every 60 seconds. You can use this switch to override the default refresh interval.

Syntax: `--httprefresh` *seconds*

Example: `--httprefresh 120`

59.9.5 --httpsl

Enables the GWIA to use a secure connection to a Web browser being used to display the GWIA Web console. The Web browser must also be enabled to use SSL; if it is not, a non-secure connection is used. See [Section 55.4, "Securing GWIA Connections with SSL,"](#) on page 812.

Syntax: --httpsl

59.10 SSL Switches

The GWIA can use SSL to enable secure SMTP, POP, IMAP, and HTTP connections. The following switches can be used to 1) specify the server certificate file, key file, and key file password required for SSL and 2) enable or disable SSL for SMTP, POP, IMAP, and HTTP connections. See [Section 55.4, "Securing GWIA Connections with SSL,"](#) on page 812.

--certfile
--keyfile
--keypasswd
--smtpssl
--httpsl
--popssl
--imapssl
--ldapssl

59.10.1 --certfile

Specifies the server certificate file to use. The file must be in Base64/PEM or PFX format. If the file is not in the same directory as the GWIA program, specify the full path.

Syntax: --certfile *file_name*

Example: --certfile \\server1\sys\server1.crt

59.10.2 --keyfile

Specifies the private key file to use. The key file is required if the certificate file does not contain the key. If the certificate file contains the key, do not use this switch. When specifying a file name, use the full path if the file is not in the same directory as the GWIA program.

Syntax: --keyfile *file_name*

Example: --keyfile \\server1\sys\server1.key

59.10.3 --keypasswd

Specifies the private key password. If the key does not require a password, do not use this switch.

Syntax: --keypasswd *password*

Example: --keypasswd novell

59.10.4 --smtpssl

Enables the GWIA to use a secure connection to other SMTP hosts. The SMTP host must also be enabled to use SSL or TLS (Transport Layer Security); if it is not, a non-secure connection is used. Valid settings are enabled and disabled.

Syntax: `--smtpssl setting`

Example: `--smtpssl enabled`

59.10.5 --httpsl

Enables the GWIA to use a secure connection to a Web browser being used to display the GWIA Web console. The Web browser must also be enabled to use SSL; if it is not, a non-secure connection is used. Valid settings are enabled and disabled.

Syntax: `--httpsl setting`

Example: `--httpsl enabled`

59.10.6 --popssl

Disables, enables, or requires secure (SSL) connections between POP3 clients and the GWIA.

Syntax: `--popssl enabled|disabled|required`

Example: `--popssl required`

Option	Description
enabled	The POP3 client determines whether an SSL connection or non-SSL connection is used. By default, the GWIA listens for SSL connections on port 995 and non-SSL connections on port 110. You can use the <code>--popsport</code> and <code>--popport</code> switches to change these ports.
required	The GWIA forces SSL connections on port 995 and port 110. Non-SSL connections are denied. You can use the <code>--popsport</code> and <code>--popport</code> switches to change these ports.
disabled	The GWIA listens for connections only on port 110, and the connections are not secure. You can use the <code>--popport</code> switch to change this port.

59.10.7 --imapssl

Disables, enables, or requires secure (SSL) connections between IMAP4 clients and the GWIA.

Syntax: `--IMAP4ssl enabled|disabled|required`

Example: `--popssl required`

Option	Description
enabled	The IMAP4 client determines whether an SSL connection or non-SSL connection is used. By default, the GWIA listens for SSL connections on port 993 and non-SSL connections on port 143. You can use the <code>--imapsport</code> and <code>--imapport</code> switches to change these ports.
required	The GWIA forces SSL connections on port 993 and port 143. Non-SSL connections are denied. You can use the <code>--imapsport</code> and <code>--imapport</code> switches to change these ports.

Option	Description
disabled	The GWIA listens for connections only on port 143, and the connections are not secure. You can use the <code>/imapport</code> switch to change this port.

59.10.8 /ldapssl

Instructs the GWIA to use a secure (SSL) connection with an LDAP server. For more information about why the GWIA would need to connect to an LDAP server, see [Section 59.11, “LDAP Switches,” on page 887](#)

Syntax: `/ldapssl`

59.11 LDAP Switches

The GWIA can perform GroupWise authentication of POP3/IMAP4 clients through an LDAP server and can also perform LDAP queries for GroupWise information. see [Section 53.3.1, “Enabling LDAP Services,” on page 783](#).

The following sections describe the switches required to configure this functionality:

- [Section 59.11.1, “GroupWise Authentication Switches,” on page 887](#)
- [Section 59.11.2, “LDAP Query Switches,” on page 888](#)

59.11.1 GroupWise Authentication Switches

When a POP3/IMAP4 user attempts to access a GroupWise mailbox on a post office that has been configured for LDAP authentication, the GWIA connects to the post office’s POA, which then connects to the LDAP server so that the LDAP server can authenticate the user.

This process works automatically if the GWIA’s link to the post office is client/server (meaning that it communicates through TCP/IP to the post office’s POA). If the GWIA is using a direct link to the post office directory rather than a client/server link to the post office’s POA, the GWIA must communicate directly with the LDAP server rather communicate through the POA.

The following switches are used to provide the GWIA with the required LDAP server information:

`--ldapipaddr`

`--ldapport`

`--ldapssl`

`--ldapuser`

`--ldappwd`

--ldapipaddr

Specifies the IP address of the LDAP server through which GroupWise authentication takes place.

Syntax: `--ldapipaddr address`

Example: `--ldapipaddr 172.16.5.18`

--ldapport

Specifies the port number being used by the LDAP server. The standard non-SSL LDAP port number is 389. The standard SSL LDAP port number is 636.

Syntax: `--ldapport number`

Example: `--ldapport 389`

--ldapssl

Instructs the GWIA to use a secure (SSL) connection with the LDAP server.

Syntax: `--ldapssl`

--ldapuser

Specifies a user that has rights to the LDAP directory. The user must have at least Read rights.

Syntax: `--ldapuser user_name`

Example: `--ldapuser ldap`

--ldappwd

Specifies the password of the user specified by the `--ldapuser` switch.

Syntax: `--ldappwd password`

Example: `--ldappwd pwd1`

59.11.2 LDAP Query Switches

The GWIA can function as an LDAP server, allowing LDAP queries for GroupWise user information contained in the directory. The following switches configure the GWIA as an LDAP server.

`--ldap`

`--ldaphthrd`

`--ldapcntxt`

`--ldaprefurl`

`--ldaprefcntxt`

`--ldapserversport`

`--ldapserversslport`

--ldap

Enables the GWIA as an LDAP server.

Syntax: `--ldap`

--ldapthrd

Specifies the maximum number of threads the GWIA can use for processing LDAP queries. The default is 10.

Syntax: `--ldapthrd number`

Example: `--ldapthrd 5`

--ldapcntxt

Limits the directory context in which the LDAP server searches. For example, you could limit LDAP searches to a single Novell organization container located under the United States country container.

If you restrict the LDAP context, you must make sure that users, when defining the directory in their email client, enter the same context (using the identical text you did) in the Search Base or Search Root field.

Syntax: `--ldapcntxt "context"`

Example: `--ldapcntxt "O=Novell,C=US"`

--ldaprefurl

Defines a secondary LDAP server to which you can refer an LDAP query if the query fails to find a user or address in your GroupWise system. For this option to work, the requesting Web browser must be able to track referral URLs.

Syntax: `--ldaprefurl url`

Example: `--ldapurl ldap://ldap.provider.com`

--ldaprefcntxt

Limits the directory context in which the secondary (referral) LDAP server searches.

Syntax: `--ldaprefcntxt "context"`

Example: `--ldaprefcntxt "O=Novell,C=US"`

--ldapserversport

Changes the LDAP listen port from the default of 389.

Syntax: `--ldapserversport port_number`

Example: `--ldapserversport 390`

--ldapserversslport

Changes the LDAP SSL listen port from the default of 636.

Syntax: `--ldapserversslport port_number`

Example: `--ldapserversslport 637`

59.12 Log File Switches

The following switches control how the GWIA uses the log file. The log file keeps a record of all GWIA activity. See [Section 56.6, “Using GWIA Log Files,”](#) on page 833.

--log
--logdays
--loglevel
--logmax

59.12.1 --log

The default location for GWIA log files varies by platform:

Linux: /var/log/novell/groupwise/domain_name.gwia
Windows domain\wpgate\gwia\000.prc

The log files are named after the month, day, and log number for that date (*mmddgwia.nn*). You can use the --log switch to redirect the log files to a different location.

Syntax: --log-*log_file_directory*

Linux Example: --log /opt/novell/groupwise/agents/log

Windows Example: --log-c:\log\gwia

59.12.2 --logdays

By default, log files are deleted after 30 days. This switch overrides the default setting. The range is from 1 to 360 days.

Syntax: --logdays *days*

Example: --logdays 5

59.12.3 --loglevel

Defines the amount of information to record in log files.

The values are:

- ♦ Diagnostic
- ♦ Verbose
- ♦ Normal (Default)
- ♦ Off

Syntax: --loglevel *level*

Example: --loglevel verbose

59.12.4 --logmax

Controls the maximum amount of disk space for all log files. The amount of disk space each log file consumes is added together to determine the total amount of disk space used. When the limit is reached, the GWIA deletes the existing log files, starting with the oldest one. The default is 102400 (100 MB). The maximum allowable setting is 102400000 (1 GB). Specify 0 (zero) for unlimited disk space.

Syntax: --logmax *KB*

Example: --logmax 512

XIII WebAccess

- ♦ Chapter 60, “Accessing Your GroupWise Mailbox in a Web-Based Environment,” on page 895
- ♦ Chapter 61, “Scaling Your GroupWise WebAccess Installation,” on page 899
- ♦ Chapter 62, “Configuring the WebAccess Application,” on page 903
- ♦ Chapter 63, “Monitoring the WebAccess Application,” on page 917

For a complete list of port numbers used by the WebAccess Application, see [Section A.7, “WebAccess Application Port Numbers,”](#) on page 1172.

For detailed Linux-specific WebAccess Application information, see [Appendix C, “Linux Commands, Directories, and Files for GroupWise Administration,”](#) on page 1179.

For additional assistance in managing the WebAccess Application, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

60 Accessing Your GroupWise Mailbox in a Web-Based Environment

GroupWise WebAccess consists of the WebAccess Application, which is installed to your Web server, and the WebAccess user interface, where users work in their GroupWise mailboxes. WebAccess offers three different Web-based environments for users. All three environments are made available when you install the WebAccess Application.

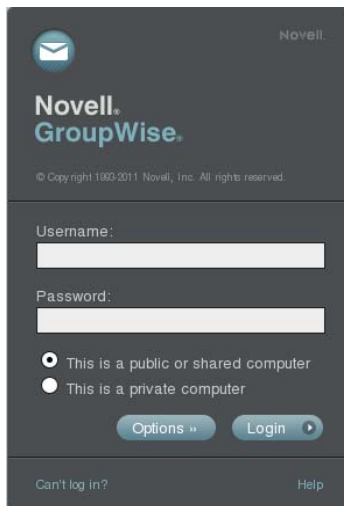
- [Section 60.1, “Using WebAccess on a Desktop Workstation,” on page 895](#)
- [Section 60.2, “Using WebAccess on a Tablet Device,” on page 896](#)
- [Section 60.3, “Using the WebAccess Basic Interface on a Mobile Device,” on page 897](#)

60.1 Using WebAccess on a Desktop Workstation

- 1 To access GroupWise WebAccess in a desktop browser, use the following URL:

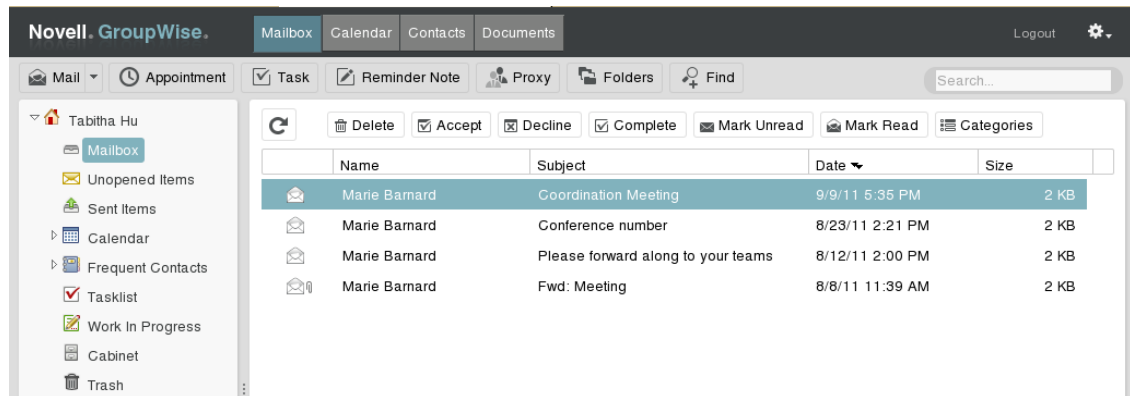
`http://web_server_address/gw/webacc`

Replace *web_server_address* with the IP address or DNS hostname of your Web server. If the Web server uses SSL, use `https` rather than `http`.

The image shows a screenshot of the Novell GroupWise WebAccess login page. At the top left is a blue envelope icon, and at the top right is the word "Novell.". Below this is the "Novell. GroupWise." logo. Underneath the logo is a small copyright notice: "© Copyright 1993-2011 Novell, Inc. All rights reserved.". The main part of the page contains a "Username:" label followed by a text input field, and a "Password:" label followed by a password input field. Below the password field are two radio buttons: the first is selected and labeled "This is a public or shared computer", and the second is labeled "This is a private computer". At the bottom of the form are two buttons: "Options" with a left-pointing arrow and "Login" with a right-pointing arrow. At the very bottom of the page are two links: "Can't log in?" on the left and "Help" on the right.

- 2 Type your GroupWise user ID in the *Username* box and your GroupWise mailbox password in the *Password* box.

- 3 (Optional) If you are in a secure location, select *This is a private computer*.
On a private computer in a secure location, the default WebAccess timeout is 480 minutes (8 hours), which is convenient for day-long use. On a public or shared computer, the default timeout is 20 minutes, which protects your personal data. You can change these settings, as described in [Section 62.2.1, “Setting the Timeout Interval for Inactive Sessions,” on page 907](#).
- 4 (Optional) To change the WebAccess interface language, click Options, then select the language you want from the *Language* drop-down list.
- 5 Click *Login* to display the GroupWise WebAccess main window.



- 6 Click *Help* for more information about using GroupWise WebAccess.

60.2 Using WebAccess on a Tablet Device

- 1 To access GroupWise WebAccess on your Apple iPad, use the following URL:

`http://web_server_address/gw/webacc`

Replace *web_server_address* with the IP address or DNS hostname of your Web server. If the Web server uses SSL, use `https` rather than `http`. The WebAccess Application detects that it is communicating with a tablet device and provides the WebAccess Mobile interface.

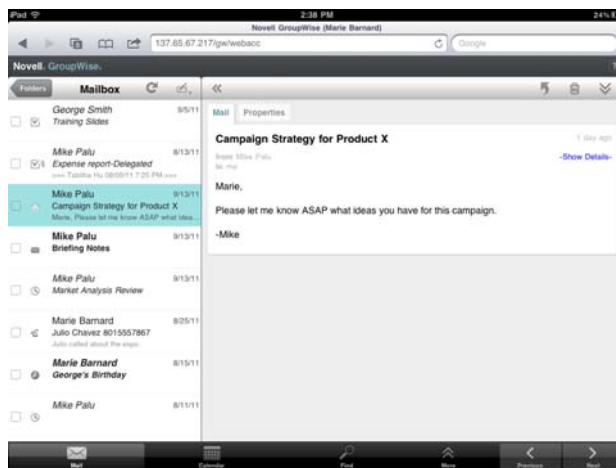


or

(Conditional) If you have a tablet device that is not yet [supported](#), but you want to see how well the mobile interface works on your device, use the following URL:

`http://web_server_address/gw/webacc?User.interface=mobile`

- 2 Type your GroupWise user ID in the *Username* box and your GroupWise mailbox password in the *Password* box.
- 3 (Optional) To change the WebAccess interface language, click *Settings*, then select the language you want from the *Language* drop-down list.
- 4 Click *Login* to display the GroupWise WebAccess main window on your iPad.



- 5 Click *More > Help* for more information about using GroupWise WebAccess on your iPad.

60.3 Using the WebAccess Basic Interface on a Mobile Device

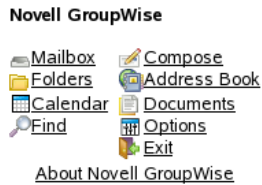
- 1 To access GroupWise WebAccess in the Web browser on your mobile device such as a cell phone, use the following URL:

`http://web_server_address/gw/webacc`

Replace *web_server_address* with the IP address or DNS hostname of your Web server. If the Web server uses SSL, use `https` rather than `http`. The WebAccess Application detects that it is communicating with a mobile device such as a cell phone and provides the WebAccess basic interface.

- 2 Enter your GroupWise user ID and GroupWise mailbox ID.

The appearance of the WebAccess basic interface varies, depending on the size of the screen where it is displayed.



- 3 For more information about using WebAccess on your mobile device, see the [WebAccess Basic Interface Quick Start](http://www.novell.com/documentation/groupwise2012/pdfdoc/gw2012_qs_webaccbasic/gw2012_qs_webaccbasic.pdf) (http://www.novell.com/documentation/groupwise2012/pdfdoc/gw2012_qs_webaccbasic/gw2012_qs_webaccbasic.pdf).
- 4 Follow the instructions in your mobile device's documentation to add this URL to your Favorites or Bookmarks so you don't need to type the URL every time you log in on your mobile device.

As an alternative to this limited interface, you can synchronize GroupWise data to your mobile device using the Novell Data Synchronizer Mobility Pack. For more information, see the [Novell Data Synchronizer Documentation Web site](http://www.novell.com/documentation/datasynchronizer1) (<http://www.novell.com/documentation/datasynchronizer1>).

61 Scaling Your GroupWise WebAccess Installation

If your GroupWise system is relatively small (one domain and a few post offices) and all post offices reside in the same location, installing the GroupWise WebAccess Application on one Web server might meet your needs. However, if your GroupWise system is large, spans multiple locations, or requires failover support, you might need to install the WebAccess Application on multiple Web servers to meet the reliability, performance, and availability needs of your GroupWise WebAccess users.

The following sections provide information about the various configurations you can implement and instructions to help you create the configuration you choose:

- ◆ [Section 61.1, “WebAccess Configurations,” on page 899](#)
- ◆ [Section 61.2, “WebAccess Installation on Additional Web Servers,” on page 901](#)

For information about installing the initial instance of the WebAccess Application, see [“Installing GroupWise WebAccess”](#) in the *GroupWise 2012 Installation Guide*.

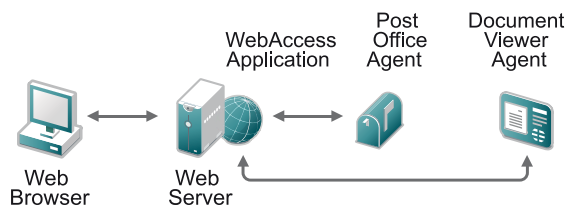
61.1 WebAccess Configurations

Depending on the needs of your GroupWise system, it might be necessary for you to have multiple Web servers running the WebAccess Application.

- ◆ [Section 61.1.1, “Basic WebAccess Application Installation,” on page 899](#)
- ◆ [Section 61.1.2, “Multiple POAs for a WebAccess Application,” on page 900](#)
- ◆ [Section 61.1.3, “Multiple DVAs for a WebAccess Application,” on page 900](#)
- ◆ [Section 61.1.4, “Multiple WebAccess Applications and Web Servers for a Large WebAccess Installation,” on page 900](#)

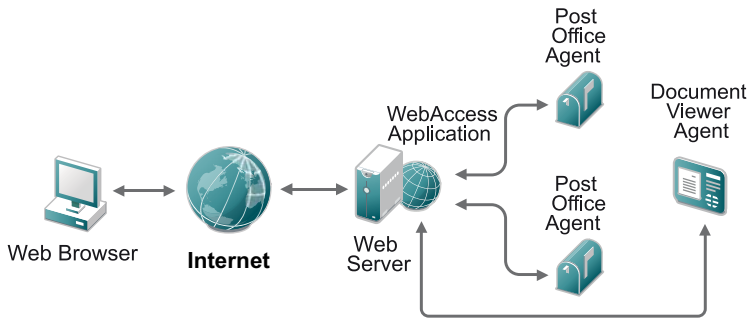
61.1.1 Basic WebAccess Application Installation

A basic installation of GroupWise WebAccess requires the WebAccess Application, a POA, and a DVA, as shown in the following diagram.



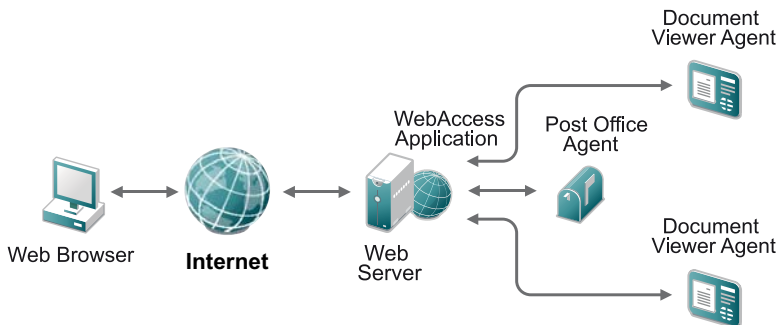
61.1.2 Multiple POAs for a WebAccess Application

When you install the WebAccess Application, you configure it to communicate with a single POA. However, in this simple configuration, if that POA goes down, WebAccess users cannot access their mailboxes, even if all other the POAs in your GroupWise system are still running. Configuring the WebAccess Application for multiple POAs provides more stable access. Three POAs are recommended, but there is no limit to the number of POAs that you can configure the WebAccess Application to communicate with. When a POA stops responding, the WebAccess Application contacts the next POA in the list to provide uninterrupted access (except, of course, for the users whose mailboxes are in the post office where the POA is down).



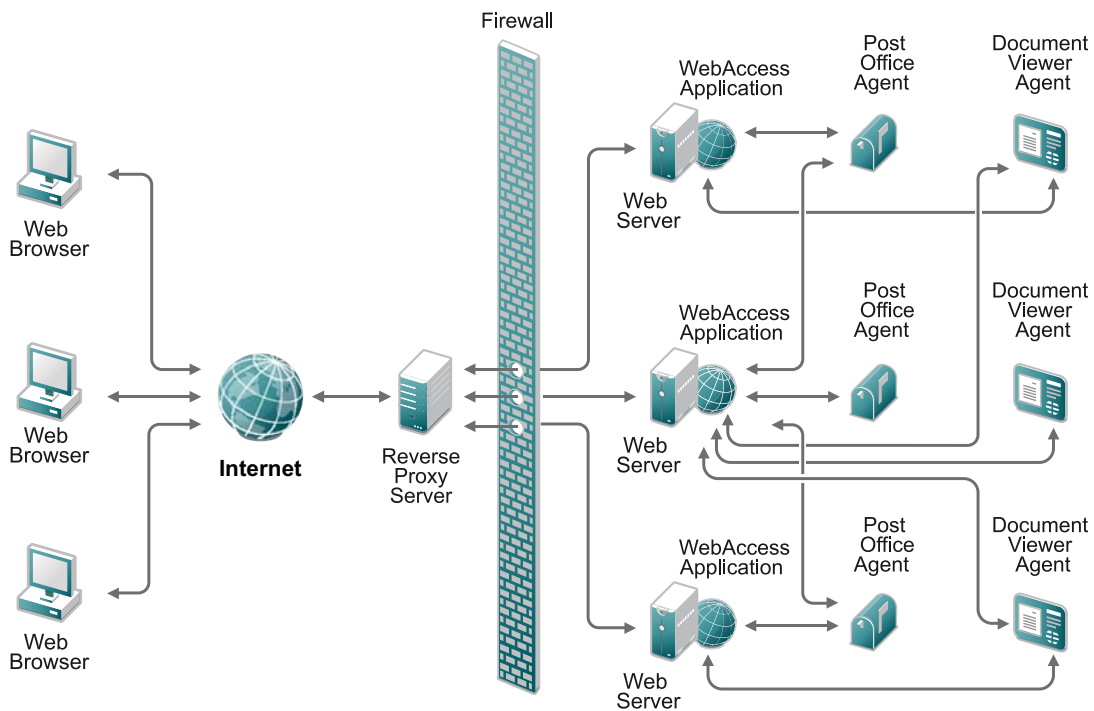
61.1.3 Multiple DVAs for a WebAccess Application

When you install the WebAccess Application, you configure it to communicate with a single DVA. Again, in this simple configuration, if that DVA goes down, no WebAccess users can view attached documents until that DVA is running again. Configuring the WebAccess Application for multiple DVAs provides more reliable document conversion. Three DVAs are recommended, but there is no limit to the number of DVAs that you can configure the WebAccess Application to communicate with. When a DVA stops responding, the WebAccess Application contacts the next DVA in the list to provide uninterrupted document conversion.



61.1.4 Multiple WebAccess Applications and Web Servers for a Large WebAccess Installation

In a larger GroupWise system, you can install the WebAccess Application to multiple Web servers.



There are various reasons why you might want to add additional WebAccess Applications, including:

- ♦ **Improving WebAccess reliability:** One WebAccess Application might provide sufficient access and performance, but you want to protect against downtime that would occur if the WebAccess Application became unavailable because of Web server failure or some other reason. Installing more than one WebAccess Application enables you to set up failover support to make your system more reliable.
- ♦ **Improving WebAccess performance:** The WebAccess Application is designed to be close to GroupWise post offices. It requires SOAP access to the POAs. For best performance, you should ensure that the WebAccess Application is on the same local area network as the POA that it communicates with. For example, in most cases you do not want a WebAccess Application in Los Angeles communicating with a POA in London.
- ♦ **Improving WebAccess availability:** Adding additional WebAccess Applications enables GroupWise WebAccess users on an intranet to access GroupWise through an internal Web server and WebAccess users on the Internet to access GroupWise through an exposed Web server.
- ♦ **Improving Web server performance:** Adding additional WebAccess Applications increases Web server performance by balancing the workload among several Web servers, especially if you are using the Web server for other purposes in addition to GroupWise WebAccess.

61.2 WebAccess Installation on Additional Web Servers

On each Web server where you want to install the WebAccess Application, follow the instructions in [“Installing GroupWise WebAccess”](#) in the *GroupWise 2012 Installation Guide*.

When you have multiple WebAccess Applications for your GroupWise system, you must select one Web server to have a friendly hostname such as `gmail.yourcompanyname.com` that users can type in their Web browsers. Then you set up a DNS redirection so that `gmail.yourcompanyname.com`

automatically redirects to `https://gwmial.yourcompanyname.com/gw/webacc`. The WebAccess Application on that main Web server communicates with a POA, which then redirects the WebAccess user to the proper post office and POA for mailbox access.

62 Configuring the WebAccess Application

For WebAccess system requirements, see “[WebAccess System Requirements](#)” in the *GroupWise 2012 Installation Guide*. For detailed instructions about installing and setting up the WebAccess Application for the first time, see “[Installing GroupWise WebAccess](#)” in the *GroupWise 2012 Installation Guide*.

The default configuration of WebAccess is adequate for users to start accessing their GroupWise mailboxes from Web browsers. You can customize the WebAccess configuration to meet the specific needs of you and your GroupWise users by editing the `webacc.cfg` file.

- ◆ [Section 62.1, “Customizing the WebAccess Application,” on page 903](#)
 - [Configuring Multiple POAs for the WebAccess Application](#)
 - [Configuring Multiple DVAs for the WebAccess Application](#)
 - [Adjusting Session Security](#)
 - [Accommodating Single Sign-On Products](#)
- ◆ [Section 62.2, “Managing User Access,” on page 907](#)
 - [Setting the Timeout Interval for Inactive Sessions](#)
 - [Customizing Auto-Save Functionality](#)
 - [Preventing Users from Changing Their GroupWise Passwords in WebAccess](#)
 - [Helping Users Who Forget Their GroupWise Passwords](#)
 - [Controlling WebAccess Usage](#)
- ◆ [Section 62.3, “Customizing User Functionality,” on page 911](#)
 - [Customizing the WebAccess User Interface with Your Company Logo](#)
 - [Controlling Viewable Attachment Types](#)
 - [Controlling Viewable Attachment Size](#)
 - [Customizing the Default Calendar View](#)
 - [Customizing the Default List Functionality](#)
 - [Enabling an LDAP Address Book](#)

62.1 Customizing the WebAccess Application

The WebAccess Application, which resides on the Web server, provides the GroupWise WebAccess user interface. As users perform actions in GroupWise WebAccess, the WebAccess Application passes information between the Web browser, the POA, and the DVA.

During installation, the WebAccess Application is set up with a default configuration in the `webacc.cfg` file. You can modify the WebAccess Application configuration to meet the needs of your WebAccess users and your administrator preferences.

- ◆ [Section 62.1.1, “Editing the webacc.cfg File,” on page 904](#)
- ◆ [Section 62.1.2, “Configuring Multiple POAs for the WebAccess Application,” on page 904](#)
- ◆ [Section 62.1.3, “Configuring Multiple DVAs for the WebAccess Application,” on page 905](#)
- ◆ [Section 62.1.4, “Adjusting Session Security,” on page 905](#)

- ♦ [Section 62.1.5, “Accommodating Single Sign-On Products,”](#) on page 906
- ♦ [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,”](#) on page 906

62.1.1 Editing the webacc.cfg File

The location of the `webacc.cfg` file varies by platform:

Linux: `/var/opt/novell/groupwise/webaccess`

Windows: `c:\Novell\GroupWise\webaccess`

You can use any ASCII text edit that you prefer to edit the `webacc.cfg` file.

IMPORTANT: We strongly recommend that you do not modify any settings that are not documented in the following sections.

62.1.2 Configuring Multiple POAs for the WebAccess Application

When you install the WebAccess Application, you configure it to communicate with a single POA. After installation, you can configure the WebAccess Application to communicate with multiple POAs. There is no limit to the number of POAs you can specify. Three POAs is recommended. The POAs you specify must be configured for SOAP.

If the POA that the WebAccess Application is communicating with becomes unavailable, the WebAccess Application contacts the next POA in the list, providing uninterrupted service for WebAccess users.

To specify additional POAs:

- 1 Open the `webacc.cfg` file in a text editor.
- 2 Search to find the following lines:

```
Provider.SOAP.1.ip=  
Provider.SOAP.1.port=
```

These lines identify the POA that you specified during installation.

- 3 Copy and paste those two lines, replace 1 with 2, then specify the IP address and SOAP port of a another POA, for example:

```
Provider.SOAP.2.ip=172.16.5.18  
Provider.SOAP.2.port=7191
```

- 4 Repeat [Step 3](#), incrementing the number, and providing the IP addresses and SOAP ports for additional POAs as needed.
- 5 Save the `webacc.cfg` file.
- 6 Skip to [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,”](#) on page 906.

62.1.3 Configuring Multiple DVAs for the WebAccess Application

When you install the WebAccess Application, you configure it to communicate with a single DVA. After installation, you can configure the WebAccess Application to communicate with multiple DVAs. There is no limit to the number of DVAs you can specify. Three DVAs is recommended.

If the DVA that the WebAccess Application is communicating with becomes unavailable, the WebAccess Application contacts the next DVA in the list, providing uninterrupted document conversion for viewing attachments in HTML format.

To specify additional POAs:

- 1 Open the [webacc.cfg file](#) in a text editor.
- 2 Search to find the following lines:

```
Provider.DVA.1.ip=  
Provider.DVA.1.port=
```

These lines identify the DVA that you specified during installation.

- 3 Copy and paste those two lines, replace 1 with 2, then specify the IP address and SOAP port of a another DVA, for example:

```
Provider.DVA.2.ip=172.17.5.18  
Provider.DVA.2.port=8301
```

- 4 Repeat [Step 3](#), incrementing the number, and providing the IP addresses and SOAP ports for additional DVAs as needed.
- 5 Save the `webacc.cfg` file.
- 6 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.1.4 Adjusting Session Security

By default, the WebAccess Application uses the Web browser IP address of the WebAccess user to confirm that, during the same session, it is always communicating with the same user. This is the highest form of security and works well for users on desktop workstations. However, for laptops and mobile devices that are carried to different places, possibly from one network segment to another, this level of security can cause interruptions in user sessions.

Other WebAccess Application security features, such as session cookies, provide excellent security, even without the IP address checking. If you have a large number of mobile WebAccess users, you can turn off the Web browser IP address confirmation to make WebAccess more stable for these mobile users.

To disable IP address checking:

- 1 Open the [webacc.cfg file](#) in a text editor.
- 2 Search to find the following line:

```
Security.UseClientIP.enable=
```

- 3 Change `true` to `false`.
- 4 Save the `webacc.cfg` file.
- 5 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.1.5 Accommodating Single Sign-On Products

Some organizations choose to place a single sign-on product such as [Novell Identity Manager \(IDM\)](http://www.novell.com/products/identitymanager) (<http://www.novell.com/products/identitymanager>) between users on the Web and the applications they access that are running behind the organization's firewall. If you use a single sign-on product with WebAccess, you must configure the WebAccess Application to accommodate the single sign-on product.

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the following line:

```
#Cookie.domain=.novell.com
```

- 3 Remove the pound sign (#) to activate the setting.
- 4 Replace `.novell.com` with the part of your organization's Internet domain name that is common between the single sign-on product and the Web server where the WebAccess Application is installed.

For example, if the IDM server is at `idm.novell.com` and the WebAccess Application is at `webacc.novell.com`, the domain name used to create cookies would be `.novell.com`, so that the cookies are accepted by both servers.

- 5 Save the `webacc.cfg` file.
- 6 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.1.6 Putting WebAccess Configuration Changes into Effect

- ♦ ["Accepting the Default Time Interval" on page 906](#)
- ♦ ["Changing the Default Time Interval" on page 906](#)
- ♦ ["Immediately Putting the Configuration Changes into Effect" on page 907](#)

Accepting the Default Time Interval

By default, the WebAccess Application checks the `webacc.cfg` file and the `gwac.xml` file for changes every 10 minutes. When it finds changes, it puts the changes into effect without restarting Tomcat. If you are satisfied with having your changes put into effect within this time interval, no action is required on your part after you edit the `webacc.cfg` file or the `gwac.xml` file.

Changing the Default Time Interval

You can change the time interval at which the WebAccess Application checks the `webacc.cfg` file and the `gwac.xml` file for changes.

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the following line:

```
Config.Update.check=10
```

- 3 Change 10 to the number of minutes you want the WebAccess Application to wait before checking for changes to its configuration file.
- 4 Save the `webacc.cfg` file.

Immediately Putting the Configuration Changes into Effect

You can also manually restart Tomcat in order to put the changes into effect immediately.

OES 11: `rcnovell-tomcat6 stop`
 `rcnovell-tomcat6 start`

OES 2 Linux: `rcnovell-tomcat5 stop`
 `rcnovell-tomcat5 start`

SLES 11: `rctomcat6 stop`
 `rctomcat6 start`

SLES 10: `rctomcat5 stop`
 `rctomcat5 start`

Windows: 1. At the Windows server, click *Start > Administrative Tools > Services*.
 2. Right-click *Tomcat 6*, then click *Restart*.

62.2 Managing User Access

You can manage various aspects of GroupWise WebAccess user sessions.

- ♦ [Section 62.2.1, “Setting the Timeout Interval for Inactive Sessions,” on page 907](#)
- ♦ [Section 62.2.2, “Customizing Auto-Save Functionality,” on page 908](#)
- ♦ [Section 62.2.3, “Preventing Users from Changing Their GroupWise Passwords in WebAccess,” on page 908](#)
- ♦ [Section 62.2.4, “Helping Users Who Forget Their GroupWise Passwords,” on page 909](#)
- ♦ [Section 62.2.5, “Controlling WebAccess Usage,” on page 909](#)

62.2.1 Setting the Timeout Interval for Inactive Sessions

Users are eventually logged out of GroupWise WebAccess if they have not performed any actions that generate requests. Actions such as opening or sending a message generate requests. Other actions, such as scrolling through the Item List, composing a mail message without sending it, and reading Help topics, do not generate requests.

The timeout interval depends on whether the user selects *This is a public or shared computer* or *This is a private computer* in the Login window. On a private computer in a secure location, the default WebAccess timeout is 480 minutes (8 hours), which is convenient for day-long use. On a public or shared computer, the default timeout is 20 minutes, which protects your personal data. The timeout interval provides security for GroupWise WebAccess users who forget to log out. It also helps the performance of the Web server by freeing the resources dedicated to that user’s connection.

The WebAccess Application on the Web server controls the timeout. At the time the user is logged out, the WebAccess Application saves the user’s current session to a directory on the Web server, where it is stored for 24 hours. If the logged-out user attempts to continue the session, he or she is prompted to log in again, after which the WebAccess Application renews the session. For example, suppose a user is composing a message when the timeout interval expires and then attempts to send the message. The user is prompted to log in again, after which the message is sent. No information is lost.

To adjust the timeout interval:

- 1 Open the [webacc.cfg](#) file in a text editor.

- 2 To change the timeout interval for use on a public or shared computer, search to find the following line:

```
Security.timeout=20
```

- 3 Change the default of 20 to the number of minutes that you prefer for the public/shared timeout interval.
- 4 To change the timeout interval for use on a private computer, search to find the following line:

```
Security.Private.timeout=480
```

- 5 Change the default of 480 to the number of minutes that you prefer for the private timeout interval.
- 6 Save the `webacc.cfg` file.
- 7 Skip to [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,”](#) on page 906.

The timeout interval applies to all users who log in through the Web server where the WebAccess Application is running. You cannot set individual user timeout intervals. However, if you have multiple Web servers, you can set different timeout intervals for the Web servers by completing the above steps for each server’s WebAccess Application.

62.2.2 Customizing Auto-Save Functionality

By default, GroupWise WebAccess automatically saves users’ work on a regular basis, so that if a problem with a Web server occurs or the user times out, their work is not lost. For details about the Auto-Save feature, see [“Saving Unfinished Email”](#) in [“Email”](#) in the *GroupWise 2012 WebAccess User Guide*.

Increasing the settings so that users’ work is saved less frequently reduces the load on the Web server but increases the amount of work that users could potentially lose. Reducing the settings so that users’ work is saved more frequently increases the load on the Web server, but reduces the amount of work that users could potentially lose.

To adjust the Auto-Save intervals:

- 1 Open the `webacc.cfg` file in a text editor.
- 2 Search to find the Auto Save section.
- 3 For the `Autosave.NonUse.timer` setting, increase or decrease the number of seconds after which the content is saved if there have been no modifications since the last save.
The default non-use interval is 10 seconds. Specify 0 (zero) to turn off this functionality.
- 4 For the `Autosave.Use.timer` setting, increase or decrease the number of seconds after which the content is saved even when users are actively composing content.
The default is 60 seconds. Specify 0 (zero) to turn off this functionality.
- 5 Save the `webacc.cfg` file.
- 6 Skip to [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,”](#) on page 906.

62.2.3 Preventing Users from Changing Their GroupWise Passwords in WebAccess

By default, users are allowed to change their GroupWise passwords in WebAccess. You can prevent them from doing so if you prefer that users change their passwords in some other way, for example if you are using an LDAP directory for authentication.

To adjust password security:

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the following line:

```
User.Access.security
```
- 3 Change `true` to `false`.
- 4 Save the `webacc.cfg` file.
- 5 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.2.4 Helping Users Who Forget Their GroupWise Passwords

The GroupWise WebAccess Login page provides a *Can't log in* link for users to click when they have forgotten their GroupWise passwords. By default, the link displays the following file:

```
/var/opt/novell/tomcat5/webapps/gw/webaccess/yyyymddnnnn/images/helpdesk.htm
```

The variable `yyyymddnnnn` represents the year, month, day, and build number of the WebAccess software that you have installed.

You can use your HTML editor of choice to customize the contents of this file. For example, you might want to include the email address of the local GroupWise administrator who handles password issues, or perhaps the URL of your company's Help Desk Web page.

As an alternative, you can configure the WebAccess Application to display any URL of your choosing.

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the following line:

```
#Helpdesk.url=http://www.novell.com/helpdesk.html
```
- 3 Remove the pound sign (`#`) to activate the setting.
- 4 Replace the sample URL with wherever you want users to be directed when they have forgotten their GroupWise passwords.
- 5 Save the `webacc.cfg` file.
- 6 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.2.5 Controlling WebAccess Usage

You can control which users can use WebAccess to access their GroupWise mailboxes. By default, all GroupWise users can use WebAccess.

You can control access based on the domain or post office where the user's mailbox is located. You can control access for groups of users based on distribution lists, and you can control access for individual users.

Access control is established through the `gwac.xml` file, located in the same directory with the `webacc.cfg` file.

The default `gwac.xml` file illustrates the following options:

```
<!-- To allow access to all EXCEPT a few, use this technique. -->
<!--
<gwac access="prevent">
  <domain name="domain1" />
  <postOffice name="po2.domain2" />
  <user name="jdoe.po3.domain3" />
  <distributionList name="helpdesk.po4.domain4" />
  <resource name="confroom.po4.domain4" />
</gwac>
-->

<!-- To prevent access to all EXCEPT a few, use this technique -->
<!--
<gwac access="allow">
  <domain name="domain1" />
  <postOffice name="po2.domain2" />
  <user name="jdoe.po3.domain3" />
  <distributionList name="helpdesk.po4.domain4" />
  <resource name="confroom.po4.domain4" />
</gwac>
-->
```

You can use any ASCII text editor that you prefer to edit the `gwac.xml` file.

- 1 Open the `gwac.xml` file in a text editor.

Typically, you use the `gwac.xml` file to override the default of allowing all users to use WebAccess.

- 2 (Optional) Under the `<gwac access="prevent">` line, create one or more lines to prevent users in one or more domains from using WebAccess, for example:

```
<domain name="provo5"/>
<domain name="provo6"/>
```

- 3 (Optional) Create one or more lines to prevent users in one or more post offices from using WebAccess, for example:

```
<postOffice name="interns.provo1"/>
<postOffice name="temps.provo1"/>
```

Specify the post office in `post_office.domain` format.

- 4 (Optional) Create one or more lines to prevent users in one or more distribution lists from using WebAccess, for example:

```
<distributionList name="webaccessdenied.admin.provo1"/>
```

Specify the distribution list in `distribution_list.post_office.domain` format.

Using one or more distribution lists is the most flexible approach to access control for WebAccess. The distribution list belongs to a specific post office (for example, the one you belong to), but it can include GroupWise users located anywhere in your GroupWise system. By using a distribution list, you can easily modify access control for specific users by modifying the distribution list in ConsoleOne, rather than needed to modify the `gwac.xml` file whenever access control changes are needed. For more information about distribution lists, see [Chapter 18, "Creating and Managing Distribution Lists,"](#) on page 285.

- 5 (Optional) Create one or more lines to prevent specific users from using WebAccess, for example:

```
<user name="sjones.interns.provo1"/>
<user name="gbock.interns.provo1"/>
```

- 6 (Conditional) If you want to prevent most users and allow only specified users, use a `<gwac access="allow">` line instead of a `<gwac access="prevent">` line.
- 7 Save the `gwac.xml` file.
- 8 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.3 Customizing User Functionality

You can control the functionality of certain aspects of the GroupWise WebAccess user interface. Any changes you make take effect the next time users log in to WebAccess.

- ♦ [Section 62.3.1, "Customizing the WebAccess User Interface with Your Company Logo,"](#) on page 911
- ♦ [Section 62.3.2, "Controlling Viewable Attachment Types,"](#) on page 912
- ♦ [Section 62.3.3, "Controlling Viewable Attachment Size,"](#) on page 913
- ♦ [Section 62.3.4, "Customizing the Default Calendar View,"](#) on page 913
- ♦ [Section 62.3.5, "Customizing the Default List Functionality,"](#) on page 915
- ♦ [Section 62.3.6, "Enabling an LDAP Address Book,"](#) on page 916

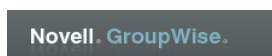
62.3.1 Customizing the WebAccess User Interface with Your Company Logo

You can customize the WebAccess user interface to display your company logo. In the WebAccess Login window, you can replace the GroupWise envelope icon and the words "Novell GroupWise" in the upper left corner. In the main WebAccess window, you can replace the words "Novell GroupWise" in the menu bar.

The logo size for the WebAccess Login window must not exceed 215 pixels in width by 120 pixels in height.



The logo size for the upper left corner of the main WebAccess window must not exceed 220 pixels in width by 40 pixels in height.



Interface customizations are established through the [customization.cfg](#) file, which is located in the same directory as the [webacc.cfg](#) file.

- 1 Make sure that you have company logo images that approximately match the size and shape of the Novell logos that you are replacing.
- 2 Copy the logo image files to a location on your Web server where they can be displayed by specifying a URL.
The logo image files must reside on the same server with the WebAccess Application that you are configuring. You can put them in a subdirectory under your Web server's document root directory.
- 3 Open the [customization.cfg](#) file in a text editor.
- 4 Specify the logo image to use in the WebAccess Login window:
 - 4a Uncomment the following line:

```
Company.Logo.Login.src=
```
 - 4b Replace the sample URL with the URL for the company logo file for the Login window.
 - 4c Replace the sample mouse-over text with the mouse-over text for your company logo.
- 5 Specify the logo image to use in the main WebAccess window:
 - 5a Uncomment the following line:

```
Company.Logo.Caption.src=
```
 - 5b Replace the sample URL with the URL for the company logo file for the main WebAccess window.
 - 5c Replace the sample mouse-over text with the mouse-over text for your company logo.
- 6 Save the [customization.cfg](#) file.
- 7 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.3.2 Controlling Viewable Attachment Types

By default, WebAccess allows users to view attachments in their native file formats for all file extensions except `.rar` (Roshall Archive, a compressed archive format) and `.avi` (Audio Visual Interleaf format). For all other file types, the *View* link is available in WebAccess. You can configure the WebAccess Application so that the *View* link is not available for additional file types.

To add to the list of file types that WebAccess users cannot view in native file format:

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the following line:

```
Document.View.excludeDocExtensions=
```
- 3 Add file extensions to the list, separating each file extension with a comma.
Do not include periods on the file extensions or spaces between the file extensions.
- 4 Save the [webacc.cfg](#) file.
- 5 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.3.3 Controlling Viewable Attachment Size

By default, users can view allowable attachment types that are less than 1 MB in size. Increasing the maximum viewable attachment size increases the load on the Web server. Decreasing the maximum viewable attachment size decreases the load on the Web server.

For allowable attachment types that do not exceed the size limit, the *View* link is available in WebAccess. For allowable attachment types that exceed the size limit, the *View* link is not available, and users must save the large attachments in order to view them.

To adjust the viewable attachment size limit:

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the following line:

```
Document.View.maxSize=
```
- 3 Increase or decrease the size as needed.
Specify the size in bytes. For example, 1024000 is 1 MB.
- 4 Save the `webacc.cfg` file.
- 5 Skip to [Section 62.1.6, "Putting WebAccess Configuration Changes into Effect,"](#) on page 906.

62.3.4 Customizing the Default Calendar View

By default, WebAccess displays the Week view of the calendar:

The screenshot shows the Novell GroupWise web interface. At the top, there are navigation tabs for Mailbox, Calendar, Contacts, and Documents. Below these are various icons for Mail, Appointment, Task, Reminder Note, Proxy, and Find. The main area is divided into three sections: Calendars, a central calendar grid, and Notes/Tasks. The Calendars section on the left has checkboxes for 'Calendar' and 'Personal'. The central calendar grid shows the week of October 23-29, 2011, with the 27th highlighted. The time slots range from 8:00 AM to 5:00 PM. The Notes and Tasks sections on the right are currently empty.

You can change the default to the Day view.

Novell GroupWise. Mailbox Calendar Contacts Documents Logout

Mail Appointment Task Reminder Note Proxy Find

Today [1] [7] [31] Print View

Calendars

- Calendar
- Personal

October 2011

Thursday 27

8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
2:00 PM
3:00 PM
4:00 PM
5:00 PM

Notes

Add a note

Tasks

Add a task

Oct 2011

S	M	T	W	T	F	S
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Or you can change the default to the month view.

Novell GroupWise. Mailbox Calendar Contacts Documents Logout

Mail Appointment Task Reminder Note Proxy Find

Today [1] [7] [31] Print View

Calendars

- Calendar
- Personal

October 2011

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Oct 2011

Jan	Feb	Mar
Apr	May	Jun
Jul	Aug	Sep
Oct	Nov	Dec

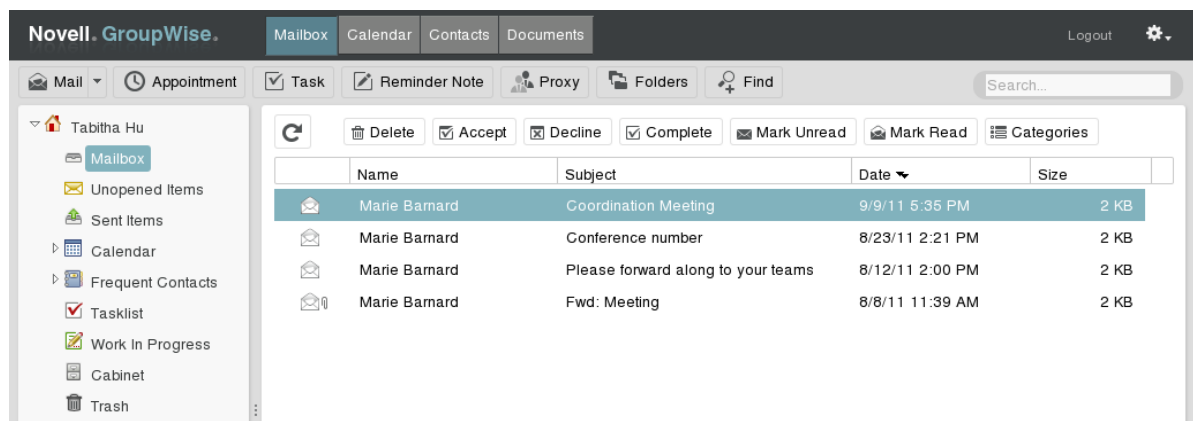
The default you select affects how the Calendar displays for GroupWise users to access their mailboxes through this instance of the WebAccess Application.

To change the default Calendar view:

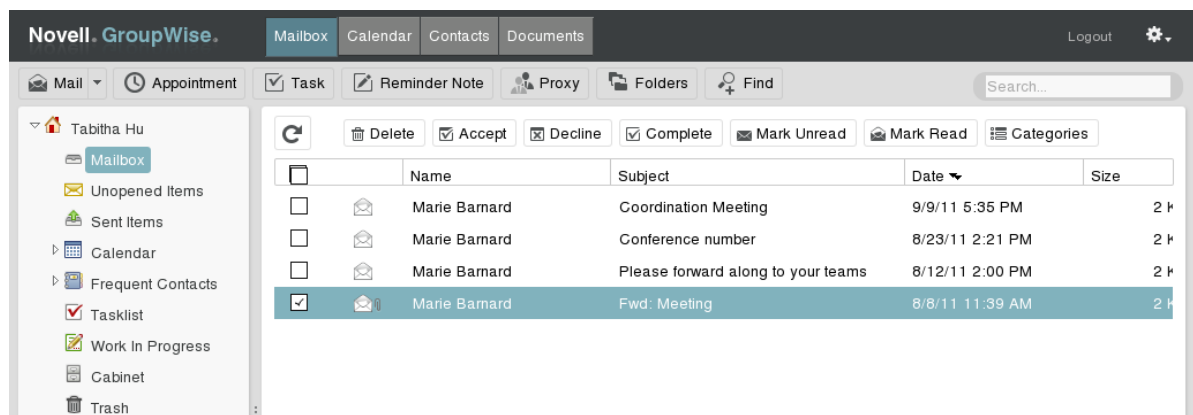
- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the following line:
`User.Calendar.defaultView=`
- 3 Change Week to Day or Month.
- 4 Save the `webacc.cfg` file.
- 5 Skip to [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,”](#) on page 906.

62.3.5 Customizing the Default List Functionality

By default, in lists of items, contacts, and Find results, GroupWise WebAccess users can Shift+click and Ctrl+click to select multiple items to perform an action on.



Some Web-based interfaces use check boxes for multiple selection. This interface option is also available for GroupWise WebAccess.



To configure WebAccess to display check boxes:

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the following line:


```
List.Checkboxes.show=
```

- 3 Change `false` to `true`.
- 4 Save the `webacc.cfg` file.
- 5 Skip to [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,”](#) on page 906.

62.3.6 Enabling an LDAP Address Book

You can configure WebAccess to access an LDAP directory as if it is a GroupWise address book.

- 1 Open the `webacc.cfg` file in a text editor.
- 2 Search to find the following line:

```
User.Access.LDAP=false
```
- 3 Change `false` to `true` to enable users to access an LDAP address book.
- 4 Save the `webacc.cfg` file.
- 5 Open the `ldap.cfg` file in a text editor.
- 6 Replace the sample information in the `ldap.cfg` file with the specific information for the LDAP directory that you want users to access as a GroupWise address book.
- 7 Save the `ldap.cfg` file.
- 8 Follow the instructions in [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,”](#) on page 906.
- 9 Verify that the LDAP directory is available as a GroupWise address book:
 - 9a In WebAccess, open a new item.
 - 9b Click *Address*, then click the *Plus* icon .
 - 9c Expand the list of address books, then select the LDAP address book.
- 10 (Conditional) If the LDAP address book does not appear in the list:
 - 10a Check your modifications to the `webacc.cfg` file and `ldap.cfg` file for errors.
 - 10b Check the WebAccess Application log file for error messages.

For assistance, see [Section 63.2, “Using WebAccess Application Log Files,”](#) on page 918.
 - 10c Resolve the problem, so that the LDAP address book appears in the list of address books.
- 11 Verify that the LDAP address book works as expected:
 - 11a Send a message to a recipient in the LDAP address book.
 - 11b Verify that the message was delivered successfully.
- 12 Notify GroupWise users that the LDAP address book is available, and explain to them how to access it.

The LDAP address book is available only in the Address Selector and only in WebAccess. It is not available in the GroupWise client.

63 Monitoring the WebAccess Application

The WebAccess Application can be monitored in your Web browser. You can also use log files to monitor the WebAccess Application.

- ♦ [Section 63.1, “Using the WebAccess Application Web Console,” on page 917](#)
- ♦ [Section 63.2, “Using WebAccess Application Log Files,” on page 918](#)

63.1 Using the WebAccess Application Web Console

The WebAccess Application includes a Web console that you can use to monitor it. The Web console lets you see information about logged-in users, such as their IP address, their GroupWise and Web browser versions. In addition, you can view the WebAccess Application’s log files and configuration files. The WebAccess Application Web console is enabled by default.

63.1.1 Enabling the WebAccess Application Web Console

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the Application Administration Tool section.
- 3 For the `Admin.WebConsole.enable` setting, change `false` to `true`.
- 4 For the `Admin.WebConsole.username` setting, specify the user name for accessing the WebAccess Application Web console.
- 5 For the `Admin.WebConsole.password` setting, specify the password for accessing the WebAccess Application Web console.
- 6 Save the `webacc.cfg` file.
- 7 Skip to [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,” on page 906](#).

63.1.2 Using the WebAccess Application Web Console

- 1 In a Web browser, enter the following URL:

```
http://server_address/gw/webacc?action=Admin.Open
```

Replace `server_address` with the Web server’s IP address or DNS hostname.

- 2 When prompted, enter the user name and password.

The Web console is displayed.

Novell GroupWise WebAccess Application							Monday - December 5, 2011 20:09
Status Configuration Log Files Refresh Help							
Up Time: 0 Days 5 Hours 58 Minutes							
User Information - 1 Active User(s)							
User Id	Logged In	Last Access	Interface	Domain	Post Office	Language	Client IP
mpalu@yourcompanyname.com	12/05/11 20:09	12/05/11 20:09	css	Provo1	Development	en	172.15.7.17
Total Active Users: 1							

63.2 Using WebAccess Application Log Files

Error messages and other information about WebAccess Application functioning are written to log files as well as displaying on the WebAccess Application server console (Windows only). Log files can provide a wealth of information for resolving problems with WebAccess Application functioning or message flow. Logging is enabled by default.

- ♦ [Section 63.2.1, “Locating WebAccess Application Log Files,” on page 918](#)
- ♦ [Section 63.2.2, “Configuring WebAccess Application Log Settings,” on page 918](#)
- ♦ [Section 63.2.3, “Viewing WebAccess Application Log Files,” on page 919](#)
- ♦ [Section 63.2.4, “Interpreting WebAccess Application Log File Information,” on page 919](#)

63.2.1 Locating WebAccess Application Log Files

By default, WebAccess Application log files (*mmdwas.nnn*) are located in the [GroupWise Web application working directory](#).

You can change the location where the WebAccess Application creates its log files, as described in [Configuring WebAccess Application Log Settings](#).

63.2.2 Configuring WebAccess Application Log Settings

- 1 Open the [webacc.cfg](#) file in a text editor.
- 2 Search to find the Logging Information section.
- 3 Adjust the following log settings as needed:

Log.maxSize: Specify the maximum amount of disk space you want to use for WebAccess Application log files. If the disk space limit is exceeded, the WebAccess Application deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 102400 KB (100 MB).

Log.maxAge: Specify the number of days you want to retain the log files. The WebAccess Application retains log files for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 30 days.

Log.level: There are three log levels:

- ♦ **Normal (default)** Displays warnings and errors.
- ♦ **Verbose:** Displays the Normal log level information, plus information messages and user requests.

- ♦ **Diagnostic:** Displays all possible information. Use Diagnostic only if you are troubleshooting a problem with the WebAccess Application.

The Verbose and Diagnostic log levels do not degrade WebAccess Application performance, but log files consume more disk space when Verbose or Diagnostic logging is in use.

Log.path: Specify the file path where you would like the log files to be stored. For example:

```
Log.path=C:/User/jdoe/logs
```

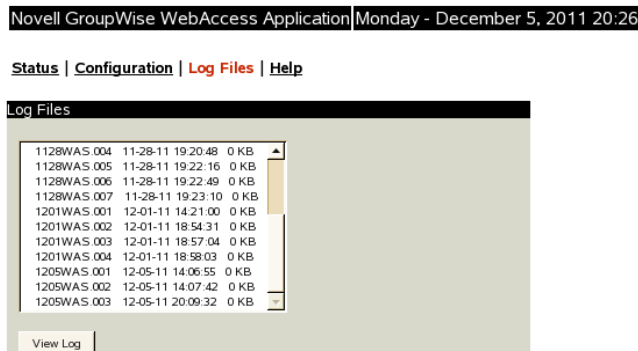
- 4 Save the webacc.cfg file.
- 5 Skip to [Section 62.1.6, “Putting WebAccess Configuration Changes into Effect,”](#) on page 906.

63.2.3 Viewing WebAccess Application Log Files

For the default location of the WebAccess Application log files, see [Section 63.2.1, “Locating WebAccess Application Log Files,”](#) on page 918.

When logging is turned on, the WebAccess Application creates a new log file each day and each time it is restarted (as part of the Web server startup). Therefore, you find multiple log files in the log file directory. The first four characters represent the date (*mmdd*). The next three characters identify the WebAccess Application (*waa*). A three-digit extension allows for multiple log files created on the same day. For example, a log file named 0518waa.001 indicates that it is a WebAccess Application log file, created on May 18.

For convenience, you can view WebAccess Application log files in the [WebAccess Application Web console](#):



63.2.4 Interpreting WebAccess Application Log File Information

In its log file, the WebAccess Application records user activity in GroupWise WebAccess, along with a time stamp showing when the activity took place.

XIV Calendar Publishing Host

- ♦ [Chapter 64, “Configuring the Calendar Publishing Host,”](#) on page 923
- ♦ [Chapter 65, “Monitoring Calendar Publishing,”](#) on page 931
- ♦ [Chapter 66, “Creating a Corporate Calendar Browse List,”](#) on page 933
- ♦ [Chapter 67, “Managing Your Calendar Publishing Host,”](#) on page 935

For a complete list of port numbers used by the Calendar Publishing Host, see [Section A.8, “Calendar Publishing Host Port Numbers,”](#) on page 1172.

64 Configuring the Calendar Publishing Host

For Calendar Publishing Host system requirements, see “[Calendar Publishing Host System Requirements](#)” in the *GroupWise 2012 Installation Guide*. For detailed instructions about installing and setting up the GroupWise Calendar Publishing Host for the first time, see “[Installing the GroupWise Calendar Publishing Host](#)” in the *GroupWise 2012 Installation Guide*.

The default configuration of the Calendar Publishing Host is adequate to begin publishing calendars. As your GroupWise system grows and evolves, you might need to modify its configuration to meet the changing needs of the users it services.

- ◆ [Section 64.1, “Using the Administration Web Console,” on page 923](#)
 - [Changing Post Office Settings](#)
 - [Adjusting Log Settings](#)
 - [Configuring LDAP Authentication](#)
 - [Customizing the Calendar Publishing Host Logo](#)
- ◆ [Section 64.2, “Using the calhost.cfg File,” on page 928](#)
 - [Setting the Published Calendar Auto-Refresh Interval](#)
 - [Setting the Default Published Calendar View](#)
 - [Configuring an External POA IP Address](#)
 - [Changing the SSL Trusted Root Certificate](#)

64.1 Using the Administration Web Console

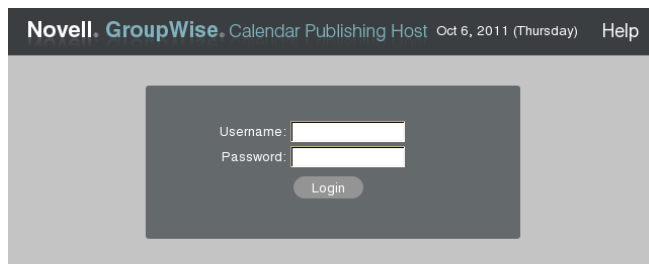
Some aspects of the Calendar Publishing Host can be configured using the Administration Web console.

- ◆ [Section 64.1.1, “Logging In to the Administration Web Console,” on page 923](#)
- ◆ [Section 64.1.2, “Changing Post Office Settings,” on page 924](#)
- ◆ [Section 64.1.3, “Adjusting Log Settings,” on page 924](#)
- ◆ [Section 64.1.4, “Configuring LDAP Authentication,” on page 926](#)
- ◆ [Section 64.1.5, “Customizing the Calendar Publishing Host Logo,” on page 927](#)
- ◆ [Section 64.1.6, “Logging Out of the Administration Web Console,” on page 927](#)

64.1.1 Logging In to the Administration Web Console

The Calendar Publishing Host Administration Web console is a browser-based administration tool that enables you to easily change the configuration of the Calendar Publishing Host.

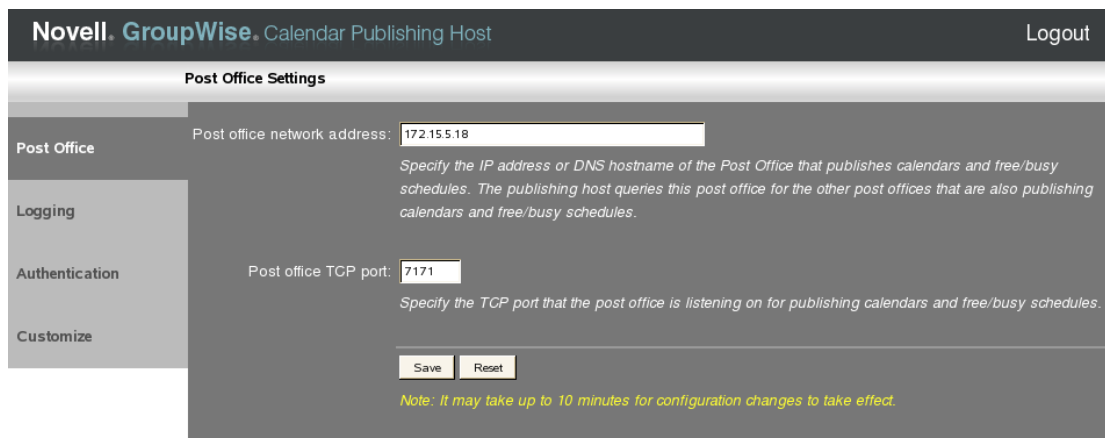
- 1 Display the Calendar Publishing Host Administration Web console login page:
`http://network_address/gwcal/admin`



- 2 Provide the administrative user and password you set up in “[Setting Up a Calendar Publishing Host](#)” in the *GroupWise 2012 Installation Guide*, then click *Login*.

64.1.2 Changing Post Office Settings

- 1 Log in to the [Calendar Publishing Host Administration Web console](#).



The Post Office page provides the information that the Calendar Publishing Host needs in order to communicate with a POA to obtain calendar and free/busy information. The initial information was provided during installation, as described in “[Configuring a POA for Calendar Publishing](#)” in “[Installing the GroupWise Calendar Publishing Host](#)” in the *GroupWise 2012 Installation Guide*.

- 2 Change the post office settings as needed.

Post office network address: Specify the IP address or DNS hostname of the POA that is configured for calendar publishing.

Post office TCP port: Specify the calendar publishing port that the POA uses to communicate with the Calendar Publishing Host.

- 3 If you make changes, click *Save*.

64.1.3 Adjusting Log Settings

- 1 Log in to the [Calendar Publishing Host Administration Web console](#), then click *Logging* to define log settings for the Calendar Publishing Host:

Novell GroupWise Calendar Publishing Host Logout

Log Settings

Post Office	Enable logging: <input checked="" type="checkbox"/> <i>Select this option to turn on logging for the Calendar Publishing Host.</i>
Logging	Log file path: <input type="text" value="\${WebApp.Config.path}/logs"/> <i>Specify the path where the Calendar Publishing Host logs messages.</i>
Authentication	Max size for log files: <input type="text" value="102400"/> <i>Specify in kilobytes the maximum size for log files. When the combined size of log files reaches this size, the oldest log files are deleted.</i>
Customize	Max Log File Age: <input type="text" value="7"/> <i>Enter the number of days for the maximum age for a log file. When the log files are this old, they are deleted</i>
	Log level: <input type="text" value="Normal"/> ▼ <i>Select the level of detail that you want recorded in the log file.</i>
	Use Tomcat log file: <input type="checkbox"/> <i>Select this option to log information to the servlet container's log file in addition to the standard log file.</i>
<input type="button" value="Save"/> <input type="button" value="Reset"/>	
<i>Note: It may take up to 10 minutes for configuration changes to take effect.</i>	

Logging is enabled by default. Default settings are provided for the rest of the fields.

2 Change the Calendar Publishing Host log settings as needed:

Enable Logging: Deselect this option to turn off Calendar Publishing Host logging.

Log File Path: The default log file location is the [GroupWise Web application working directory](#).

Change the log file settings as needed:

Max Size for Log Files: Specify in kilobytes the maximum size for log files. When the combined size of log files reaches this size the oldest log files are deleted.

Max Log File Age: Specify the number of days for the maximum age for a log file. When a log file reaches this age, it is deleted.

Log Level: Select the level of detail that you want recorded in the log file.

Use Tomcat Log File: Select this option if you want the same information logged to the Tomcat log file as is logged to the Calendar Publish Host log file. The location of the Tomcat log file varies by platform:

OES 11: [/var/opt/novell/tomcat6/logs](#)

OES 2 Linux: [/var/opt/novell/tomcat5/logs](#)

SLES 11: [/usr/share/tomcat6/logs](#)

SLES 10: [/srv/www/tomcat5/base/logs](#)

Windows: [c:\novell\tomcat6\logs](#)

3 If you make changes, click *Save*.

64.1.4 Configuring LDAP Authentication

- 1 Log in to the [Calendar Publishing Host Administration Web console](#), then click *Authentication*.

The screenshot shows the 'Administrator LDAP Authentication Settings' page in the Novell GroupWise Calendar Publishing Host Administration Web console. The page has a dark header with the Novell GroupWise logo and 'Calendar Publishing Host' text, and a 'Logout' link in the top right. A left sidebar contains navigation options: 'Post Office', 'Logging', 'Authentication', and 'Customize'. The main content area is titled 'Administrator LDAP Authentication Settings' and contains several configuration fields with text boxes and descriptive text:

- LDAP authority network address:** . Specify the IP address or DNS hostname of the LDAP server to use when authenticating Calendar Publishing Host administrators.
- LDAP context:** . Specify a formatting string to create the full LDAP context for the authenticating object. Use {0} in place of the object name. For example, a formatting string of `cn={0},o=novell` is translated to `cn=admin,o=novell` if admin is entered as the username on the login screen.
- Required LDAP attribute:** . Specify the name of the LDAP attribute that must contain the required value in order to allow administrator access.
- Required LDAP value:** . Specify the value of the required LDAP attribute that must be present in order to allow administrator access. Separate multiple choices for values with the vertical bar (|).

At the bottom of the form are 'Save' and 'Reset' buttons, and a note: *Note: It may take up to 10 minutes for configuration changes to take effect.*

The Authentication page provides the information that the Calendar Publishing Host needs in order to log into eDirectory. The Calendar Publishing Host uses LDAP authentication to log in. The initial information was provided during installation, as described in “[Setting Up Calendar Publishing Administration](#)” in “[Installing the GroupWise Calendar Publishing Host](#)” in the *GroupWise 2012 Installation Guide*.

- 2 Change the authentication information as needed:

LDAP Authority Network Address: Specify the IP address or DNS hostname of an LDAP server where users of the Calendar Publishing Host Administration Web console have accounts. Include the port number (typically 389 for non-secure connections and 636 for secure SSL connections).

LDAP Context. Specify the context in which the User objects for Calendar Publishing Host administrators are located. The variable {0} represents whatever user name is provided on the Administration Web console login page. The User object for the administrator must be located in the specified context. By providing the context here, administrators do not need to provide the context when they log in to the Administration Web console.

Required LDAP Attribute: By default, the Calendar Publishing Host checks users for membership in a specific group before it grants access to the Calendar Publishing Host Administration Web console. This default is typically appropriate.

Required LDAP Value: If you retain the default LDAP attribute of groupMembership, specify the full context of the group to which Calendar Publishing Host administrator users must belong in order to log in to the Administration Web console. If you change the default LDAP attribute, specify the required value for that attribute.

- 3 If you make changes, click *Save*.

The SSL trusted root certificate that you supplied when you installed the Calendar Publishing Host cannot be changed from the Administration Web console. If you need to change the certificate information, see [Section 64.2.5, “Changing the SSL Trusted Root Certificate,”](#) on page 929.

64.1.5 Customizing the Calendar Publishing Host Logo

- 1 Log in to the [Calendar Publishing Host Administration Web console](#), then click *Customize* to modify the appearance of the main browser page displayed by the Calendar Publishing Host.



The Customize page enables you to use a different logo, perhaps your company logo, on the main Calendar Publishing Web page.

- 2 Provided the information for your company logo:

Logo Image: Specify the full path and file name of the customized image file.

Logo Text: Specify the text to accompany the customized image.

Logo Text Position: Select *Top*, *Middle*, or *Bottom*, based on the example displayed in the box below the field.

- 3 Click *Save*.

64.1.6 Logging Out of the Administration Web Console

When you close the browser page, you are automatically logged out of the Calendar Publishing Host Web console.

The Calendar Publishing Host checks its configuration file (`calhost.cfg`) every 10 minutes. Therefore, it can take up to 10 minutes for the changes you made in the Administration Web console to take effect in the functionality of the Calendar Publishing Host.

Restarting Tomcat

If you want your changes to take effect immediately, restart Tomcat:

OES 11: `rcnovell-tomcat6 stop`
 `rcnovell-tomcat6 start`

OES 2 Linux: `rcnovell-tomcat5 stop`
 `rcnovell-tomcat5 start`

SLES 11: `rctomcat6 stop`
 `rctomcat6 start`

SLES 10: `rctomcat5 stop`
 `rctomcat5 start`

Windows: 1. At the Windows server, click *Start > Administrative Tools > Services*.
 2. Right-click *Tomcat 6*, then click *Restart*.

64.2 Using the calhost.cfg File

Some aspects of the Calendar Publishing Host cannot be configured in the Administration Web console, so you must manually edit the `calhost.cfg` file instead.

- ◆ [Section 64.2.1, “Editing the calhost.cfg File,” on page 928](#)
- ◆ [Section 64.2.2, “Setting the Published Calendar Auto-Refresh Interval,” on page 928](#)
- ◆ [Section 64.2.3, “Setting the Default Published Calendar View,” on page 929](#)
- ◆ [Section 64.2.4, “Configuring an External POA IP Address,” on page 929](#)
- ◆ [Section 64.2.5, “Changing the SSL Trusted Root Certificate,” on page 929](#)
- ◆ [Section 64.2.6, “Restarting the Web Server,” on page 930](#)

64.2.1 Editing the calhost.cfg File

You can use any ASCII text edit that you prefer to edit the `calhost.cfg` file.

IMPORTANT: It is strongly recommended that you do not modify any settings that are not documented in the following sections.

64.2.2 Setting the Published Calendar Auto-Refresh Interval

By default, when users view a published calendar, the calendar view in the user’s browser is not refreshed while users are viewing the calendar. You can configure the Calendar Publishing Host to automatically refresh the information that displays in a published calendar. This is especially helpful when calendars for resources such as conference rooms are published and displayed outside of the rooms.

- 1 Edit the `calhost.cfg` file.
- 2 Find the line that starts with:

```
Templates.Content.Refresh=
```

- 3 Replace 0 (zero) with the number of seconds after which you want the Calendar Publishing Host to refresh the content of published calendars.

- 4 Save the `calhost.cfg` file, then exit the text editor.
- 5 Skip to [Section 64.2.6, “Restarting the Web Server,” on page 930](#).

64.2.3 Setting the Default Published Calendar View

By default, published calendars are displayed in the Week view. A Day view and a Month view are also available.

- 1 Edit the `calhost.cfg` file.
- 2 Find the line that starts with:

```
User.Calendar.defaultView=
```
- 3 Replace `Week` with `Day` or `Month` as desired.
- 4 Save the `calhost.cfg` file, then exit the text editor.
- 5 Skip to [Section 64.2.6, “Restarting the Web Server,” on page 930](#).

64.2.4 Configuring an External POA IP Address

If the POAs in your GroupWise system are configured to use an external IP address, as described in [Section 36.3.1, “Securing Client/Server Access through an External Proxy Server,” on page 506](#), you can configure the Calendar Publishing Host to always communicate with the POAs in your GroupWise system through that same external IP address.

- 1 Edit the `calhost.cfg` file.
- 2 Find the line that starts with:

```
po.1.Is.IPAddress.External=
```
- 3 Replace `0` with `1` to enable this functionality.
- 4 Add the following lines to the `calhost.cfg` file to define the external POA:

```
po.1.IPAddress=ip_address  
po.1.port=calendar_publishing_port
```

- 4a Replace `ip_address` with the external IP address used by the POAs in your GroupWise system.
 - 4b Replace `calendar_publishing_port` with the calendar publishing port number for the POAs.

The default calendar publishing port number is 80.
- 5 Save the `calhost.cfg` file, then exit the text editor.
- 6 Skip to [Section 64.2.6, “Restarting the Web Server,” on page 930](#).

64.2.5 Changing the SSL Trusted Root Certificate

LDAP authentication using SSL was originally set up during installation, as described in [“Configuring Authentication to the Administration Web Console”](#) in [“Installing the GroupWise Calendar Publishing Host”](#) in the *GroupWise 2012 Installation Guide*. If you need to change the SSL trusted root certificate information, you can rerun the Calendar Publishing Host Installation program

and specify new information, as described in “[Installing the GroupWise Calendar Publishing Host](#)” in “[Installation](#)” in the *GroupWise 2012 Installation Guide*, or you can edit the `calhost.cfg` file, as described below.

- 1 Edit the `calhost.cfg` file.
- 2 Find the line that starts with:

```
Admin.Ldap.trustedRoot=
```
- 3 Specify the full path to the trusted root certificate file.
- 4 Save the `calhost.cfg` file, then exit the text editor.
- 5 Skip to [Section 64.2.6, “Restarting the Web Server,”](#) on page 930.

64.2.6 Restarting the Web Server

After you edit the `calhost.cfg` file, you must restart Apache and Tomcat in order to put the changes into effect.

```
OES 11:    rcnovell-tomcat6 stop
           rcapache2 stop
           rcapache2 start
           rcnovell-tomcat6 start
```

```
OES 2 Linux: rcnovell-tomcat5 stop
              rcapache2 stop
              rcapache2 start
              rcnovell-tomcat5 start
```

```
SLES 11:    rctomcat6 stop
            rcapache2 stop
            rcapache2 start
            rctomcat6 start
```

```
SLES 10:    rctomcat5 stop
            rcapache2 stop
            rcapache2 start
            rctomcat5 start
```

- Windows:
1. At the Windows server, click *Start > Administrative Tools > Services*.
 2. Right-click *Tomcat 6*, then click *Restart*.
 3. Right-click *World Wide Web Publishing Service*, then click *Restart*.

65 Monitoring Calendar Publishing

By monitoring the Calendar Publishing Host and the POAs it communicates with, you can determine whether or not its current configuration is meeting the needs of your GroupWise users.

- ♦ [Section 65.1, “Viewing Calendar Publishing Status at the POA Web Console,” on page 931](#)
- ♦ [Section 65.2, “Using Calendar Publishing Host Log Files,” on page 932](#)
- ♦ [Section 65.3, “Using POA Log Files,” on page 932](#)

65.1 Viewing Calendar Publishing Status at the POA Web Console

- 1 Display the POA Web console at the following URL:

`http://network_address:port`

Replace *network_address* with the IP address or DNS hostname of a POA that is configured for calendar publishing and *port* is the POA HTTP port. The default HTTP port is 7181.

- 2 Click *Configuration*.
- 3 Under the *Internet Protocol Agent Settings* heading, view the configuration information about the POA’s connection to the Calendar Publishing Host.

Internet Protocol Agent Settings:	
IMAP Agent	Disabled
SOAP Agent	Enabled
SOAP Port for incoming SOAP requests:	7191
SOAP over SSL:	Disabled
SOAP Notification List	
Event Configuration List	
Log SOAP Trace	
Calendar/Free Busy Publishing:	Enabled
Calendar Publishing Port:	7171 (Default)
Calendar Publishing Post Office List	Show
Calendar/Free Busy Publishing User List	Show
Calendar Publishing Hosts:	OES Calendar Publishing Host (172.17.5.18:80)
	SLES Calendar Publishing Host (172.17.5.21:80)
	Windows Calendar Publishing Host (172.17.5.19:80)

- 4 Click *Calendar Publishing Post Office List* to view all POAs in your GroupWise system that have been configured for calendar publishing.

GroupWise 2012 POA - Development.Provo1				
Status Configuration Environment Log Files Scheduled Events MTP Status Help				
Calendar Publishing Post Office List				
Domain Name	Post Office Name	Agent Name	IP Address	Publish Port
Provo1	Development	POA	172.17.5.18	7171
Provo2	Sales	POA	172.17.5.21	7171

- 5 Click *Calendar Free/Busy Publishing User List* to view all users who have published free/busy information or personal calendars.

A list of all Calendar Publishing Hosts in your GroupWise system is also provided.

65.2 Using Calendar Publishing Host Log Files

The default log file location is in the [GroupWise Web application working directory](#).

Logging is enabled by default. You can increase the amount of information that is logged, as described in [Section 64.1.3, "Adjusting Log Settings,"](#) on page 924.

65.3 Using POA Log Files

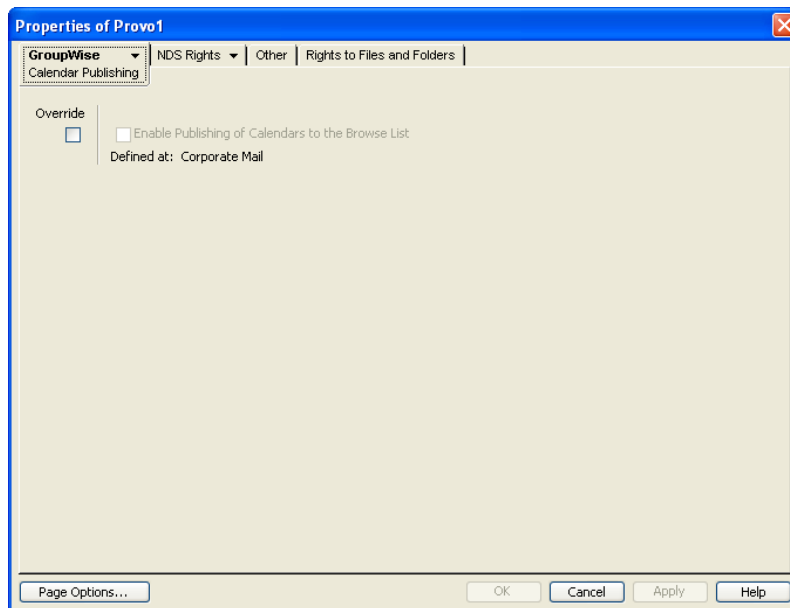
To find status information about how the Calendar Publishing Host is communicating with the POA, you can check the POA log files. For more information, see [Section 37.3.3, "Viewing POA Log Files,"](#) on page 552.

66 Creating a Corporate Calendar Browse List

The Calendar Publishing Host creates a browse list of published calendars. However, by default, no calendars are displayed in the calendar browse list. To create a corporate calendar browse list, you need to grant rights to specific users, or at the post office or domain level, in order to publish to the corporate calendar browse list.

In ConsoleOne:

- 1 Browse to and right-click an individual user, or right-click a post office or domain where you want all users to have rights to publish to the browse list, then click *Properties*.
- 2 Click *GroupWise > Calendar Publishing*.



- 3 Select *Override*, then select *Enable Publishing of Calendars to the Browse List*.
This grants the right to publish calendars to the calendar browse list.
- 4 Click *OK*.
- 5 Repeat [Step 1](#) through [Step 4](#) as needed to grant rights to publish to the corporate calendar browse list.

67 Managing Your Calendar Publishing Host

As circumstances change over time, you might need to change the configuration of your Calendar Publishing Host to better meet the needs of your GroupWise users.

- ♦ [Section 67.1, “Adding Multiple Calendar Publishing Hosts,” on page 935](#)
- ♦ [Section 67.2, “Assigning a Different Calendar Publishing Host to Users,” on page 936](#)
- ♦ [Section 67.3, “Editing Calendar Publishing Host Configuration,” on page 936](#)
- ♦ [Section 67.4, “Deleting a Calendar Publishing Host,” on page 937](#)

67.1 Adding Multiple Calendar Publishing Hosts

Often, one Calendar Publishing Host is sufficient to service all Internet users who want to access your GroupWise users’ calendar and free/busy information. However, you might want to add an additional Calendar Publishing Host for load balancing or to improve response time for Internet users in different geographical locations.

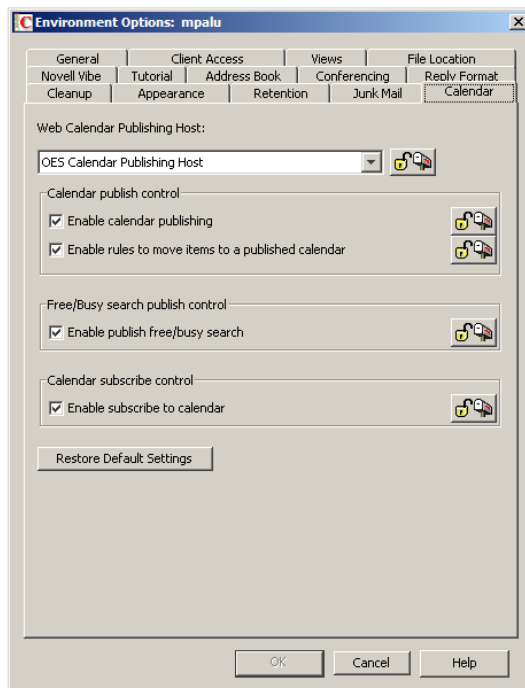
However, if you have users in remote locations, and response time is slow for these users, you can add a Calendar Publishing Host to a POA that is closer to these remote users.

NOTE: Sections referenced in the following steps are found in the [GroupWise 2012 Installation Guide](#).

- 1 Install the Calendar Publish Host software to a remote Web server, as described in [“Installing the GroupWise Calendar Publishing Host”](#).
- 2 Add and configure the new Calendar Publishing Host, as described in [“Configuring the Calendar Publishing Host in ConsoleOne”](#). Make sure you restart the POAs for post offices that support calendar publishing so that the POAs pick up the configuration information for the new Calendar Publishing Host.
- 3 Restart the Web Server and Tomcat on the server where you installed the new Calendar Publishing Host to establish it as part of your GroupWise system, as described in [“Restarting the Web Server and Tomcat”](#).
- 4 Make sure that the new Calendar Publishing Host is accessible by following the procedures provided in [“Testing Calendar Publishing”](#) in the [GroupWise 2012 Installation Guide](#).
- 5 To improve performance when you set up multiple Calendar Publishing Hosts, follow the instructions in TID 7007208: [“Load Balancing and High Availability for GroupWise Calendar Publishing”](#) in the [Novell Support Knowledgebase \(http://www.novell.com/support\)](http://www.novell.com/support).
- 6 Continue with [“Assigning a Different Calendar Publishing Host to Users” on page 936](#).

67.2 Assigning a Different Calendar Publishing Host to Users

- 1 In ConsoleOne, browse to and select a user or a post office with users to whom the new Calendar Publishing Host will be assigned.
- 2 Click *Tools > GroupWise Utilities*.
- 3 Click *Client Options > Environment > Calendar*.



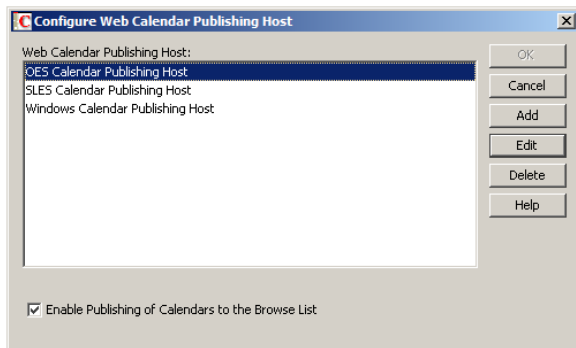
- 4 In the *Web Calendar Publishing Host* field, select the new Calendar Publishing Host, then click the *Lock* button to ensure that the new Calendar Publishing Host setting overrides the previous setting.
- 5 Click *OK*, then click *Close*.
- 6 Repeat [Step 1](#) through [Step 5](#) until you are finished moving users.
- 7 Notify the GroupWise users to whom the new Calendar Publishing Host as been assigned that they need to notify their Internet colleagues of the new URL for their published calendars and free/busy information.

67.3 Editing Calendar Publishing Host Configuration

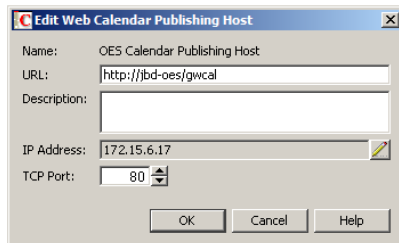
Over time, you might need to set up the Calendar Publishing Host on a different Web server with a different IP address or port number.

NOTE: Sections referenced in the following steps are found in the [GroupWise 2012 Installation Guide](#).

- 1 If necessary, install the Calendar Publishing Host to a new Web server, as described in [“Installation”](#).
- 2 In ConsoleOne, select the GroupWise System object, then click *Tools > GroupWise System Operations > Web Calendar Publishing Hosts*.



- 3 Select the Calendar Publishing Host whose configuration you need to change, then click *Edit*.

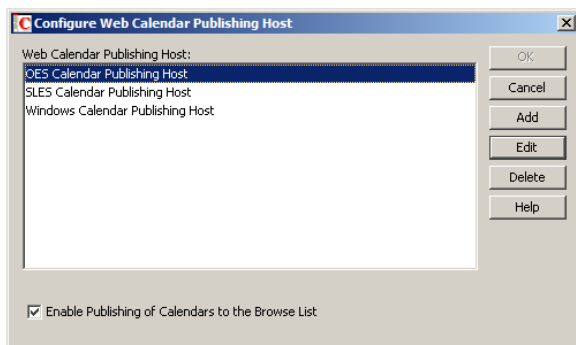


Do not change the URL unless absolutely necessary. Changing the URL would invalidate the URL that GroupWise users have sent to Internet colleagues to access published calendars and free/busy information.

- 4 Modify the IP address or port number as needed, then click *OK* twice.
- 5 Restart Tomcat where the modified Calendar Publishing Host is installed, as described in [“Restarting Tomcat” on page 928](#).
- 6 Restart the POA so that it picks up the updated configuration information for the modified Calendar Publishing Host.
- 7 Make sure that users can still access the Calendar Publishing Host by following the procedures provided in [“Testing Calendar Publishing”](#).

67.4 Deleting a Calendar Publishing Host

- 1 If necessary, move users, [Section 67.2, “Assigning a Different Calendar Publishing Host to Users,” on page 936](#).
- 2 In ConsoleOne, select the GroupWise System object, then click *Tools > GroupWise System Operations > Web Calendar Publishing Hosts*.



- 3 Select the Calendar Publishing Host to delete, then click *Delete*.
- 4 Click *OK*.
- 5 Restart Tomcat where the Calendar Publishing Host has been deleted, as described in [“Restarting Tomcat” on page 928](#).
- 6 Restart the POA that used to communicate with the deleted Calendar Publishing Host, so that the POA does not try to reestablish the connection.

XV Monitor

- ♦ [Chapter 68, “Understanding the Monitor Agent Consoles,”](#) on page 941
- ♦ [Chapter 69, “Configuring the Monitor Agent,”](#) on page 945
- ♦ [Chapter 70, “Configuring the Monitor Application,”](#) on page 969
- ♦ [Chapter 71, “Using GroupWise Monitor,”](#) on page 973
- ♦ [Chapter 72, “Comparing the Monitor Consoles,”](#) on page 1001
- ♦ [Chapter 73, “Using Monitor Agent Startup Switches,”](#) on page 1003

For a complete list of port numbers used by Monitor, see [Section A.9, “Monitor Agent Port Number,”](#) on page 1173 and [Section A.10, “Monitor Application Port Numbers,”](#) on page 1173.

For detailed Linux-specific Monitor information, see [Appendix C, “Linux Commands, Directories, and Files for GroupWise Administration,”](#) on page 1179.

68 Understanding the Monitor Agent Consoles

The Monitor Agent offers three different consoles where you can check the status of your GroupWise agents:

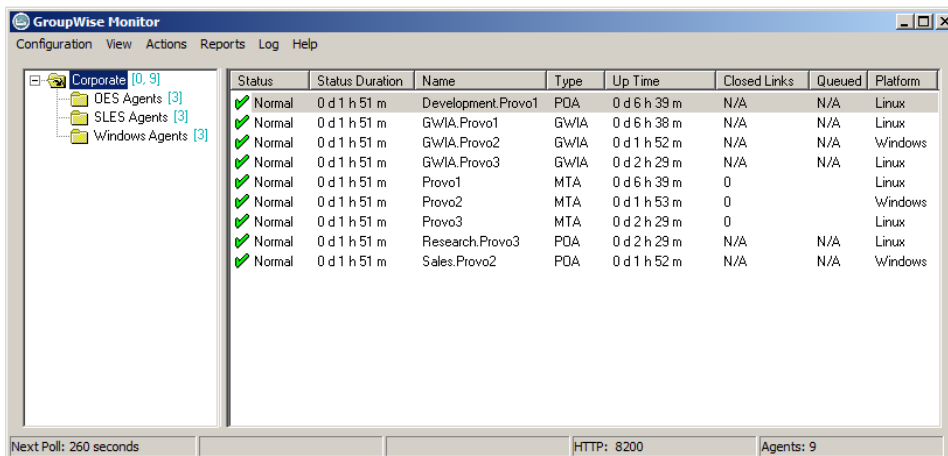
- ♦ [Section 68.1, “Monitor Agent Server Console,” on page 941](#)
- ♦ [Section 68.2, “Monitor Agent Web Console,” on page 942](#)
- ♦ [Section 68.3, “Monitor Web Console,” on page 942](#)

For a comparison of the capabilities of the three consoles, see [Chapter 72, “Comparing the Monitor Consoles,” on page 1001](#).

For detailed instructions about installing and starting the GroupWise Monitor Agent for the first time, see “[Installing GroupWise Monitor](#)” in the *GroupWise 2012 Installation Guide*.

68.1 Monitor Agent Server Console

The Monitor Agent server console is available for the Windows Monitor Agent but not for the Linux Monitor Agent.



All agent configuration tasks can be performed at the Monitor Agent server console, but some reports are not available.

68.2 Monitor Agent Web Console

The Monitor Agent Web console is platform-independent and can be viewed at the following URL:

`http://web_server_address:8200`

[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)

The screenshot displays the 'Monitored agents for Corporate' section. On the left, there is a sidebar with a tree view showing 'Corporate' with three subgroups: 'OES Agents [3]', 'SLES Agents [3]', and 'Windows Agents [3]'. Below this are buttons for 'Create', 'Rename', 'Move', and 'Delete'. The main area shows a table of monitored agents with columns for Status, Duration, Name, Type, Up Time, Closed Links, Queued, Platform, and Version. The table contains 10 rows of agent data, all with a status of 'Normal' and an up time of 0 d 2 h 5 m.

<input type="checkbox"/>	Status	Status Duration	Name	Type	Up Time	Closed Links	Queued	Platform	Version
<input type="checkbox"/>	Normal	0 d 2 h 5 m	Development Provo1	POA	0 d 6 h 49 m	N/A	N/A	Linux	12.0.0 (12/03/2011)
<input type="checkbox"/>	Normal	0 d 2 h 5 m	GWIA Provo1	GWIA	0 d 6 h 48 m	N/A	N/A	Linux	12.0.0 (12/03/2011)
<input type="checkbox"/>	Normal	0 d 2 h 5 m	GWIA Provo2	GWIA	0 d 2 h 2 m	N/A	N/A	Windows	12.0.0 (12/03/11)
<input type="checkbox"/>	Normal	0 d 2 h 5 m	GWIA Provo3	GWIA	0 d 2 h 39 m	N/A	N/A	Linux	12.0.0 (12/03/2011)
<input type="checkbox"/>	Normal	0 d 2 h 5 m	Provo1	MTA	0 d 6 h 49 m	0	0	Linux	12.0.0 (12/03/2011)
<input type="checkbox"/>	Normal	0 d 2 h 5 m	Provo2	MTA	0 d 2 h 3 m	0	0	Windows	12.0.0 (12/3/2011)
<input type="checkbox"/>	Normal	0 d 2 h 5 m	Provo3	MTA	0 d 2 h 39 m	0	0	Linux	12.0.0 (12/03/2011)
<input type="checkbox"/>	Normal	0 d 2 h 5 m	Research Provo3	POA	0 d 2 h 39 m	N/A	N/A	Linux	12.0.0 (12/03/2011)
<input type="checkbox"/>	Normal	0 d 2 h 5 m	Sales Provo2	POA	0 d 2 h 2 m	N/A	N/A	Windows	12.0.0 (12/3/2011)

To create the Monitor Agent Web console display, your Web server communicates directly with the Monitor Agent to obtain agent status information. You must be behind your firewall to use the Monitor Agent Web console. Because the Linux Monitor Agent does not have a server console, you use the Monitor Agent Web console in its place on Linux.

The Monitor Agent Web console is divided into the Agent Groups window on the left and the Agent Status window on the right. You can use the Agents Groups window to create and manage agent groups in the same way that you can at the Monitor Agent server console.

Several Monitor features are available at the Monitor Agent Web console that are not available at the Monitor Agent server console or the Monitor Web console. These are summarized in [Chapter 72, "Comparing the Monitor Consoles,"](#) on page 1001.

68.3 Monitor Web Console

The Monitor Web console is also platform-independent and can be viewed at the following URL:

`http://web_server_address/gwmon/gwmonitor`

GroupWise® Monitor Novell.

Corporate

- QES Agents
- SLES Agents
- Windows Agents

Monitored agents for "Corporate" group
Total: 9 Displayed: 1 - 9

Refresh

Hide Subgroup Agents Problem Suspend Resume Move Options Thresholds Help

<input type="checkbox"/>	Name	Status	Status Duration	Up Time	Type	Version	Platform
<input type="checkbox"/>	Provo1	Normal	0 d 1 h 54 m	0 d 6 h 39 m	MTA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	Development.Provo1	Normal	0 d 1 h 54 m	0 d 6 h 39 m	POA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	GWIA.Provo1	Normal	0 d 1 h 54 m	0 d 6 h 38 m	GWIA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	Provo3	Normal	0 d 1 h 54 m	0 d 2 h 29 m	MTA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	GWIA.Provo3	Normal	0 d 1 h 54 m	0 d 2 h 29 m	GWIA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	Research.Provo3	Normal	0 d 1 h 54 m	0 d 2 h 29 m	POA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	Provo2	Normal	0 d 1 h 54 m	0 d 1 h 53 m	MTA	12.0.0 (12/3/2011)	Windows
<input type="checkbox"/>	GWIA.Provo2	Normal	0 d 1 h 54 m	0 d 1 h 52 m	GWIA	12.0.0 (12-03-11)	Windows
<input type="checkbox"/>	Sales.Provo2	Normal	0 d 1 h 54 m	0 d 1 h 52 m	POA	12.0.0 (12/3/2011)	Windows

Create
Rename
Move
Delete
Refresh
Help

To create the Monitor Web console display, your Web server communicates with the Monitor Application (a component of your Web server), which then communicates with the Monitor Agent to obtain agent status information. This enables the Monitor Web console to be available outside your firewall, while the Monitor Agent Web console can be used only inside your firewall.

The Monitor Web console is divided into the Agent Groups window on the left and the Agent Status window on the right. Using the Agents Groups window, you can create and manage agent groups the same as you can at the Monitor Agent server console.

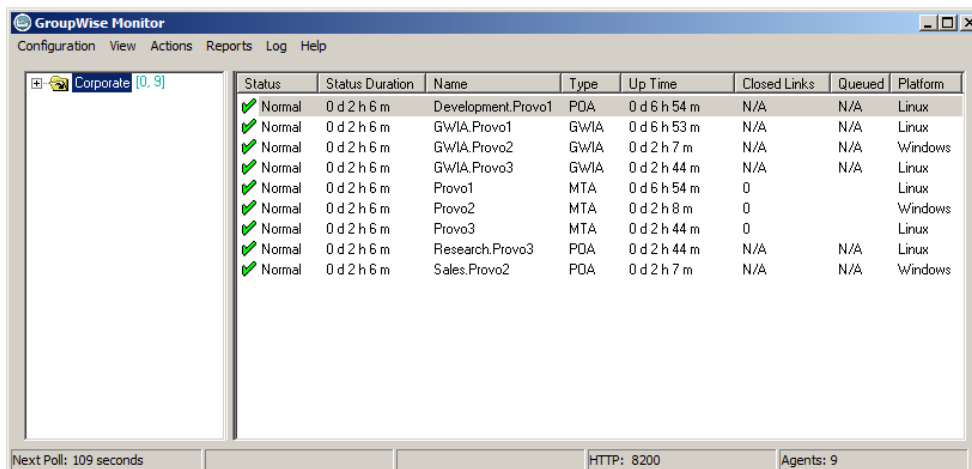
The Monitor Web console does not include some features that are available at the Monitor Agent server console and the Monitor Agent Web console. These are summarized in [Chapter 72, "Comparing the Monitor Consoles,"](#) on page 1001.

69 Configuring the Monitor Agent

For GroupWise Monitor system requirements, see “[Monitor System Requirements](#)” in the *GroupWise 2012 Installation Guide*. For detailed instructions about installing and starting the GroupWise Monitor Agent for the first time, see “[Installing GroupWise Monitor](#)” in the *GroupWise 2012 Installation Guide*.

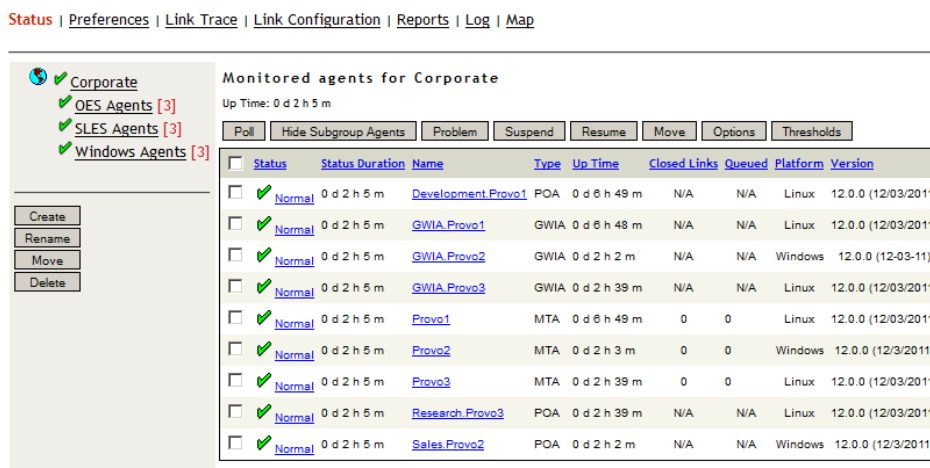
The default configuration of the GroupWise Monitor Agent is adequate to begin monitoring existing GroupWise agents (Post Office Agents, Message Transfer Agents, and Internet Agents). You can also customize the configuration to meet your specific monitoring needs.

On Windows, you configure the Monitor Agent at the Monitor Agent server console on the Windows server where the Monitor Agent is running.



On Linux, similar functionality is available in your Web browser at the Monitor Agent Web console:

<http://localhost:8200>



The following topics help you customize the Monitor Agent for your specific needs:

- ◆ Section 69.1, “Selecting Agents to Monitor,” on page 946
- ◆ Section 69.2, “Creating and Managing Agent Groups,” on page 949
- ◆ Section 69.3, “Configuring Monitoring Protocols,” on page 952
- ◆ Section 69.4, “Configuring Polling of Monitored Agents,” on page 956
- ◆ Section 69.5, “Configuring Email Notification for Agent Problems,” on page 957
- ◆ Section 69.6, “Configuring Audible Notification for Agent Problems,” on page 961
- ◆ Section 69.7, “Configuring SNMP Trap Notification for Agent Problems,” on page 962
- ◆ Section 69.8, “Configuring Authentication and Intruder Lockout for the Monitor Web Console,” on page 964
- ◆ Section 69.9, “Configuring Monitor Agent Log Settings,” on page 965
- ◆ Section 69.10, “Configuring Proxy Service Support for the Monitor Web Console,” on page 966
- ◆ Section 69.11, “Monitoring Messenger Agents,” on page 967
- ◆ Section 69.12, “Supporting the GroupWise High Availability Service on Linux,” on page 968

69.1 Selecting Agents to Monitor

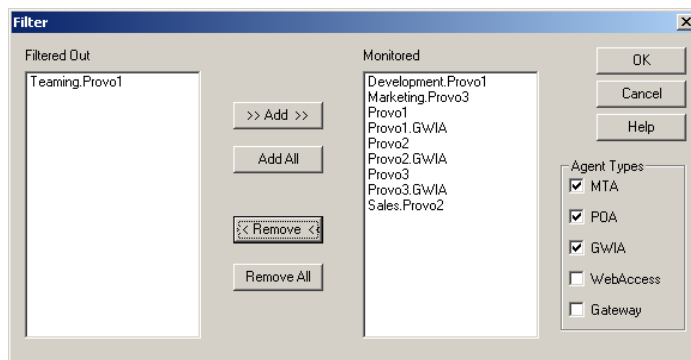
By default, the Monitor Agent starts monitoring all GroupWise agents (Post Office Agents, Message Transfer Agents, and Internet Agents) in your GroupWise system, based on the information from a domain database (`wpdomain.db`). You might not want to continue monitoring all agents. Under certain circumstances, you might want to monitor agents that are not part of your local GroupWise system.

- ◆ Section 69.1.1, “Filtering the Agent List,” on page 946
- ◆ Section 69.1.2, “Adding an Individual Agent,” on page 947
- ◆ Section 69.1.3, “Adding All Agents on a Server,” on page 948
- ◆ Section 69.1.4, “Adding All Agents on a Subnet,” on page 948
- ◆ Section 69.1.5, “Removing Added Agents,” on page 949

69.1.1 Filtering the Agent List

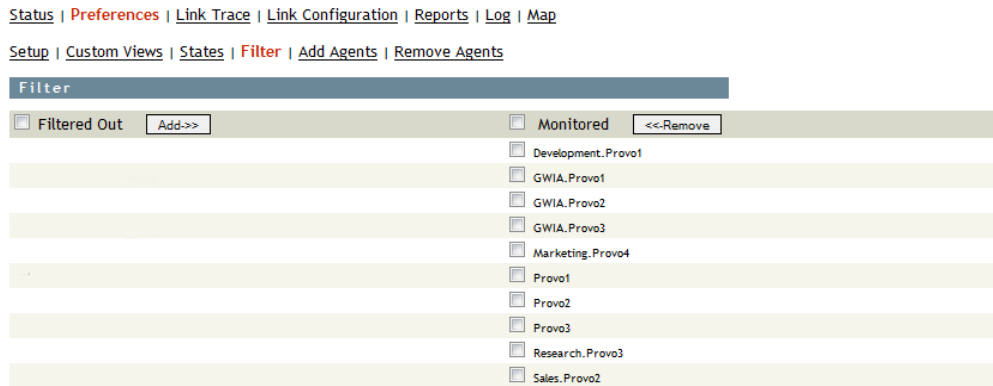
You can configure the Monitor Agent to stop and start monitoring selected agents as needed.

- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > Filter*.



or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Filter*.



The *Filtered Out* list displays all agents that are not currently being monitored.

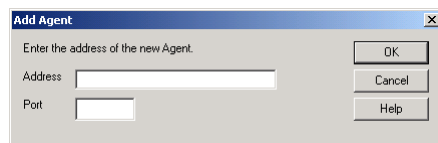
- 2 Select one or more agents in the *Monitored* list, then click *Remove* to move them to the *Filtered Out* list.
- 3 Click *OK*.

Agents in the *Filtered Out* list are not monitored and do not appear at the Monitor Agent server console or at the Monitor Agent Web console. To start monitoring a filtered-out agent, move it back to the *Monitored* list.

69.1.2 Adding an Individual Agent

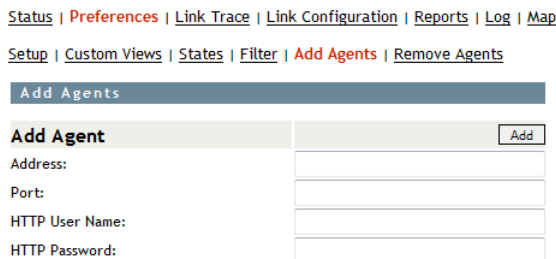
You can start monitoring an individual agent anywhere in your GroupWise system or another GroupWise system.

- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > Add Agent*.



or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Add Agents*.



- 2 Type the IP address of the server where the agent runs.
- 3 Type the port number the agent listens on.

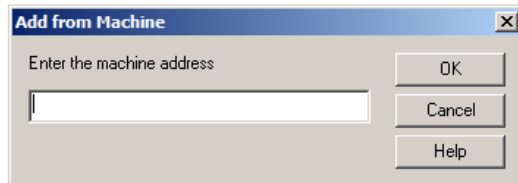
- 4 Click *OK*.

The agent is added to the list of monitored agents.

69.1.3 Adding All Agents on a Server

If you add a new server to your GroupWise system or want to monitor agents in a different GroupWise system, you can easily start monitoring all the agents running on that server.

- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > Add from Machine*.



or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Add Agents*.

Add from Machine		Add
Machine Address:	<input type="text"/>	
SNMP Community String:	<input type="text"/>	

- 2 Type the IP address of the new server, then click *OK*.

All GroupWise agents on the new server are added to the list of monitored agents.

If the new server is part of your local GroupWise system, you can simply restart the Monitor Agent and it picks up all new agents in your system.

69.1.4 Adding All Agents on a Subnet

If you add several new servers to your GroupWise system or want to monitor agents in a different GroupWise system, you can easily start monitoring all the agents running on the same subnet.

- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > Add from Network*.



or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Add Agents*.

Add from Network		Add
Subnet Address:	<input type="text"/>	
SNMP Community String:	<input type="text"/>	

- 2 Type the subnet portion of the IP addresses of the new servers, then click *OK*.

All GroupWise agents on the subnet are added to the list of monitored agents.

If the new servers are part of your local GroupWise system, you can simply restart the Monitor Agent and it picks up all new agents in your system.

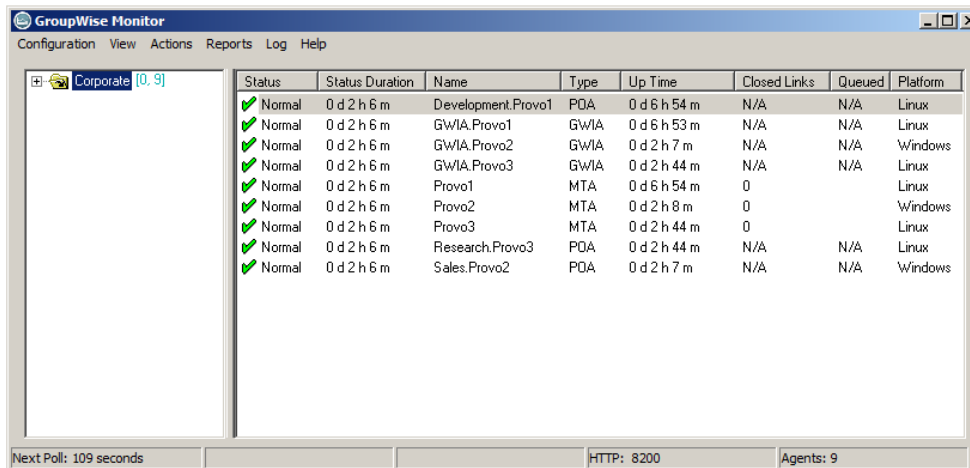
69.1.5 Removing Added Agents

To stop monitoring agents that you have manually added to the Monitor Agent's configuration:

- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > Remove Agents*.
or
On Linux, at the [Monitor Agent Web console](#), click *Preferences > Remove Agents*.
- 2 Select the agents you want to remove, then click *Remove*.
- 3 Click *OK*.

69.2 Creating and Managing Agent Groups

You might find it convenient to group related agents together for monitoring purposes. Initially, all agents are in a single group with the same name as your GroupWise system.

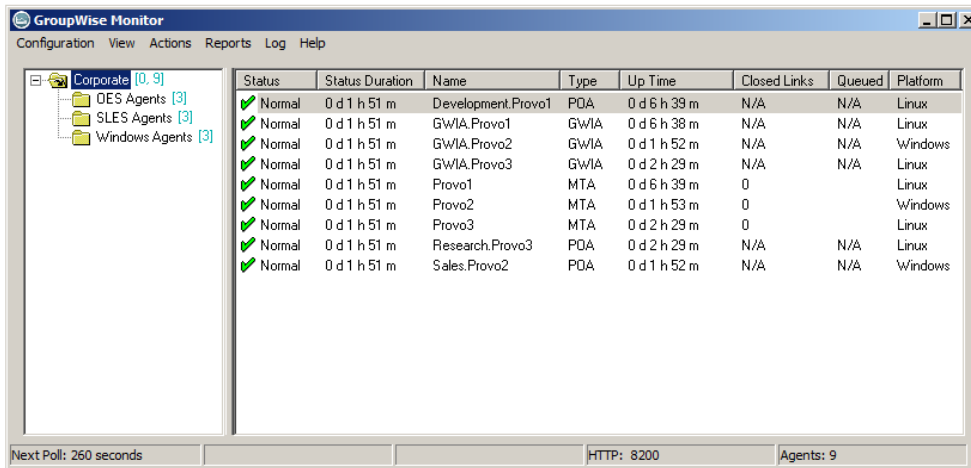


The screenshot shows the GroupWise Monitor application window. The title bar reads "GroupWise Monitor" and the menu bar includes "Configuration", "View", "Actions", "Reports", "Log", and "Help". On the left, a tree view shows a folder named "Corporate" with a sub-item "[0, 9]". The main area displays a table of agents with the following columns: Status, Status Duration, Name, Type, Up Time, Closed Links, Queued, and Platform.

Status	Status Duration	Name	Type	Up Time	Closed Links	Queued	Platform
✓ Normal	0 d 2 h 6 m	Development.Provo1	POA	0 d 6 h 54 m	N/A	N/A	Linux
✓ Normal	0 d 2 h 6 m	GWIA.Provo1	GWIA	0 d 6 h 53 m	N/A	N/A	Linux
✓ Normal	0 d 2 h 6 m	GWIA.Provo2	GWIA	0 d 2 h 7 m	N/A	N/A	Windows
✓ Normal	0 d 2 h 6 m	GWIA.Provo3	GWIA	0 d 2 h 44 m	N/A	N/A	Linux
✓ Normal	0 d 2 h 6 m	Provo1	MTA	0 d 6 h 54 m	0		Linux
✓ Normal	0 d 2 h 6 m	Provo2	MTA	0 d 2 h 8 m	0		Windows
✓ Normal	0 d 2 h 6 m	Provo3	MTA	0 d 2 h 44 m	0		Linux
✓ Normal	0 d 2 h 6 m	Research.Provo3	POA	0 d 2 h 44 m	N/A	N/A	Linux
✓ Normal	0 d 2 h 6 m	Sales.Provo2	POA	0 d 2 h 7 m	N/A	N/A	Windows

At the bottom of the window, there are three status boxes: "Next Poll: 109 seconds", "HTTP: 8200", and "Agents: 9".

Agent groups are displayed on the left side of the Monitor Agent server console. When you select an agent group, the monitored agents in the group and their status information are listed on the right side of the Monitor Agent server console.



You can create additional groups and subgroups as needed to make monitoring similar agents easier. You might want to create agent groups based on geographical areas, on administrative responsibilities, or on agent configuration similarities. The number of agents in the group is displayed to the right of the group name in the Agent Groups window.

In addition, by creating agent groups, you can provide configuration settings for monitoring just once for all agents in each group, rather than providing them individually for each agent in your GroupWise system.

- ♦ [Section 69.2.1, “Creating an Agent Group,”](#) on page 950
- ♦ [Section 69.2.2, “Managing Agent Groups,”](#) on page 951
- ♦ [Section 69.2.3, “Viewing Your Agent Group Hierarchy,”](#) on page 951
- ♦ [Section 69.2.4, “Configuring an Agent Group,”](#) on page 952

NOTE: On Linux, you perform these tasks at the [Monitor Agent Web console](#) or [Monitor Web console](#), using steps similar to those provided in this section.

69.2.1 Creating an Agent Group

On Windows, at the [Monitor Agent server console](#):

- 1 Right-click the folder where you want to create the agent group, then click *Create*.
- 2 Type a name for the new group, then click *OK* to create a new folder for the agent group.
The group name must be unique within its parent group.
- 3 Click a folder containing agents that you want to add to the new group.
- 4 Drag and drop agents into the new group as needed.
- 5 Click the new group to view its contents.

On Linux, at the [Monitor Agent Web console](#):

- 1 In the Agent Groups window, click *Create*.
- 2 Type a name for the new group, select the parent group for the new group, then click *Create*.

- 3 In the Agent Status window, select one or more agents to add to the new group, then click *Move*.
- 4 In the list of available groups, select the new group, then click *Move*.
- 5 Click the new group to view its contents.

You can nest groups within groups as needed.

69.2.2 Managing Agent Groups

On Windows, at the [Monitor Agent server console](#):

- ♦ To rename an agent group, right-click the agent group, click *Rename*, type the new name, then press Enter.
- ♦ To move an agent group, drag and drop it to its new location.
- ♦ To delete an agent group, right-click the agent group, then click *Delete*. A group must be empty before you can delete it.

On Linux, at the [Monitor Agent Web console](#):

- ♦ To rename an agent group, click *Rename*, type the new name, select the group to rename, then click *Rename*.
- ♦ To move an agent group, click *Move*, select the group to move, select the new location, then click *Move*.
- ♦ To delete an agent group, click *Delete*, select the group to delete, then click *Delete*.

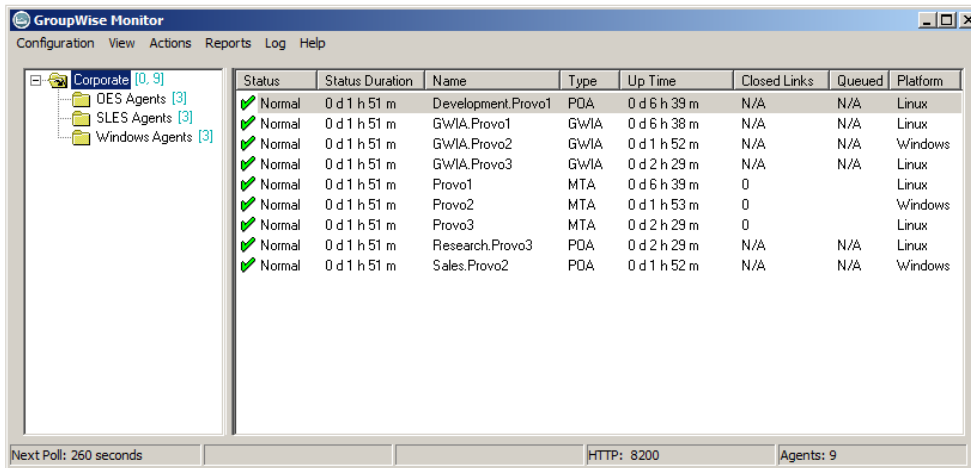
69.2.3 Viewing Your Agent Group Hierarchy

When you create nested groups, you can choose how much of the hierarchy you want displayed.

On Windows, at the [Monitor Agent server console](#):

- ♦ To open and close groups, click the plus or minus icons next to each folder.
- ♦ To expand your entire group hierarchy, click *View > Expand Tree*.

- To collapse your entire group hierarchy, click *View > Collapse Tree*.
- You can decide whether you want to view just the agents in the currently selected group or the agents in subgroups as well. By default, only the agents in the selected folder are listed in the agent window. Right-click an agent group, then click *Show Subgroup Agents* to display the contents of nested groups along with the selected group.



Numbers in brackets next to each group indicate the number of agents in the selected group and the total number displayed.

69.2.4 Configuring an Agent Group

Configuration settings for monitoring can be set individually for each monitored agent, for each agent group, or for all monitored agents collectively.

You can establish default configuration settings for all agents by setting them on the root agent group that is named the same as your GroupWise system. Those default settings can be inherited by each subgroup that you create thereafter if you select *Apply Options to Subgroups*. Those default settings can be overridden by establishing different settings for an agent group or for an individual agent if you deselect *Use Parent Options*.

69.3 Configuring Monitoring Protocols

By default, the Monitor Agent uses HTTP to communicate with the agents it monitors. If HTTP is not available, the Monitor Agent changes automatically to SNMP.

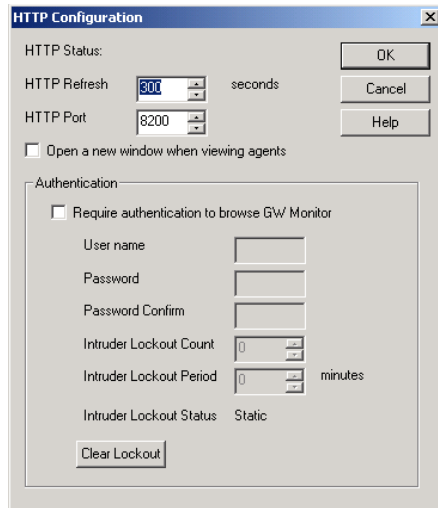
GroupWise 2012 agents, GroupWise 8 agents, GroupWise 7 agents, GroupWise 6.x agents and 6.x-level gateways, as well as the GroupWise agents provided with the GroupWise 5.5 Enhancement Pack, can be monitored using HTTP. Agents dating from GroupWise 5.5 and earlier, as well as 5.5-level GroupWise gateways, must be monitored using SNMP.

- [Section 69.3.1, “Configuring the Monitor Agent for HTTP,” on page 953](#)
- [Section 69.3.2, “Configuring the Monitor Agent for SNMP,” on page 955](#)

69.3.1 Configuring the Monitor Agent for HTTP

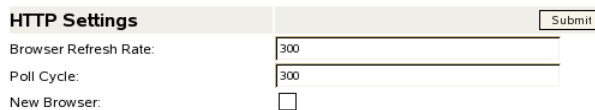
You can customize how the Monitor Agent communicates with your Web browser.

- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > HTTP*.



or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Setup*, then scroll down to the *HTTP Settings* section.



- 2 Modify the HTTP settings as needed:

HTTP Refresh: Specify the number of seconds after which the Monitor Agent sends updated information to the Monitor Web console. The default is 300 seconds (5 minutes).

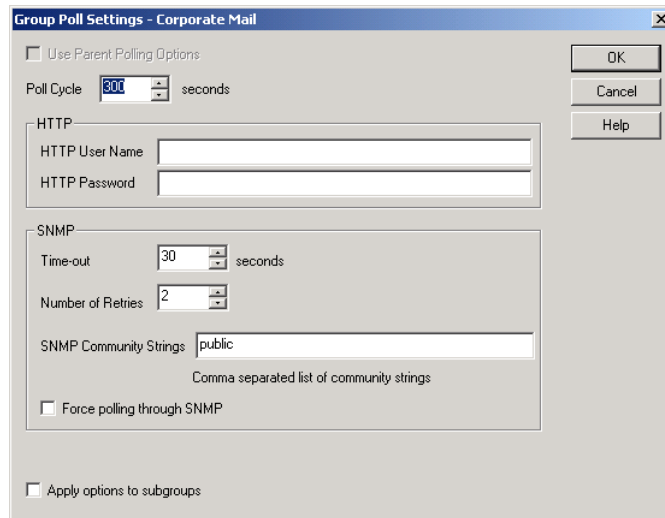
HTTP Port: Specify the port number for the Monitor Agent to listen on for requests for information from the Web console. The default port number is 8200.

NOTE: On Linux, at the [Monitor Agent Web console](#), the *HTTP Port* field is not available. However, you can use the `--httpport` startup switch when you start the Monitor Agent to achieve the same functionality. For more information, see [Chapter 73, “Using Monitor Agent Startup Switches,”](#) on page 1003.

Open a new window when viewing agents: Select this option to open a new Web browser window whenever you display an agent Web console. This enables you to view the Monitor Web console and an agent Web console at the same time, or to view two agent Web consoles at the same time for comparison.

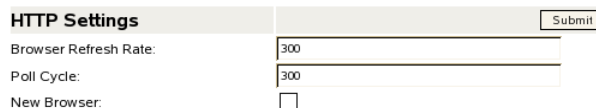
- 3 Click *OK* to put the new HTTP settings into effect.

- 4 On Windows, at the [Monitor Agent server console](#), click *Configuration > Poll Settings*.



or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Setup*, then scroll down to the *HTTP Settings* section.



- 5 Fill in the following fields:

Poll Cycle: Specify the number of seconds after which the Monitor Agent polls all monitored GroupWise agents for updated information.

By default, the Monitor Agent starts 20 threads to poll monitored agents. You can use the `--pollthreads` startup switch to adjust the number of threads. For more information, see [Chapter 73, “Using Monitor Agent Startup Switches,”](#) on page 1003.

By default, the Monitor Agent communicates with other GroupWise agents by way of XML. However, if XML is unavailable, the Monitor Agent automatically uses SNMP instead. Prior to the GroupWise 5.5 Enhancement Pack, GroupWise agents did not support XML, so the Monitor Agent must use SNMP to monitor these older agents. If you need to monitor older agents, see [Section 69.3.2, “Configuring the Monitor Agent for SNMP,”](#) on page 955.

If all monitored agents in the group require the same user name and password in order to communicate with the Monitor Agent, you can provide that information as part of the Monitor Agent’s configuration.

HTTP User Name: Provide the user name for the Monitor Agent to use when contacting monitored agents in the group for status information.

HTTP Password: Provide the password, if any, associated with the user name specified in the field above.

NOTE: On Linux, at the [Monitor Agent Web console](#), the *HTTP User Name* and *HTTP Password* fields are not available. However, you can use the `--httpagentuser` and `--httpagentpassword` startup switches when you start the Monitor Agent to achieve the same functionality. For more information, see [Chapter 73, “Using Monitor Agent Startup Switches,”](#) on page 1003.

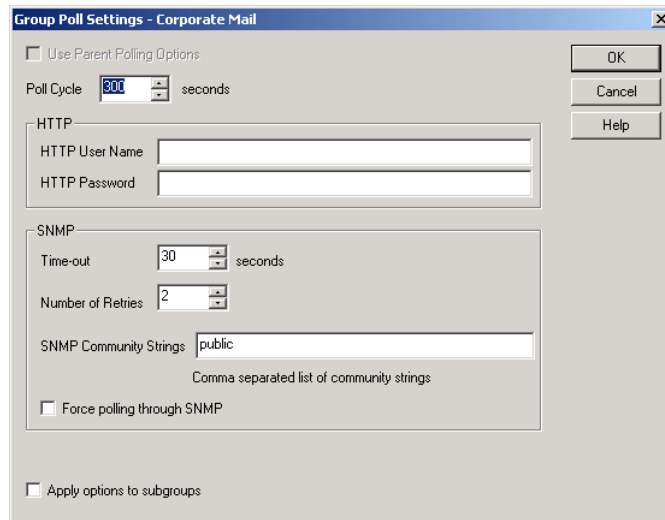
If the monitored agents use different user names and passwords, you are prompted to supply them when the Monitor Agent needs to communicate with the monitored agents.

- 6 Select *Apply options to subgroups* if you want subgroups to inherit these settings.
- 7 Click *OK* to put the specified poll cycle into effect.

69.3.2 Configuring the Monitor Agent for SNMP

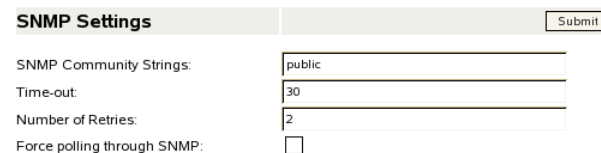
The Monitor Agent must use SNMP to communicate with GroupWise agents that date from earlier than the GroupWise 5.5 Enhancement Pack. You can customize how the Monitor Agent communicates with such older agents and how it communicates with SNMP monitoring and management programs.

- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > Poll Settings*.



or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Setup*, then scroll down to the *SNMP Settings* section.



- 2 Specify the number of seconds after which the Monitor Agent polls all monitored GroupWise agents for updated information using SNMP.

- 3 In the SNMP box, modify the SNMP settings as needed:

Time-out: Specify the number of seconds the Monitor Agent should wait for a response from servers where GroupWise agents run.

Number of Retries: Specify how often the Monitor Agent should try to contact the servers where GroupWise agents run.

SNMP Community Strings: Provide a comma-delimited list of community strings required to access the servers where GroupWise agents run.

Force polling through SNMP: Select this option to use SNMP polling instead of the default of XML polling when contacting servers where agents in the group run.

- 4 Click *Apply options to subgroups* if you want subgroups to inherit these settings.
- 5 Click **OK** to put the new SNMP settings into effect.
- 6 Make sure the GroupWise agents you want to monitor using SNMP are enabled for SNMP. See [Section 37.6.1, “Setting Up SNMP Services for the POA,”](#) on page 553 and [Section 43.6.1, “Setting Up SNMP Services for the MTA,”](#) on page 679. The same instructions can be followed for all versions of the GroupWise agents.

69.4 Configuring Polling of Monitored Agents

By default, the Monitor Agent polls all monitored agents every five minutes. You can adjust the poll cycle as needed.

- 1 On Windows, at the [Monitor Agent server console](#), select the root agent group to set the poll cycle default for all monitored agents.

or

Select any agent group to set the poll cycle for the agents in the selected group.

or

Select any agent to set the poll cycle for that individual agent.

then

Click *Configuration > Poll Settings*.

The screenshot shows the 'Group Poll Settings - Corporate Mail' dialog box. It features a title bar with a close button. The main area contains several sections: 'Use Parent Polling Options' (checkbox, unchecked), 'Poll Cycle' (spin box set to 800, followed by 'seconds'), 'HTTP' section with 'HTTP User Name' and 'HTTP Password' text boxes, 'SNMP' section with 'Time-out' (spin box set to 30, followed by 'seconds'), 'Number of Retries' (spin box set to 2), 'SNMP Community Strings' (text box containing 'public', with a note 'Comma separated list of community strings'), and 'Force polling through SNMP' (checkbox, unchecked). At the bottom, there is an 'Apply options to subgroups' checkbox (unchecked). On the right side, there are three buttons: 'OK', 'Cancel', and 'Help'.

Unless you selected the root agent group, *Use Parent Polling Options* is selected and all options are dimmed. Deselect *Use Parent Polling Options* to configure polling for an agent group or individual agent.

or

On Linux, at the [Monitor Agent Web console](#), select one or more agents, click *Preferences > Setup*, then scroll down to the *HTTP Settings* section.

HTTP Settings		Submit
Browser Refresh Rate:	<input type="text" value="300"/>	
Poll Cycle:	<input type="text" value="300"/>	
New Browser:	<input type="checkbox"/>	

NOTE: The *Use Parent Polling Options* and *Apply Options to Subgroups* options are not available on Linux.

- 2 Increase or decrease the poll cycle as needed, then click *OK*.

69.5 Configuring Email Notification for Agent Problems

The Monitor Agent can notify you by email when agent problems arise.

- ♦ [Section 69.5.1, “Configuring Email Notification,”](#) on page 957
- ♦ [Section 69.5.2, “Customizing Notification Thresholds,”](#) on page 959

69.5.1 Configuring Email Notification

You can configure the Monitor Agent to notify one or more users by email if an agent goes down. You can also receive email confirmation messages showing that the Monitor Agent itself is still running normally.

- 1 On Windows, at the [Monitor Agent server console](#), select the root agent group to set up email notification defaults for all monitored agents.
or
Select any agent group to set up email notification for the agents in the selected group.
or
Select any agent to set up email notification for that individual agent.
then

Click *Configuration > Notification*.

The screenshot shows a configuration window titled "Group Notification - Corporate Mail". It contains several sections: "Use Parent Notification Options" (unchecked), "Notification List" (text input), "Mail Domain Name" (text input), "Relay Address" (text input), "Send SNMP Traps" (unchecked), "Play Sound" (checked) with a "Sounds" button, "Notification Events" (Agent Down, Server Down, Threshold Exceeded, State returns to Normal all checked) with a "Thresholds" button and a "Minimum threshold level for notification" dropdown set to "Unknown", "Repeat Notification After" (15 minutes), "Periodic Monitor Confirmation" (unchecked) with a "Confirm" input (1 minutes), and "Apply options to subgroups" (unchecked). Buttons for "OK", "Cancel", "Test Notify", and "Help" are on the right.

Unless you selected the root agent group, *Use Parent Notification Options* is selected and all options are dimmed. Deselect *Use Parent Notification Options* to set up email notification for an agent group or an individual agent.

or

On Linux, at the [Monitor Agent Web console](#), select one or more agents, then click *Preferences > Setup* to display the *Notify* settings.

[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)
[Setup](#) | [Custom Views](#) | [States](#) | [Filter](#) | [Add Agents](#) | [Remove Agents](#)

The screenshot shows the "Preferences" page with the "Notify" tab selected. It includes a "Submit" button and the following settings: "Notification List" (text input), "Mail Domain Name" (text input), "Relay Address" (text input), "Send SNMP Traps" (unchecked), "Trap Targets" (text input with a note: "Comma separated list of address:community pairs"), "Agent Down" (checked), "Server Down" (checked), "Threshold Exceeded" (checked), "Minimum Threshold" (dropdown set to "Unknown"), "State returns to Normal" (checked), "Notification Repeat Time (minutes)" (15), and "Periodic Notification" (0).

NOTE: The *Use Parent Notification Options* and *Apply Options to Subgroups* options are not available on Linux.

- 2 Specify one or more email addresses or pager addresses to send notifications to.
- 3 Specify the Internet domain name of your GroupWise system.
- 4 If the mail system to which email notification is being sent performs reverse DNS lookups, specify the IP address or hostname of a server to relay the notification messages through.

The Monitor Agent should relay email notifications through a server that has a published DNS address.

- 5 On Windows, at the [Monitor Agent server console](#), click *Test Notify* to determine if the Monitor Agent can successfully send to the addresses specified in the *Notification List* field.

A message informs you of the results of the test. If the test is successful, a test message arrives shortly at each address. If the test is unsuccessful, verify the information you provided in the *Notification List*, *Mail Domain Name*, and *Relay Address* fields.

NOTE: On Linux, at the [Monitor Agent Web console](#), email notifications cannot be tested.

- 6 Select the events to trigger email notification messages.
 - ◆ Agent Down
 - ◆ Server Down
 - ◆ Threshold Exceeded
 - ◆ State returns to Normal

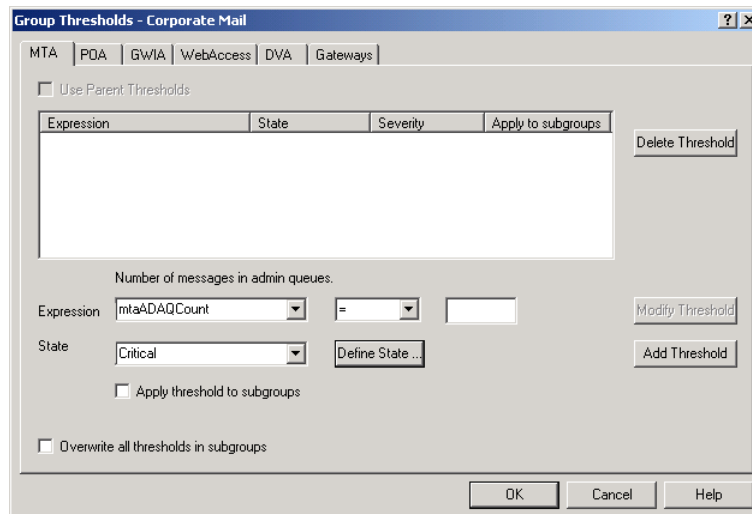
If you want to be notified of more specific states, see [Section 69.5.2, “Customizing Notification Thresholds,”](#) on page 959.

- 7 Select the amount of time that you want to elapse before repeat email notifications are sent.
- 8 To monitor the Monitor Agent and assure it is functioning normally, select *Periodic Monitor Confirmation*, then select the number of minutes between Monitor Agent email confirmation messages.
- 9 Click *OK* to save the email notification settings.

69.5.2 Customizing Notification Thresholds

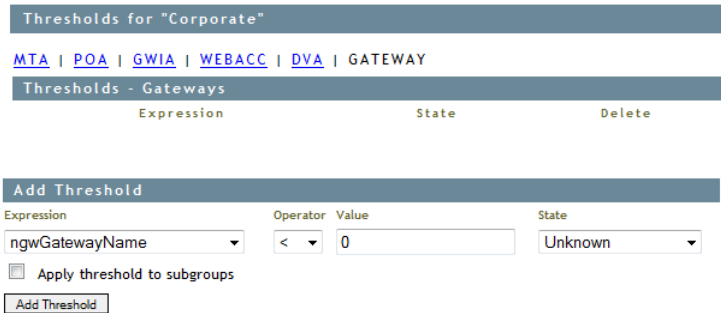
To refine the types of events that trigger email notification messages, you can create your own thresholds that describe very specific states. Using thresholds, you can configure the Monitor Agent to notify you of problem situations peculiar to your GroupWise system.

- 1 Make sure that notification has been properly set up as described in [Section 69.5.1, “Configuring Email Notification,”](#) on page 957.
- 2 On Windows, at the [Monitor Agent server console](#), click *Configuration > Thresholds*.



or

On Linux, at the [Monitor Agent Web console](#), click *Thresholds* on the Status page.



The tabs at the top of the dialog box enable you to create a separate threshold for each type of GroupWise agent.

- 3 Select the type of agent to create a threshold for.
- 4 In the *Expression* field, select a MIB variable.

GroupWise agent MIB files are located in the [/agents/snmpmibs](#) directory of your GroupWise software distribution directory or the downloaded *GroupWise 2012* software image. The MIB files list the meanings of the MIB variables and what type of values they represent. The meaning of the MIB variable selected in the *Expression* field is displayed above the field.

- 5 Select an operator from the drop-down list.
- 6 Type the value to test for.

For example, you might want to test the *mtaOldestQMsg* variable for a specific number of seconds that you consider to be too long for a message to be in the queue.

- 7 In the *State* field, select an existing state.

Icon	State
	Unknown
	Normal
	Informational
	Marginal
	Warning
	Minor
	Major
	Critical

or

Create a new state:

- 7a On Windows, at the [Monitor Agent server console](#), click *Define State*.

or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > States*.

- 7b Type a name for the new state.

- 7c Select a severity level.
- 7d Provide instructions about how to handle the new state.
- 7e Click *Close* to save the new state.
- 8 Click *OK* to create the new threshold.
- 9 Repeat [Step 2](#) through [Step 8](#) for each type of agent that you want to create a customized state for.
- 10 Make sure *Threshold Exceeded* is selected in the *Notification Events* box.
- 11 Click *OK* to save the new notification settings.

69.6 Configuring Audible Notification for Agent Problems

If the server where the Monitor Agent runs is located where someone can respond immediately to a GroupWise agent problem, you can configure the Monitor Agent to produce different sounds according to the nature of the problem.

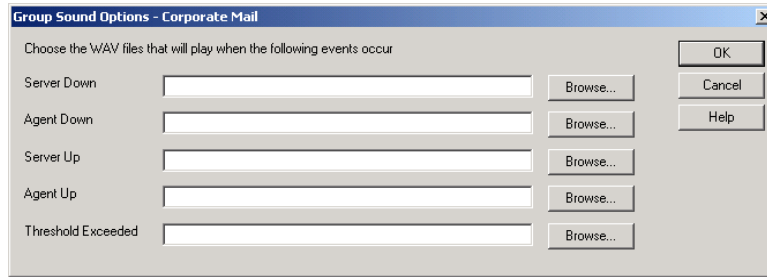
NOTE: Audible notification is not available on Linux.

On Windows, at the [Monitor Agent server console](#):

- 1 Select the root agent group to set up audible notification defaults for all monitored agents.
or
Select any agent group to set up audible notification for the agents in the selected group.
or
Select any agent to set up audible notification for that individual agent.
- 2 Click *Configuration > Notification*.

Unless you selected the root agent group, *Use Parent Notification Options* is selected and all options are dimmed. Deselect *Use Parent Notification Options* to set up notification for an agent group or individual agent.

- 3 Select *Play Sound*, then click *Sounds*.



- 4 For each event, browse to and select a sound file to provide audible notification for each type of event for the selected agent group.

The Monitor Agent launches the default media player for whatever type of sound file you select. Basic sound files are available in the `c:\windows\media` directory.

- 5 Click *OK* to return to the Notification dialog box.
- 6 Select notification events and other notification settings as described in [Section 69.5, "Configuring Email Notification for Agent Problems,"](#) on page 957.
- 7 Click *OK* to save the audible notification settings.

69.7 Configuring SNMP Trap Notification for Agent Problems

The Monitor Agent can throw SNMP traps for use by the Management and Monitoring component of Novell ZENworks for Servers or any other SNMP management and monitoring program.

- 1 On Windows, at the [Monitor Agent server console](#), select the root agent group to set up SNMP trap notification defaults for all monitored agents.
or
Select any agent group to set up SNMP trap notification for the agents in the selected group.
or
Select any agent to set up SNMP trap notification for that individual agent.
then

Click *Configuration > Notification*.

Group Notification - Corporate Mail

Use Parent Notification Options

Notification List

Comma separated list of users to notify

Mail Domain Name

Relay Address

Send SNMP Traps

Play Sound

Notification Events

Agent Down

Server Down

Threshold Exceeded

Minimum threshold level for notification: Unknown

State returns to Normal

Repeat Notification After: 15 minutes

Periodic Monitor Confirmation

Confirm: 1 minutes

Apply options to subgroups

Unless you selected the root agent group, *Use Parent Notification Options* is selected and all options are dimmed. Deselect *Use Parent Notification Options* to set up notification for an agent group or individual agent.

or

On Linux, at the [Monitor Agent Web console](#), select one or more agents, then click *Preferences > Setup* to display the *Notify* settings.

[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)

[Setup](#) | [Custom Views](#) | [States](#) | [Filter](#) | [Add Agents](#) | [Remove Agents](#)

Preferences

Notify

Notification List:

Mail Domain Name:

Relay Address:

Send SNMP Traps:

Trap Targets:

Comma separated list of address:community pairs

Agent Down:

Server Down:

Threshold Exceeded:

Minimum Threshold: Unknown

State returns to Normal:

Notification Repeat Time (minutes): 15

Periodic Notification: 0

NOTE: The *Use Parent Notification Options* and *Apply Options to Subgroups* options are not available on Linux.

- 2 Select *Send SNMP Traps*, then click *OK*.
- 3 Make sure that the Monitor Agent is properly configured for SNMP, as described in [Section 69.3.2, “Configuring the Monitor Agent for SNMP,”](#) on page 955.

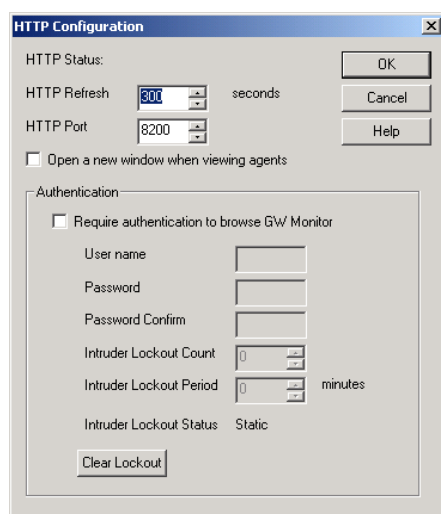
69.8 Configuring Authentication and Intruder Lockout for the Monitor Web Console

Accessing GroupWise agent status information from your Web browser is very convenient. However, you might want to limit access to that information. You can configure the Monitor Agent to request a user name and password before allowing users to access the Monitor Web console. In addition, you can configure the Monitor Agent to detect break-in attempts in the form of repeated unsuccessful logins.

NOTE: To limit access on Linux, use the `--httpmonuser` and `--httpmonpassword` startup switches when you start the Monitor Agent. For more information, see [Chapter 73, “Using Monitor Agent Startup Switches,”](#) on page 1003. The intruder lockout functionality is not available on Linux.

On Windows, at the [Monitor Agent server console](#):

- 1 Click *Configuration > HTTP*.



- 2 In the *Authentication* box, select *Require authentication to browse GW Monitor*.

- 3 Fill in the fields:

User Name: Provide a user name for the Monitor Agent to prompt for when a user attempts to access the Monitor Web console.

Password: Provide a password for the Monitor Agent to prompt for when a user attempts access. Repeat the password in the *Password Confirm* field.

For optimum security for the Monitor Web console, use the `--https` and `--httpcertfile` startup switches, along with a certificate file, when starting the Monitor Agent. For more information, see [Chapter 73, “Using Monitor Agent Startup Switches,”](#) on page 1003. For background information about SSL and how to set it up on your system, see [Section 83.2, “Server Certificates and SSL Encryption,”](#) on page 1107.

Intruder Lockout Count: Specify the number of failed attempts the Monitor Agent should allow before it stops prompting the potentially unauthorized user for a valid user name and password.

Intruder Lockout Period: Specify the number of minutes that must elapse before the user can again attempt to access the Monitor Web console.

If a valid user is locked out of the Monitor Web console, you can use *Clear Lockout* to grant access before the intruder lockout period has elapsed.

- 4 Click *OK* to put the authentication settings into effect.

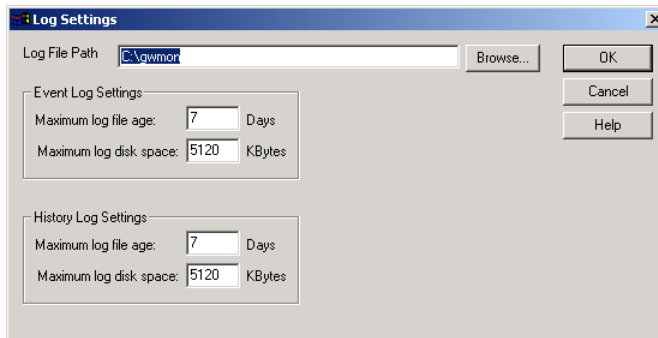
69.9 Configuring Monitor Agent Log Settings

The Monitor Agent writes to two different types of log files:

- ♦ Event log files record error messages, status messages, and other types of event-related messages.
- ♦ History log files record dumps of all MIB values gathered during each poll cycle.

Log files can provide a wealth of information for resolving problems with Monitor Agent functioning or agent monitoring.

- 1 On Windows, at the [Monitor Agent server console](#), click *Log > Log Settings*.



or

On Linux, at the [Monitor Agent Web console](#), click *Log > Log Settings*.

Log Settings		Submit
Max Event Log Age:	7	
Max Event Log Size:	5120	
Max History Log Age:	7	
Max History Log Size:	5120	
Gateway Accounting Log Path:	/var/log/novell/groupwise/gwmon/acct	
Max Accounting Log Age:	7	
Max Accounting Log Size:	10240	

- 2 Fill in the fields:

Log File Path: Specify the full path of the directory where the Monitor Agent writes its log files. The default log file location varies by platform.

Linux: `/var/log/novell/groupwise/monitor/logs`

Windows: `c:\ProgramData\Novell\GroupWise Server\Monitor\logs`

Maximum Event Log File Age: Specify the number of days you want Monitor Agent event log files to remain on disk before being automatically deleted. The default event log file age is 30 days.

Maximum Event Log Disk Space: Specify the maximum amount of disk space for all Monitor event log files. When the specified disk space is used, the Monitor Agent overwrites existing Monitor Agent event log files, starting with the oldest. The default is 102400 KB (100 MB) of disk space for all Monitor Agent event log files.

Maximum History Log File Age: Specify the number of days you want Monitor Agent history log files to remain on disk before being automatically deleted. The default history log file age is 30 days.

Maximum History Log Disk Space: Specify the maximum amount of disk space for all Monitor history log files. When the specified disk space is used, the Monitor Agent overwrites existing Monitor Agent history log files, starting with the oldest. The default is 102400 KB (100 MB) of disk space for all Monitor Agent history log files.

- 3 Click *OK* to put the new log settings into effect.
- 4 To view existing event logs, click *View > View Log Files*.
- 5 To view existing history log files, click *Log > View History Files*.

69.10 Configuring Proxy Service Support for the Monitor Web Console

The [Monitor Web console](#) provides links to the agent Web consoles. Although you can access the Monitor Web console from outside your firewall, by default you cannot access the agent Web consoles from outside your firewall. To enable the Monitor Web console to display the agent Web consoles from outside your firewall, you need to enable the Monitor Agent to support proxy service.

- 1 In a text editor, open the Monitor Application configuration file ([gwmonitor.cfg](#))
- 2 Locate the following line:

```
Provider.GWMP.Agent.Http.level=basic
```

- 3 Change it to:

```
Provider.GWMP.Agent.Http.level=full
```

The basic setting restricts use of the Monitor Web console to within a firewall, while the full setting allows use of the Web console both inside and outside a firewall. A third setting, none, disables use of the Web console.

- 4 Save and exit the Monitor Application configuration file.
- 5 Start the Monitor Agent with the `--proxy` startup switch.

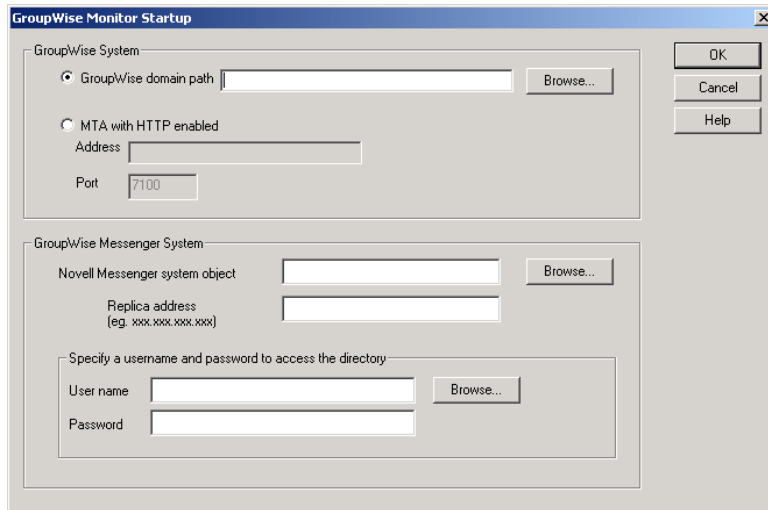
For information about startup switches, see [Chapter 73, "Using Monitor Agent Startup Switches," on page 1003](#).

Without proxy service support enabled, the Monitor Web console communicates directly with the GroupWise agent after it gets a GroupWise agent's address from the Monitor Agent. This process, however, does not work when communicating through a firewall.

With proxy service support enabled, all communication is routed through the Monitor Agent and Monitor Application (on the Web server). As long as the Web server can be accessed through the firewall, the Monitor Web console can receive information about all GroupWise agents that the Monitor Agent knows about.

69.11 Monitoring Messenger Agents

Monitor can be used to monitor Messenger agents as well as GroupWise agents. In fact, Monitor can be used independently to monitor Messenger Agents. If you start Monitor with no access to the GroupWise system, you are prompted for the information Monitor needs in order to start monitoring Messenger agents.

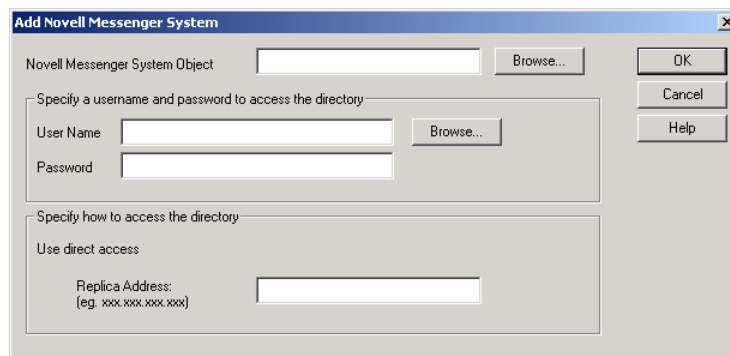


The screenshot shows the "GroupWise Monitor Startup" dialog box. It is divided into two main sections. The first section, "GroupWise System", has two radio buttons: "GroupWise domain path" (selected) and "MTA with HTTP enabled". The "GroupWise domain path" section includes a text box and a "Browse..." button. The "MTA with HTTP enabled" section includes "Address" and "Port" (set to 7100) text boxes. The second section, "GroupWise Messenger System", includes a "Novell Messenger system object" text box with a "Browse..." button, a "Replica address" text box (with a note "eg. xxx.xxx.xxx.xxx"), and a sub-section "Specify a username and password to access the directory" containing "User name" and "Password" text boxes with a "Browse..." button. On the right side, there are "OK", "Cancel", and "Help" buttons.

To make this information a permanent part of your independent Messenger system, follow the instructions in "Using GroupWise Monitor" in "Managing the Messaging Agent" in the *Novell Messenger 2.2 Administration Guide*.

If Monitor is already monitoring GroupWise agents, then it is easy to add Messenger agents.

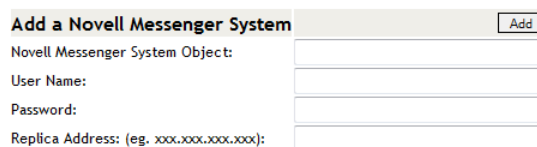
- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > Add Novell Messenger System*.



The screenshot shows the "Add Novell Messenger System" dialog box. It includes a "Novell Messenger System Object" text box with a "Browse..." button. Below this is a section "Specify a username and password to access the directory" with "User Name" and "Password" text boxes and a "Browse..." button. The bottom section, "Specify how to access the directory", has a "Use direct access" checkbox and a "Replica Address" text box (with a note "eg. xxx.xxx.xxx.xxx"). On the right side, there are "OK", "Cancel", and "Help" buttons.

OR

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Add Agents*.



The screenshot shows a web form titled "Add a Novell Messenger System" with an "Add" button. The form contains four input fields: "Novell Messenger System Object:", "User Name:", "Password:", and "Replica Address: (eg. xxx.xxx.xxx.xxx):".

- 2 Fill in the following fields in the GroupWise Monitor Startup dialog box or the Add Novell Messenger System dialog box:
 - Novell Messenger System Object:** Browse to and select the eDirectory container where you created the Messenger system.
 - User Name:** Browse to and select a User object that has sufficient rights to enable the Monitor Agent to access Messenger object properties in eDirectory.
 - Password:** Specify the network password associated with the User object.
 - Replica Address:** Specify the IP address of a server where an eDirectory replica is available.
- 3 Click *OK* to add the Messenger Agent and the Archive Agent to the list of monitored agents.

69.12 Supporting the GroupWise High Availability Service on Linux

The GroupWise High Availability service, described in “[Enabling the GroupWise High Availability Service for the Linux GroupWise Agents](#)” in “[Installing GroupWise Agents](#)” in the *GroupWise 2012 Installation Guide*, relies on the Monitor Agent to know when an agent has stopped and needs to be restarted. To enable communication between the Monitor Agent and the High Availability service, start the Monitor Agent with the `--hauser` and `--hapassword` startup switches, set to the user name and password of the Linux user you set up to represent the High Availability service on your Linux server. You can also use the `--hapoll` startup switch to control how often the Monitor Agent contacts the High Availability service with agent status information. The default is every 2 minutes.

The GroupWise High Availability server does not require that the Monitor Application is installed.

70 Configuring the Monitor Application

During installation, the GroupWise Monitor Application is set up with a default configuration. However, you can use the information in the following sections to optimize the Monitor Application configuration:

- ♦ [Section 70.1, “Editing the gwmonitor.cfg File,” on page 969](#)
- ♦ [Section 70.2, “Setting the Timeout Interval for Inactive Sessions,” on page 969](#)
- ♦ [Section 70.3, “Adjusting Session Security,” on page 970](#)
- ♦ [Section 70.4, “Accommodating Single Sign-On Products,” on page 970](#)
- ♦ [Section 70.5, “Configuring Monitor Application Log Settings,” on page 971](#)
- ♦ [Section 70.6, “Putting the Monitor Configuration Changes into Effect,” on page 972](#)

70.1 Editing the gwmonitor.cfg File

The location of the `gwmonitor.cfg` file varies by platform:

Linux: `/var/opt/novell/groupwise/monitor`

Windows: `c:\Novell\GroupWise\monitor`

You can use any ASCII text edit that you prefer to edit the `gwmonitor.cfg` file.

IMPORTANT: We strongly recommended that you do not modify any settings that are not documented in the following sections.

70.2 Setting the Timeout Interval for Inactive Sessions

By default, administrators are logged out of the Monitor Web console after 20 minutes if they have not performed any actions that generate requests. Actions such as polling agents for current status and running reports generate requests. Other actions, such as changing the view of existing information, and reading Help topics, do not generate requests.

The timeout interval provides security for GroupWise administrators who forget to log out of the Monitor Web console. It also helps the performance of the Web server by freeing the resources dedicated to that administrator’s connection.

To adjust the timeout interval:

- 1 Open the `gwmonitor.cfg` file in a text editor.
- 2 Search to find the following line:

```
Security.timeout=20
```

- 3 Change the default of 20 to the number of minutes that you prefer for the timeout interval.
- 4 Save the `gwmonitor.cfg` file.
- 5 Skip to [Section 70.6, “Putting the Monitor Configuration Changes into Effect,”](#) on page 972.

70.3 Adjusting Session Security

By default, the Monitor Application uses the Web browser IP address of the Monitor user to confirm that, during the same session, it is always communicating with the same user. This is the highest form of security and works well for users on desktop workstations. However, for laptops and mobile devices that are carried to different places, possibly from one network segment to another, this level of security can cause interruptions in user sessions.

Other Monitor Application security features such as session cookies provide excellent security, even without the IP address checking. If you have multiple GroupWise administrators who check GroupWise status from various locations, you can turn off the need for confirming the Web browser IP address to make the Monitor Web consoles more stable for these mobile administrators.

To disable IP address checking:

- 1 Open the `gwmonitor.cfg` file in a text editor.
- 2 Search to find the following line:

```
Security.UseClientIP.enable=
```
- 3 Change `true` to `false`.
- 4 Save the `gwmonitor.cfg` file.
- 5 Skip to [Section 70.6, “Putting the Monitor Configuration Changes into Effect,”](#) on page 972.

70.4 Accommodating Single Sign-On Products

Some organizations choose to place a single sign-on product such as [Novell Identity Manager \(http://www.novell.com/products/identitymanager\)](http://www.novell.com/products/identitymanager) between users on the Web and the applications they access that are running behind the organization's firewall. If you use a single sign-on product with GroupWise Monitor, you must configure the Monitor Application to accommodate the single sign-on product.

- 1 Open the `gwmonitor.cfg` file in a text editor.
- 2 Search to find the following line:

```
#Cookie.domain=.novell.com
```
- 3 Remove the pound sign (#) to activate the setting.
- 4 Replace `.novell.com` with the part of your organization's Internet domain name that is common between the single sign-on product and the Web server where the Monitor Application is installed.

For example, if the IDM server is at `idm.novell.com` and the Monitor Application is at `monitor.novell.com`, the domain name used to create cookies would be `.novell.com`, so that the cookies are accepted by both servers.
- 5 Save the `gwmonitor.cfg` file.
- 6 Skip to [Section 70.6, “Putting the Monitor Configuration Changes into Effect,”](#) on page 972.

70.5 Configuring Monitor Application Log Settings

Error messages and other information about Monitor Application functioning are written to log files. Log files can provide a wealth of information for resolving problems with Monitor Application functioning. Logging is enabled by default.

- ◆ [Section 70.5.1, “Locating Monitor Application Log Files,” on page 971](#)
- ◆ [Section 70.5.2, “Configuring Monitor Application Log Settings,” on page 971](#)
- ◆ [Section 70.5.3, “Viewing Monitor Application Log Files,” on page 971](#)

70.5.1 Locating Monitor Application Log Files

The default location of the Monitor Application log files is the [GroupWise Web application working directory](#).

You can change the location where the Monitor Application creates its log files, as described in [Configuring WebAccess Application Log Settings](#).

70.5.2 Configuring Monitor Application Log Settings

- 1 Open the [gwmonitor.cfg](#) file in a text editor.
- 2 Search to find the Logging Information section.
- 3 Adjust the following log settings as needed:

Log.maxSize: Specify the maximum amount of disk space you want to use for Monitor Application log files. If the disk space limit is exceeded, the Monitor Application deletes log files, beginning with the oldest file, until the limit is no longer exceeded. The default disk space is 102400 KB (100 MB).

Log.maxAge: Specify the number of days you want to retain the log files. The Monitor Application retains log files for the specified number of days unless the maximum disk space for the log files is exceeded. The default age is 30 days.

Log.level: There are three log levels:

- ◆ **Normal (default)** Displays warnings and errors.
- ◆ **Verbose:** Displays the Normal log level information, plus information messages and user requests.
- ◆ **Diagnostic:** Displays all possible information. Use Diagnostic only if you are troubleshooting a problem with the Monitor Application.

The Verbose and Diagnostic log levels do not degrade Monitor Application performance, but log files consume more disk space when Verbose or Diagnostic logging is in use.

- 4 Save the [gwmonitor.cfg](#) file.
- 5 Skip to [Section 70.6, “Putting the Monitor Configuration Changes into Effect,” on page 972](#).

70.5.3 Viewing Monitor Application Log Files

For the default location of the Monitor log files, see [Section 63.2.1, “Locating WebAccess Application Log Files,” on page 918](#).

When logging is turned on, the Monitor Application creates a new log file each day and each time it is restarted (as part of the Web server startup). Therefore, you find multiple log files in the log file directory. The first four characters represent the date (*mmdd*). The next three characters identify the

Monitor Application (mon). A three-digit extension allows for multiple log files created on the same day. For example, a log file named 0518mon.001 indicates that it is a Monitor Application log file, created on May 18.

Use your text editor of choice to view the Monitor Application log files.

70.6 Putting the Monitor Configuration Changes into Effect

- ♦ [Section 70.6.1, “Accepting the Default Time Interval,” on page 972](#)
- ♦ [Section 70.6.2, “Changing the Default Time Interval,” on page 972](#)
- ♦ [Section 70.6.3, “Immediately Putting the Configuration Changes into Effect,” on page 972](#)

70.6.1 Accepting the Default Time Interval

By default, the Monitor Application checks the `gwmonitor.cfg` file for changes every 10 minutes. When it finds changes, it puts the changes into effect without restarting Tomcat. If you are satisfied to have your changes put into effect within this time interval, no action is required on your part after you edit the `gwmonitor.cfg` file.

70.6.2 Changing the Default Time Interval

You can change the time interval at which the Monitor Application checks the `gwmonitor.cfg` file for changes.

- 1 Open the [gwmonitor.cfg file](#) in a text editor.
- 2 Search to find the following line:

```
Config.Update.check=10
```
- 3 Change 10 to the number of minutes Monitor Application to wait before checking for changes to its configuration file
- 4 Save the `gwmonitor.cfg` file.

70.6.3 Immediately Putting the Configuration Changes into Effect

You can manually restart Tomcat in order to immediately put the changes into effect.

OES 11:

```
rcnovell-tomcat6 stop  
rcnovell-tomcat6 start
```

OES 2 Linux:

```
rcnovell-tomcat5 stop  
rcnovell-tomcat5 start
```

SLES 11:

```
rctomcat6 stop  
rctomcat6 start
```

SLES 10:

```
rctomcat5 stop  
rctomcat5 start
```

- Windows:
1. At the Windows server, click *Start > Administrative Tools > Services*.
 2. Right-click *Tomcat 6*, then click *Restart*.

71 Using GroupWise Monitor

For a review of the three Monitor Agent consoles, see [Section 68, “Understanding the Monitor Agent Consoles,”](#) on page 941. This section focuses on using the Windows Monitor Agent server console and the Monitor Agent Web console, although many of these tasks can also be performed at the Monitor Web console.

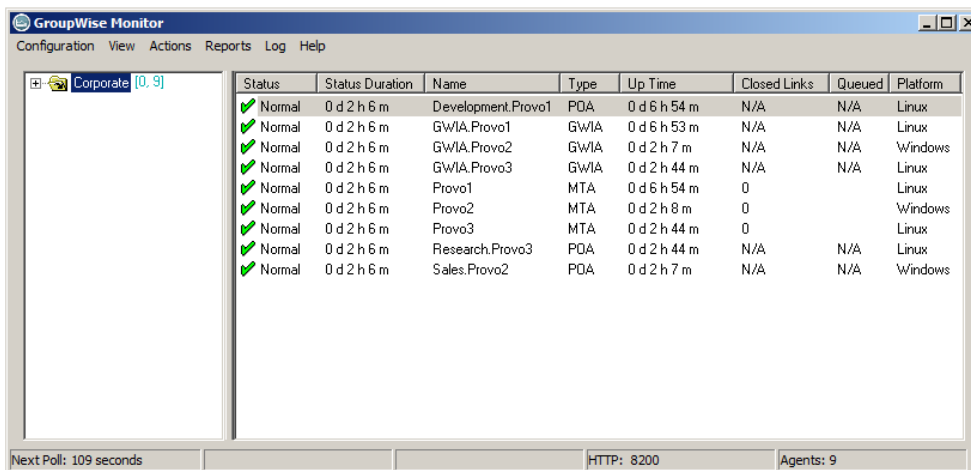
The GroupWise Windows Monitor Agent server console displays GroupWise agent status on the server where the Monitor Agent runs. On Linux, similar information can be displayed at the Monitor Agent Web console.

- [Section 71.1, “Using the Windows Monitor Agent Server Console,”](#) on page 973
- [Section 71.2, “Using the Monitor Web Console,”](#) on page 977
- [Section 71.3, “Generating Reports,”](#) on page 979
- [Section 71.4, “Measuring Agent Performance,”](#) on page 989
- [Section 71.5, “Collecting Gateway Accounting Data,”](#) on page 992
- [Section 71.6, “Assigning Responsibility for Specific Agents,”](#) on page 998
- [Section 71.7, “Searching for Agents,”](#) on page 999

71.1 Using the Windows Monitor Agent Server Console

Initially, the Windows Monitor Agent server console lists all monitored GroupWise agents, along with their statuses.

NOTE: On Windows, agents and agent groups are displayed at the [Monitor Agent server console](#). On Linux, similar functionality is available at the [Monitor Agent Web console](#).

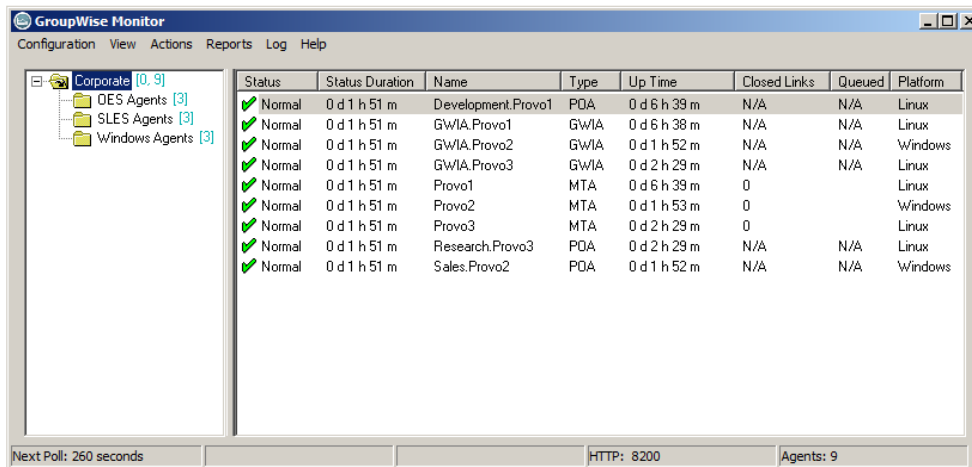


The screenshot shows the GroupWise Monitor application window. The title bar reads "GroupWise Monitor" and the menu bar includes "Configuration", "View", "Actions", "Reports", "Log", and "Help". On the left, a tree view shows a folder named "Corporate" with a sub-item "[0. 9]". The main area displays a table of agent information:

Status	Status Duration	Name	Type	Up Time	Closed Links	Queued	Platform
✓ Normal	0 d 2 h 6 m	Development.Provo1	PDA	0 d 6 h 54 m	N/A	N/A	Linux
✓ Normal	0 d 2 h 6 m	GWIA.Provo1	GWIA	0 d 6 h 53 m	N/A	N/A	Linux
✓ Normal	0 d 2 h 6 m	GWIA.Provo2	GWIA	0 d 2 h 7 m	N/A	N/A	Windows
✓ Normal	0 d 2 h 6 m	GWIA.Provo3	GWIA	0 d 2 h 44 m	N/A	N/A	Linux
✓ Normal	0 d 2 h 6 m	Provo1	MTA	0 d 6 h 54 m	0		Linux
✓ Normal	0 d 2 h 6 m	Provo2	MTA	0 d 2 h 8 m	0		Windows
✓ Normal	0 d 2 h 6 m	Provo3	MTA	0 d 2 h 44 m	0		Linux
✓ Normal	0 d 2 h 6 m	Research.Provo3	PDA	0 d 2 h 44 m	N/A	N/A	Linux
✓ Normal	0 d 2 h 6 m	Sales.Provo2	PDA	0 d 2 h 7 m	N/A	N/A	Windows

At the bottom of the window, there are three status indicators: "Next Poll: 109 seconds", "HTTP: 8200", and "Agents: 9".

After you create agent groups, as described in [Section 69.2, “Creating and Managing Agent Groups,”](#) on page 949, the agents in each group are displayed when you select a group.



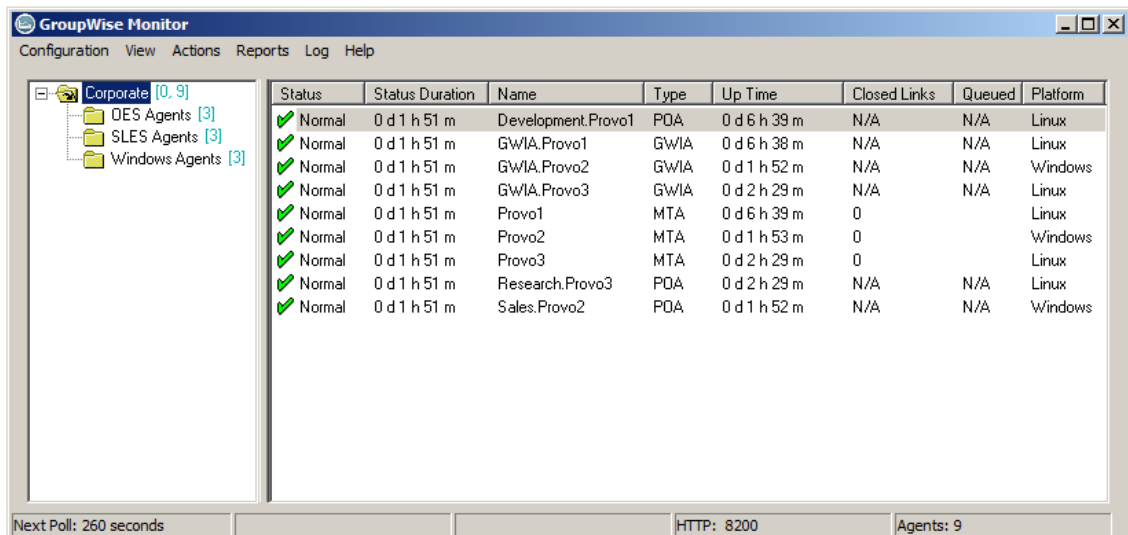
You can display many types of monitoring information at the Windows Monitor Agent server console.

- ◆ [Section 71.1.1, “Viewing All Agents,”](#) on page 974
- ◆ [Section 71.1.2, “Viewing Problem Agents,”](#) on page 975
- ◆ [Section 71.1.3, “Viewing a Windows Agent Server Console,”](#) on page 975
- ◆ [Section 71.1.4, “Viewing an Agent Web Console,”](#) on page 976
- ◆ [Section 71.1.5, “Polling the Agents for Updated Status Information,”](#) on page 977

71.1.1 Viewing All Agents

After you have separated your agents into groups, you can still view all agents in your GroupWise system in a single list.

- 1 On Windows, at the [Monitor Agent server console](#), right-click the root agent group, then click *Show Subgroup Agents*.



or

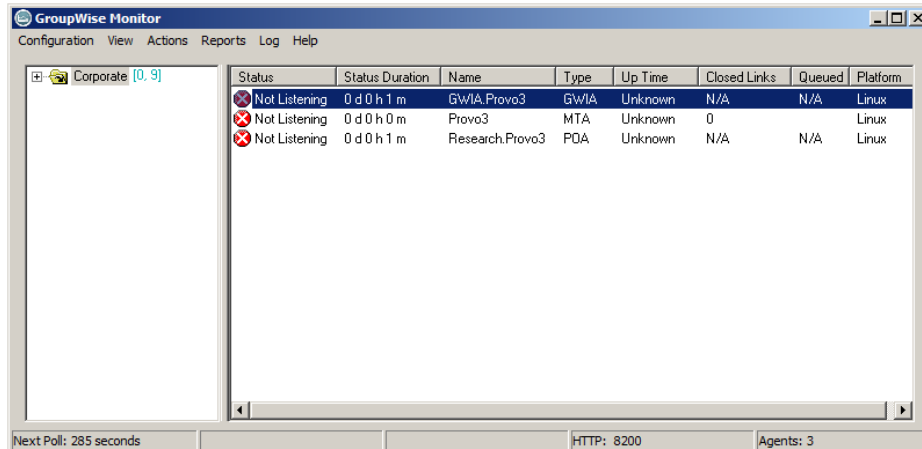
On Linux, at the [Monitor Agent Web console](#), click the root agent group, then click *Show Subgroup Agents*.

You can use the *Show Subgroup Agents* feature on any group that contains nested subgroups.

71.1.2 Viewing Problem Agents

In a single agent group or in a group with subgroups shown, you can filter the list to show only those agents whose status is not Normal.

- 1 On Windows, at the [Monitor Agent server console](#), click *View > Problem Agents*.



or

On Linux, at the [Monitor Agent Web console](#), click *Problems*.

Only problem agents are now displayed. If you leave the Monitor Agent with only problem agents displayed, many groups might appear empty because all agents have a status of *Normal*.

- 2 On Windows, to view all monitored agents again, click *View > All Agents*.

or

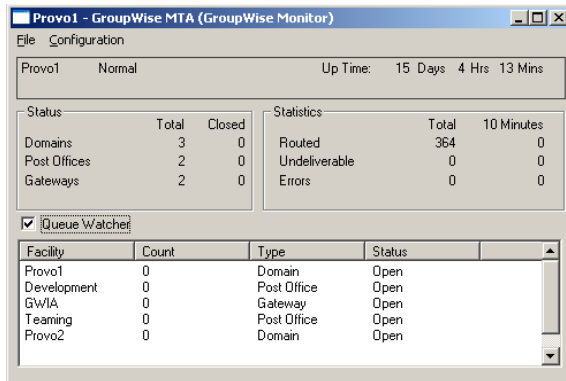
On Linux, click *System*.

71.1.3 Viewing a Windows Agent Server Console

An active agent server console displays on each server where a Windows GroupWise agent is running. You can display a similar agent server console from the Windows [Monitor Agent server console](#).

NOTE: This feature is not available on Linux.

- 1 Right-click an agent, then click *Agent Console*.



You cannot control the agent from the Monitor Agent as you can at the actual agent server console, but you can gather status information about the monitored agent.

71.1.4 Viewing an Agent Web Console

An agent Web console can be displayed anywhere you have access to a Web browser and the Internet.

- 1 On Windows, at the [Monitor Agent server console](#), right-click an agent, then click *Agent Web Console*.

or

On Linux, at the [Monitor Agent server console](#), click the domain or post office link.

	Total
C/S Users	1
Application Connections	2
Physical Connections	0
SOAP Sessions	0
Priority Queues	0
Normal Queues	0
GWCheck Auto Queues	0
GWCheck Scheduled Queues	0

	Total	Busy
C/S Handler Threads	10	0
Message Worker Threads	6	0
GWCheck Worker Threads	4	0
SOAP Threads	3	0
Calendar Publishing Threads	3	0
Message Transfer Status	Open	

	Total
C/S Requests	3682
C/S Requests Pending	0
Users Timed Out	4
SOAP Requests	21
SOAP Pending Requests	0
GWEvents	0
Calendar Publishing Requests	8
Rules Executed	0
Users Delivered	0
Message Files Processed	20

For information about the agent Web consoles, see the GroupWise agent documentation:

- ♦ [Section 37.2, “Using the POA Web Console,” on page 539](#)
- ♦ [Section 43.2, “Using the MTA Web Console,” on page 669](#)
- ♦ [Section 49.2, “Using the DVA Web Console,” on page 725](#)
- ♦ [Section 56.2, “Using the GWIA Web Console,” on page 827](#)


71.1.5 Polling the Agents for Updated Status Information

By default, the Monitor Agent polls the monitored agents every five minutes. You can change the default poll cycle, as described in [Section 69.4, “Configuring Polling of Monitored Agents,” on page 956](#). The time remaining until the next poll cycle is displayed in the lower left corner of the [Monitor Agent server console](#).

You can also manually poll monitored agents.

On Windows, at the [Monitor Agent server console](#):


- ♦ To poll all agents, click *Action > Poll All Agents*.
- ♦ To poll a specific agent, right-click the agent, then click *Poll Agent*.
- ♦ To stop polling a specific agent (for example, because the server it runs on is awaiting repairs), right-click the agent, then click *Suspend Polling*. You can specify a time interval for the agent to be suspended, after which polling resumes automatically. By suspending polling, you prevent repeat notifications for a problem that is already being addressed.

The suspended agent’s status is listed as *Suspended*, accompanied by the same icon used for the Unknown status .

- ♦ To restart regular polling of an agent for which polling was suspended, right-click the agent, then click *Resume Polling*.

On Linux, at the [Monitor Agent server console](#):

- ♦ To poll all agents, select all agents, then click *Poll*.
- ♦ To poll a specific agent, select the agent, then click *Poll*.
- ♦ To stop polling a specific agent, select the agent, then click *Suspend*. You can specify a time interval for the agent to be suspended, after which polling resumes automatically. By suspending polling, you prevent repeat notifications for a problem that is already being addressed.

The suspended agent’s status is listed as *Suspended*, accompanied by the same icon used for the Unknown status .

- ♦ To restart regular polling of an agent for which polling was suspended, select the agent, then click *Resume*.

71.2 Using the Monitor Web Console

The Monitor Web console lists all GroupWise agents that the Monitor agent is polling for status information. Use the following URL to access the Monitor Web console:

`http://web_server_address/gwmon/gwmonitor`

where *web_server_address* represents the IP address or hostname of the Web server where the Monitor Application is installed.

GroupWise® Monitor

Novell

Monitored agents for "Corporate" group
Total: 9 Displayed: 1 - 9

Refresh Hide Subgroup Agents Problem Suspend Resume Move Options Thresholds Help

<input type="checkbox"/>	Name	Status	Status Duration	Up Time	Type	Version	Platform
<input type="checkbox"/>	Provo1	Normal	0 d 1 h 54 m	0 d 6 h 39 m	MTA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	Development.Provo1	Normal	0 d 1 h 54 m	0 d 6 h 39 m	POA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	GWIA.Provo1	Normal	0 d 1 h 54 m	0 d 6 h 38 m	GWIA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	Provo3	Normal	0 d 1 h 54 m	0 d 2 h 29 m	MTA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	GWIA.Provo3	Normal	0 d 1 h 54 m	0 d 2 h 29 m	GWIA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	Research.Provo3	Normal	0 d 1 h 54 m	0 d 2 h 29 m	POA	12.0.0 (12/03/2011)	Linux
<input type="checkbox"/>	Provo2	Normal	0 d 1 h 54 m	0 d 1 h 53 m	MTA	12.0.0 (12/3/2011)	Windows
<input type="checkbox"/>	GWIA.Provo2	Normal	0 d 1 h 54 m	0 d 1 h 52 m	GWIA	12.0.0 (12-03-11)	Windows
<input type="checkbox"/>	Sales.Provo2	Normal	0 d 1 h 54 m	0 d 1 h 52 m	POA	12.0.0 (12/3/2011)	Windows

Global features of the Monitor Web console are available on icon buttons at the top of the Monitor page.

Icon Button	Feature
	Problem
	Link Trace
	Link Configuration
	Global Options
	States
	Search

Click the *Problem* icon button to display only agents in your GroupWise system whose status is other than *Normal*. Click the name of your GroupWise system to display all agents again.

Click the status of an agent in the *Status* column to display agent status details.

Click an agent in the *Name* column to open its agent Web console. For information about the agent Web consoles, see [Section 71.1.4, "Viewing an Agent Web Console," on page 976](#).

Click an agent group in the left panel to display all monitored agents in the group. Click the *Problem* button above the agent list to display only those agents whose status is other than *Normal* in the agent group. The *Problem* button then changes to *Monitored*. Click the *Monitored* button to include working agents as well as problem agents in the list.

Click *Refresh* to update the agent status information. To modify the default poll cycle, see [Section 69.4, "Configuring Polling of Monitored Agents," on page 956](#).

To see what specific tasks can be performed at the Monitor Web console, see [Chapter 72, "Comparing the Monitor Consoles," on page 1001](#).

71.3 Generating Reports

You can generate reports on demand at the Monitor Agent consoles to help you manage message flow throughout your GroupWise system.

- ♦ [Section 71.3.1, “Link Trace Report,” on page 979](#)
- ♦ [Section 71.3.2, “Link Configuration Report,” on page 980](#)
- ♦ [Section 71.3.3, “Image Map Report,” on page 981](#)
- ♦ [Section 71.3.4, “Environment Report,” on page 986](#)
- ♦ [Section 71.3.5, “User Traffic Report,” on page 986](#)
- ♦ [Section 71.3.6, “Link Traffic Report,” on page 987](#)
- ♦ [Section 71.3.7, “Message Tracking Report,” on page 987](#)
- ♦ [Section 71.3.8, “Performance Testing Report,” on page 988](#)
- ♦ [Section 71.3.9, “Connected User Report,” on page 988](#)
- ♦ [Section 71.3.10, “Gateway Accounting Report,” on page 988](#)
- ♦ [Section 71.3.11, “Trends Report,” on page 988](#)
- ♦ [Section 71.3.12, “Down Time Report,” on page 989](#)

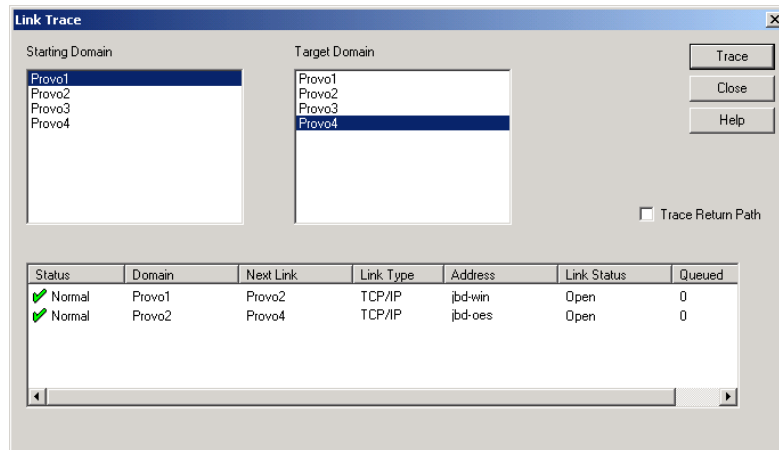
71.3.1 Link Trace Report

A link trace report enables you to follow the path a message would take between two GroupWise domains. A link trace report includes a list of all the domains through which a message would need to pass, along with their current status, link type, address, and number of messages currently queued in each domain. If any domain along the link path is closed, an error message is displayed.

If a message fails to arrive at its destination, this report can help you pinpoint its current location, so you can resolve the problem and get messages flowing smoothly again.

- 1 On Windows, at the [Monitor Agent server console](#), click *Reports > Link Trace*.
or
On Linux, at the [Monitor Agent Web console](#), click *Link Trace*.
- 2 Select a starting domain and a target domain.
- 3 If you want to trace the path back, which is the route status messages will take, select *Trace Return Path*.

- 4 Click *Trace*.



If any domain in the path is closed, an error message displays so you know where the problem is occurring.

- 5 When you are finished tracing links, click *Close*.

71.3.2 Link Configuration Report

A link configuration report enables you to list the links from one or more GroupWise domains to all other domains in your GroupWise system. This helps you identify inefficient link paths, loops, and unreachable domains. All domains must be open to obtain an accurate link map of your GroupWise system.

- 1 Make sure all domains in your GroupWise system are open.

You cannot obtain an accurate link map of your GroupWise system if any domains are closed. For assistance with closed domains, see [“Message Transfer Agent Problems”](#) in *GroupWise 2012 Troubleshooting 2: Solutions to Common Problems*.

- 2 On Windows, at the [Monitor Agent server console](#), click *Reports > Link Configuration*.

or

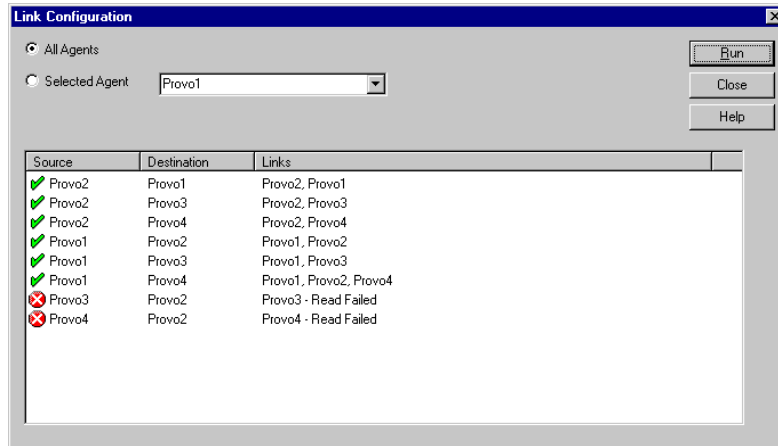
On Linux, at the [Monitor Agent Web console](#), click *Link Configuration*.

- 3 Select *All Agents*

or

Select *Selected Agent* and select a specific agent from the drop-down list.

4 Click *Run*.



The list shows what domains a message would pass through to travel from the domain in the *Source* column to the domain in the *Destination* column. If a domain displays as closed, it means that the Monitor Agent could not contact the MTA for the domain or that a loop was detected in the link configuration.

5 When you are finished checking links, click *Close*.

71.3.3 Image Map Report

An image map enables you to create a visual picture of your GroupWise system, whether it resides in a single office building or spans the globe. You provide the maps; Monitor provides the up-to-the-minute status information at a glance.

- ♦ [“Making Maps Available in Monitor” on page 981](#)
- ♦ [“Setting Up Maps” on page 982](#)
- ♦ [“Setting Up Regions” on page 983](#)
- ♦ [“Adding Agents to a Map” on page 984](#)
- ♦ [“Using an Image Map to Monitor Agents” on page 985](#)

NOTE: The image map report cannot be generated at the Windows [Monitor Agent server console](#). You must use the [Monitor Agent Web console](#).

Making Maps Available in Monitor

1 Obtain useful maps from the Internet or another location.

You can use maps that vary in detail. For example, you could have one map the focuses on a particular corporate office building, another that shows offices throughout your country, and another that shows offices throughout the world. You can select from images in PNG and JPG format.

2 Copy the maps you want to use into the maps subdirectory of the monwork directory.

The default location of the monwork directory varies by platform.

Linux: /tmp/gwmon/monwork/maps

Windows: c:\ProgramData\Novell\GroupWise Server\Monitor\monwork\maps

You can change the location using the `--monwork` startup switch. For more information, see [Chapter 73, "Using Monitor Agent Startup Switches," on page 1003](#)

- 3 Continue with [Setting Up Maps](#).

Setting Up Maps

- 1 At the [Monitor Agent Web console](#), click *Map*.

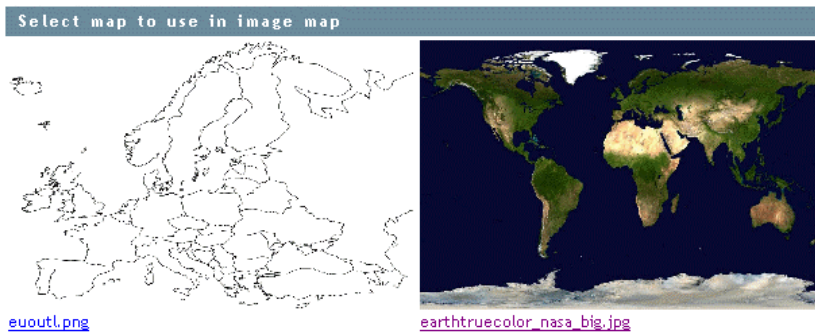
[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)



Initially, no maps are available in Monitor.

- 2 Click *New* to display all the maps that are available in the maps directory.

[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)



The file name of each map is displayed below it.

- 3 Click the map that you want to set up, specify a custom name for the map, then click *Create*.



This makes the map available for use in Monitor.

- 4 To set up additional maps for use in Monitor, click *Done* to return to the Image Map Selection menu, then repeat [Step 2](#) and [Step 3](#) for each map that is available in the maps directory to make it available in Monitor.
- 5 If you want to make one or more smaller-scale maps available from a large-scale map, continue with [“Setting Up Regions” on page 983](#).

or

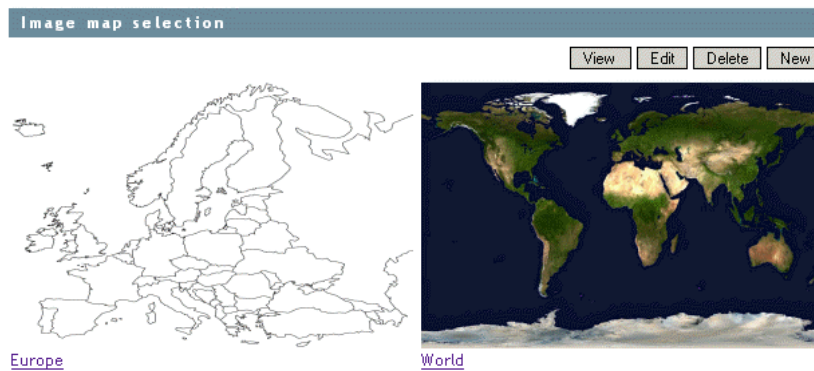
If your maps are all independent from each other, skip to [“Adding Agents to a Map” on page 984](#).

Setting Up Regions

If some of your maps are subsets of other maps, you can set up a large-scale map so that it links to one or more smaller-scale maps. For example, a map of the world could have a region for each continent or country, or a map of a city or country could have a region for each office where GroupWise domains or post offices are located.

- 1 Set up at least two maps in Monitor, as described in [“Making Maps Available in Monitor” on page 981](#).
- 2 At the [Monitor Agent Web console](#), click *Map* to display the maps that are available in Monitor.

[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)



The custom name of each map is displayed below it.

- 3 Click *Edit*, then click a large-scale map.
- 4 In the drop-down list, scroll down through the agents, click the smaller-scale map that you want to define as a region, then click on the large-scale map to refresh the view.
- 5 Click points on the map to surround the region.



- 6 Click *Done* to define the region.

With a very wide map, you need to scroll horizontally to display the *Done* button. The region appears labeled on the large-scale map.



- 7 To define more regions on the large-scale map, click *Done* to return to the available maps, then repeat [Step 3](#) through [Step 6](#) for each region.

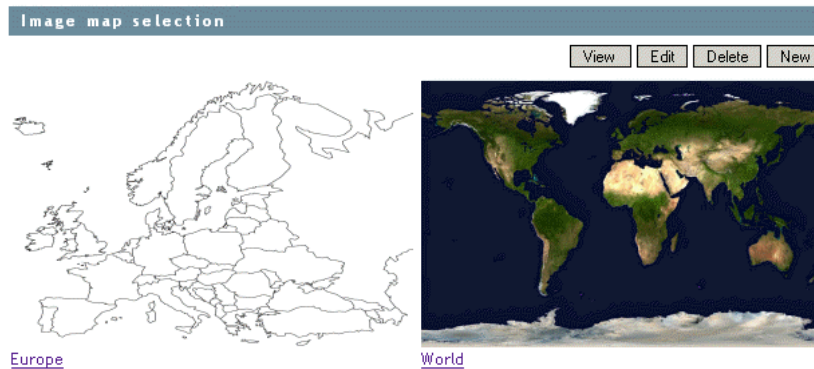
or

To place agents on a map, continue with [Adding Agents to a Map](#).

Adding Agents to a Map

- 1 At the [Monitor Agent Web console](#), click *Map* to display the maps that are available in Monitor.

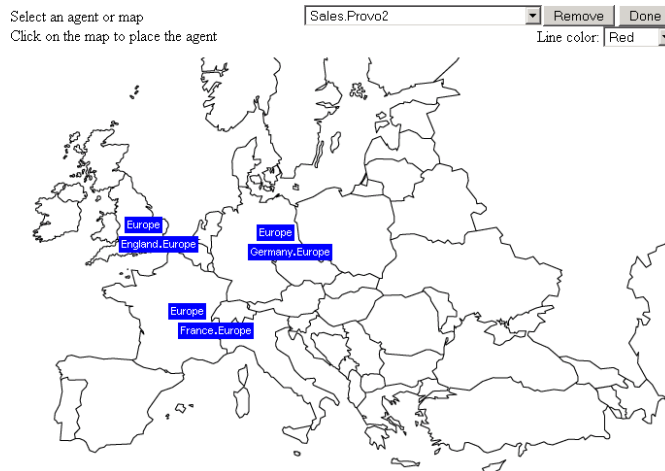
[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)



The custom name of each map is displayed below it.

- 2 Click *Edit*, then click the map where you want to add agents.
- 3 Select an agent in the drop-down list, then click the place on the map where that agent is located. The agent name appears in a blue box.

4 Select additional agents and locations as needed.



5 In the *Line Color* drop-down list, select the color to use to show links between locations.

Make sure you select a color that shows up well on the particular map. Lines display on the map only when links between locations are down.

6 Click *Done* when the map includes all the needed GroupWise agents in their respective locations.

7 Continue with [Using an Image Map to Monitor Agents](#).

Using an Image Map to Monitor Agents

1 At the [Monitor Agent Web console](#), click *Map > View*.

2 Click a map to view agent status.

or

If the map has regions, click a region to display the map that has agent status for that region.



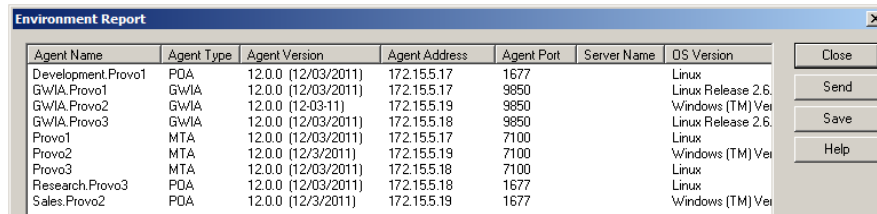
At this point, the Monitor Agent checks the status of each agent on the map. Any agent that is down or that has a status of *Major*, *Critical*, or *Warning* displays in red on the map. Agents with a lower status do not display on the map. If a link between agents is down, a line displays between the agents.

71.3.4 Environment Report

An environment report lists all monitored agents, along with each agent's location, version, IP address, port number, and operating system information.

At the Windows [Monitor Agent server console](#) or the [Monitor Agent Web console](#):

- 1 Click *Reports > Environment*.



Agent Name	Agent Type	Agent Version	Agent Address	Agent Port	Server Name	OS Version
Development.Provo1	POA	12.0.0 (12/03/2011)	172.15.5.17	1677		Linux
GWIA.Provo1	GWIA	12.0.0 (12/03/2011)	172.15.5.17	9850		Linux Release 2.6.
GWIA.Provo2	GWIA	12.0.0 (12/03/11)	172.15.5.19	9850		Windows (TM) Ver
GWIA.Provo3	GWIA	12.0.0 (12/03/2011)	172.15.5.18	9850		Linux Release 2.6.
Provo1	MTA	12.0.0 (12/03/2011)	172.15.5.17	7100		Linux
Provo2	MTA	12.0.0 (12/3/2011)	172.15.5.19	7100		Windows (TM) Ver
Provo3	MTA	12.0.0 (12/03/2011)	172.15.5.18	7100		Linux
Research.Provo3	POA	12.0.0 (12/03/2011)	172.15.5.18	1677		Linux
Sales.Provo2	POA	12.0.0 (12/3/2011)	172.15.5.19	1677		Windows (TM) Ver

- 2 Scroll through the displayed information for your own use.

or

Click *Send*, type your email address, type one or more email addresses to send the environment report to, then click *Send*.

- 3 Click *OK* to close the Environment Report dialog box.

71.3.5 User Traffic Report

A user traffic report enables you to determine how many messages a user has sent outside his or her post office. The user traffic report lists all messages sent by a specified user during a specified date/time range, along with date, time, and size information for each message. You can also generate a user traffic report for all users whose messages pass through a selected domain.

In order for the information to be available to generate a user traffic report, you must configure the MTA to perform message logging. See [Section 42.4.2, "Enabling MTA Message Logging,"](#) on [page 657](#).

At the Windows [Monitor Agent server console](#) or the [Monitor Agent Web console](#):

- 1 Click *Reports > User Traffic*.

- 2 Select the user's domain or the domain you want to generate a user traffic report for.

- 3 Type the GroupWise user ID that you want to create a report for.

or

Leave the field blank to create a report for all users whose messages pass through the selected domain.

- 4 If you want to restrict the report to a particular time interval, specify start and end dates and times.

- 5 Click *Run*.

- 6 After the results are displayed, click *Save*, provide a file name for the report, select the format for the report, then click *OK*.

Reports can be saved in comma-separated or tab-separated format to meet the needs of the program you plan to use to display and print the report. For example, you could bring the data into a spreadsheet program. If needed, you can include column headings to create an initial line in the output file that labels the contents of each column.

7 When you are finished generating user traffic reports, click *Close*.

71.3.6 Link Traffic Report

A link traffic report enables you to determine how many messages are passing from a selected GroupWise domain across a specified link. The link traffic report lists the total number and total size of all messages passing through the link during each hour or half hour of operation.

In order for the information to be available to generate a link traffic report, you must configure the MTA to perform message logging. See [Section 42.4.2, “Enabling MTA Message Logging,” on page 657](#).

At the Windows [Monitor Agent server console](#) or the [Monitor Agent Web console](#):

- 1 Click *Reports > Link Traffic*.
- 2 Select the source domain of the link.
The list includes all domains that the Monitor Agent uses XML to communicate with. If the Monitor Agent must use SNMP to communicate with a domain, that domain is not included in the list.
- 3 Select the other end of the link, which could be another domain, a post office, or a gateway.
- 4 If you want to restrict the report to a particular time interval, specify start and end dates and times.
- 5 Click *Run*.
- 6 After the results are displayed, click *Save*, provide a file name for the report, select the format for the report, then click *OK*.

Reports can be saved in comma-separated or tab-separated format to meet the needs of the program you plan to use to display and print the report. For example, you could bring the data into a spreadsheet program. If needed, you can include column headings to create an initial line in the output file that labels the contents of each column.

7 When you are finished generating link traffic reports, click *Close*.

71.3.7 Message Tracking Report

A message tracking report enables you to track an individual message through your GroupWise system. The message tracking report provides information about when a message was sent, what queues the message has passed through, and how long it spent in each message queue. If the message has not been delivered, the message tracking report shows where it is.

In order for the information to be available to generate a message tracking report, you must configure the MTAs in your GroupWise system to perform message logging. See [Section 42.4.2, “Enabling MTA Message Logging,” on page 657](#).

In addition, you need to determine the message ID of the message. Have the sender check the Sent Item Advanced Properties of the message in the GroupWise client. The *Message Id* field displays the message ID of the message; for example, 3AD5EDEB.31D : 3 : 12763.

At the Windows [Monitor Agent server console](#) or the [Monitor Agent Web console](#):

- 1 Click *Reports > Message Tracking*.

- 2 Type the message ID of the message to track.

You can obtain the message file ID in the GroupWise client. Open the Sent Items folder, right-click the message, click *Properties*, then click the *Style* drop-down list and click *Advanced Properties*. The *Message Id* field displays the message file ID; for example, 3A75BAB9.FF1 : 8 : 31642.

- 3 Select the domain where you want to start tracking.
- 4 Click *Track*.
- 5 When you are finished generating message tracking reports, click *Close*.

71.3.8 Performance Testing Report

A performance testing report enables you to measure how long it takes messages to travel through your GroupWise system. The performance testing report lists each domain that a performance test message was sent to, when it was sent by the Monitor Agent, and the number of seconds between when it was sent and when the Monitor Agent received a response from the tested agent.

In order to run a performance testing report, you must configure the Monitor Agent for performance testing. See [Section 71.4, "Measuring Agent Performance,"](#) on page 989.

71.3.9 Connected User Report

The Connected Users report lists all users that are currently connected to POAs throughout your GroupWise system. It lists user name; client version, date, and platform; login time; and the IP address of the client user.

At the [Monitor Agent Web console](#):

- 1 Click *Reports > Connected Users*.

NOTE: The Connected Users report cannot be generated at the [Windows Monitor Agent server console](#) or the [Monitor Web console](#).

71.3.10 Gateway Accounting Report

The Gateway Accounting report shows traffic through a gateway. For example, you can use a Gateway Accounting report to track traffic to and from the Internet through a GWIA.

In order to run a Gateway Accounting report, you must configure the Monitor Agent to collect gateway accounting data. See [Section 71.5, "Collecting Gateway Accounting Data,"](#) on page 992.

71.3.11 Trends Report

The Trends report presents graphs of agent MIB variables as sampled over time. Graphs are generated based on data gathered from Monitor Agent log files. The quality of the graphs depends on the quantity of data that has been gathered when the graph is generated.

In the [Monitor Agent Web console](#):

- 1 Click *Reports > Trends*.

NOTE: The Trends report cannot be generated at the [Windows Monitor Agent server console](#).

- 2 Click the type of agent for which you want to set up a Trend report.

- 3 Specify a unique name for the Trend report.
- 4 Select the MIB variables that you want to collect values for over time, then click *Add Trend*.
The Trend report appears in the *Agent Trends* list.
- 5 Click the Trend report to view the graphs.

71.3.12 Down Time Report

The Down Time report graphically illustrates how much time each GroupWise agent has been down during the day.

In the [Monitor Agent Web console](#):

- 1 Click *Reports > Down Time*.

NOTE: The Down Time report cannot be generated at the Windows [Monitor Agent server console](#).

71.4 Measuring Agent Performance

To test the performance of the agents in your GroupWise system, you can send performance test messages from a specially configured Monitor domain to target domains anywhere in your GroupWise system. The Monitor Agent measures the amount of time it takes for replies to return from the target domains, which lets you ascertain the speed at which messages flow through your GroupWise system.

- ♦ [Section 71.4.1, “Setting Up an External Monitor Domain,” on page 989](#)
- ♦ [Section 71.4.2, “Configuring the Link for the External Monitor Domain,” on page 990](#)
- ♦ [Section 71.4.3, “Configuring the Monitor Agent for Agent Performance Testing,” on page 991](#)
- ♦ [Section 71.4.4, “Viewing Agent Performance Data,” on page 992](#)
- ♦ [Section 71.4.5, “Viewing an Agent Performance Report,” on page 992](#)
- ♦ [Section 71.4.6, “Receiving Notification of Agent Performance Problems,” on page 992](#)

71.4.1 Setting Up an External Monitor Domain

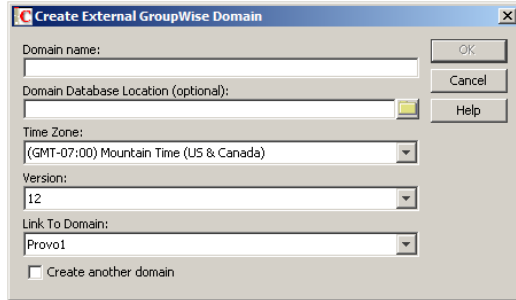
Before you can use the GroupWise Performance Testing feature to configure and enable GroupWise performance testing, you must create a specially configured Monitor domain and select an MTA to receive performance test messages from the Monitor Agent. The Monitor Agent uses an external GroupWise domain as part of measuring GroupWise agent performance.

By creating an external domain, you enable the Monitor Agent to approximate the round-trip time for email messages to travel to recipients and for status messages to travel back to senders. If you also plan to set up gateway accounting reports, as described in [Section 71.5, “Collecting Gateway Accounting Data,” on page 992](#), you can use this same external domain for collecting accounting data.

In ConsoleOne:

- 1 Connect to a domain where the MTA will communicate with the Monitor Agent for the purpose of sending accounting data to the Monitor Agent.

- 2 Create an external GroupWise domain.



For information about external GroupWise domains, see “[Creating an External Domain](#)” in “[Connecting to Other GroupWise Systems](#)” in the *GroupWise 2012 Multi-System Administration Guide*.

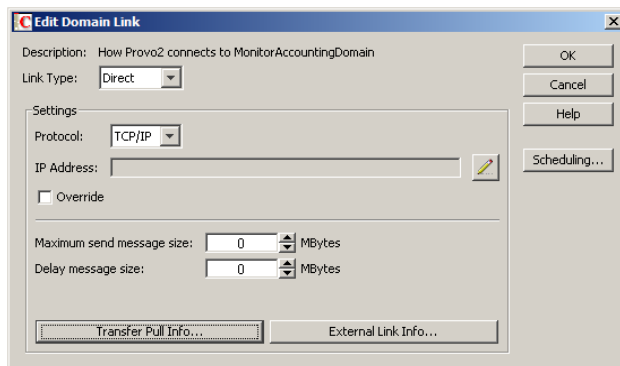
- 3 Name the external domain to reflect its role in your GroupWise system.
For example, you could name it ExternalMonitorDomain.
- 4 Continue with [Configuring the Link for the External Monitor Domain](#).

71.4.2 Configuring the Link for the External Monitor Domain

The Monitor Agent needs to send its performance testing messages to a specific MTA in your GroupWise system. It does not matter which MTA you decide to use. It could be the MTA for the domain to which the external Monitor domain is linked.

In ConsoleOne:

- 1 Click *Tools > GroupWise Utilities > Link Configuration*.
- 2 In the *Outbound Links From* box, double-click the domain whose MTA you want the Monitor Agent to communicate with.
- 3 Configure the outbound link from the selected MTA to the external Monitor domain to be a TCP/IP link.



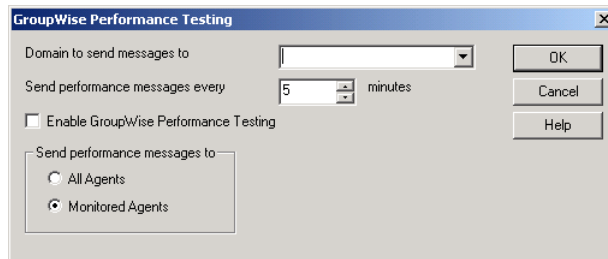
- 3a Click the pencil icon to provide the IP address of the server where the Monitor Agent runs.
- 3b Specify a unique port number for the MTA to use to communicate with the Monitor Agent.
- 3c Click *OK*.
- 4 Click *OK* to save your changes to the link.

- 5 Exit the Link Configuration Tool to save the new link configuration information.
- 6 Continue with [Configuring the Monitor Agent for Agent Performance Testing](#).

71.4.3 Configuring the Monitor Agent for Agent Performance Testing

After you have created an external Monitor domain and configured a link from it to an MTA, you are ready to configure the Monitor Agent for performance testing.

- 1 On Windows, at the [Monitor Agent server console](#), click *Configuration > Performance Testing*.



or

On Linux, at the [Monitor Agent Web console](#), click *Preferences > Setup*, then scroll down to the *Performance Testing* section.

- 2 Fill in the fields:

Domain to send messages to: Select the external Monitor domain that you configured for system performance testing.

You might need to restart the Monitor Agent in order to see the new Monitor domain in the drop-down list.

Send performance messages every: Specify in minutes the time interval for the Monitor Agent to send performance test messages.

Enable GroupWise Performance Testing: Select this option to turn on performance testing. Deselect this option when you have finished your performance testing.

Send performance messages to: Select *All Agents* to send performance test messages to all domains in your GroupWise system. Select *Monitored Agents* to send performance test messages only to the agents currently listed at the Monitor Agent console.

- 3 Click *OK* to put the performance testing settings into effect.
- 4 Continue with [Section 71.4.4, “Viewing Agent Performance Data,” on page 992](#).

or

Continue with [Section 71.4.6, “Receiving Notification of Agent Performance Problems,” on page 992](#).

71.4.4 Viewing Agent Performance Data

The information gathered by the Monitor Agent through performance test messages is recorded in the Monitor history log.

At the Windows [Monitor Agent server console](#) or the [Monitor Agent Web console](#):

- 1 Click *Log > View History Files*.
- 2 Select a history log file, then click *View*.

71.4.5 Viewing an Agent Performance Report

A performance testing report enables you to measure how long it takes messages to travel through your GroupWise system. The performance testing report lists each domain that a performance test message was sent to, when it was sent by the Monitor Agent, and the number of seconds between when it was sent and when the Monitor Agent received a response from the tested agent.

At the Windows [Monitor Agent server console](#) or the [Monitor Agent Web console](#):

- 1 Click *Reports > Performance Testing*.
- 2 Select *All Domains* to generate a performance testing report for all domains in your GroupWise system.
or
Select one domain to generate a performance testing report for it.
- 3 Click *Run* to generate the performance testing report.

71.4.6 Receiving Notification of Agent Performance Problems

If you want the Monitor Agent to notify you if system performance drops to an unacceptable level, you can create a threshold to check the `mtaLastResponseTime` and `mtaAvgResponseTime` MIB variables. The average response time is a daily average that is reset at midnight. See [Section 69.5.2, "Customizing Notification Thresholds," on page 959](#) for setup instructions.

71.5 Collecting Gateway Accounting Data

In order to run a Gateway Accounting report in Monitor, you must configure your GroupWise system to collect accounting files. The Internet Agent can be configured to generate accounting files, as described in [Section 54.3, "Tracking Internet Traffic with Accounting Data," on page 805](#). Then, the accounting files are collected and sent to the Monitor Agent for processing to create the Gateway Accounting report.

- ◆ [Section 71.5.1, "Setting Up an External Monitor Domain," on page 993](#)
- ◆ [Section 71.5.2, "Configuring the Link for the External Monitor Domain," on page 993](#)
- ◆ [Section 71.5.3, "Configuring the Monitor Agent to Communicate through the External Monitor Domain," on page 994](#)
- ◆ [Section 71.5.4, "Setting Up an External Post Office and External User for the Monitor Agent," on page 995](#)
- ◆ [Section 71.5.5, "Designating a Gateway Accountant," on page 995](#)
- ◆ [Section 71.5.6, "Receiving and Forwarding the Accounting Files," on page 996](#)
- ◆ [Section 71.5.7, "Viewing the Gateway Accounting Report," on page 997](#)

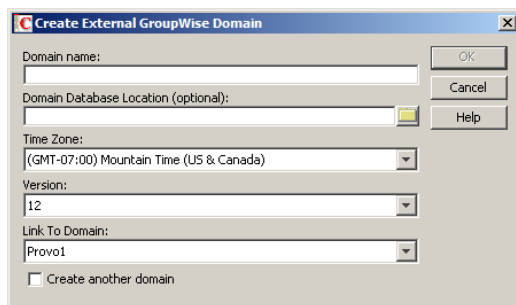
71.5.1 Setting Up an External Monitor Domain

In order to collect accounting data, you must create a specially configured Monitor domain and select an MTA to send accounting files through it to the Monitor Agent. The Monitor Agent needs the external domain to house an external post office where there is an external user that receives the accounting files from the Internet Agent.

If you are already using the GroupWise Performance Testing feature, as described in [Section 71.4, “Measuring Agent Performance,”](#) on page 989, you can use the same external domain and MTA for gathering accounting data. Skip to [Section 71.5.4, “Setting Up an External Post Office and External User for the Monitor Agent,”](#) on page 995.

In ConsoleOne:

- 1 Connect to a domain whose MTA will communicate with the Monitor Agent for the purpose of gathering accounting data.
- 2 Create an external GroupWise domain.



For background information about external GroupWise domains, see [“Creating an External Domain”](#) in [“Connecting to Other GroupWise Systems”](#) in the *GroupWise 2012 Multi-System Administration Guide*.

- 3 Name the external domain to reflect its role in your GroupWise system.
For example, you could name it ExternalMonitorDomain.
- 4 Link the external domain to the existing domain whose MTA will communicate with the Monitor Agent.
- 5 Continue with [Configuring the Link for the External Monitor Domain](#).

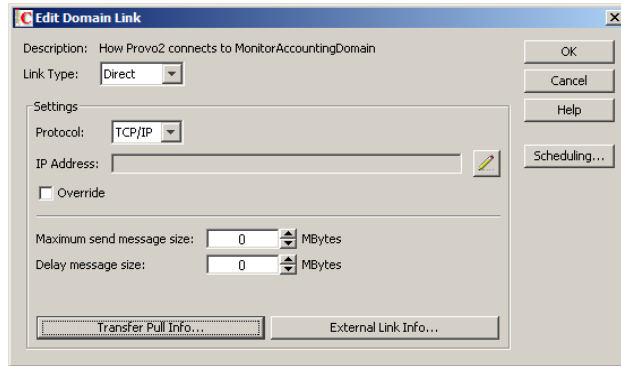
71.5.2 Configuring the Link for the External Monitor Domain

The Monitor Agent needs to receive accounting data from a specific MTA in your GroupWise system. It can be the MTA for the domain to which the external Monitor domain is linked.

In ConsoleOne:

- 1 Click *Tools > GroupWise Utilities > Link Configuration*.
- 2 In the *Outbound Links From* box, double-click the external Monitor domain.

- 3 Configure the outbound link to the external Monitor domain to be a TCP/IP link:



- 3a Click the pencil icon to provide the IP address or DNS hostname of the server where the Monitor Agent runs.
 - 3b Specify a unique port number for the Monitor Agent to use to communicate with the MTA in the domain to which the external Monitor domain is linked.
For example, you could use 7103.
 - 3c Click *OK*.
- 4 Click *OK* to save your change to the link.
 - 5 Exit the Link Configuration Tool to save the new link configuration information.
 - 6 Continue with [Configuring the Monitor Agent to Communicate through the External Monitor Domain](#).

71.5.3 Configuring the Monitor Agent to Communicate through the External Monitor Domain

In the [Monitor Agent Web console](#)

- 1 Click *Preferences*, then scroll down to the *MTP Settings* section.

- 2 Select the external Monitor domain in the drop-down list.
- 3 Specify the same port number that you specified in [Step 3b](#) in [Section 71.5.2, “Configuring the Link for the External Monitor Domain,”](#) on page 993.
- 4 Click *Submit*.
- 5 At the [server console](#) or [Web console](#) for the MTA in the domain that the external Monitor domain links to, verify that the link to the external Monitor domain is open.
- 6 Continue with [Setting Up an External Post Office and External User for the Monitor Agent](#).

71.5.4 Setting Up an External Post Office and External User for the Monitor Agent

Now that you have set up the link for the accounting data to flow through, you need to create an external user to receive the accounting files.

In ConsoleOne:

1 Create an external post office:

1a Right-click the External Domain object that you created in [Section 71.5.1, “Setting Up an External Monitor Domain,”](#) on page 993, then click *New External Post Office*.

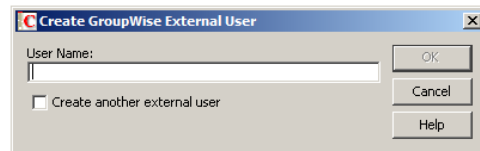


1b Name the external post office to reflect its role, such as ExternalMonitorPO.

1c Click *OK*.

2 Create an external user:

2a Right-click the External Post Office object, then click *New > External User*.



2b Name the external user to reflect its role, such as ExternalMonitorUser.

2c Click *OK*.

3 Continue with [Designating a Gateway Accountant](#).

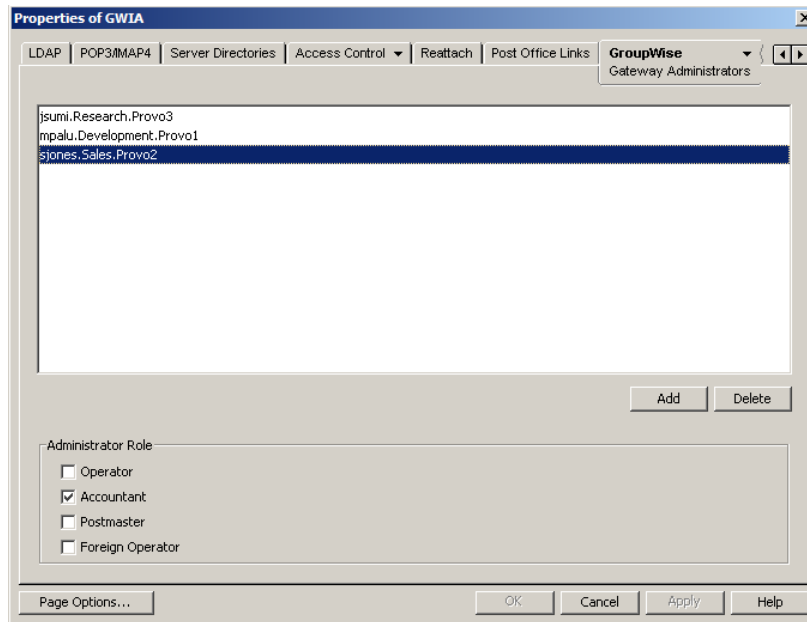
71.5.5 Designating a Gateway Accountant

As messages flow through a gateway such as the GWIA, the gateway logs the traffic and sends the accounting records to the gateway accountant once each day. For background information, see [Section 54.3, “Tracking Internet Traffic with Accounting Data,”](#) on page 805.

If you already have an accountant designated for each GWIA where you want to run accounting reports, skip to [Section 71.5.6, “Receiving and Forwarding the Accounting Files,”](#) on page 996.

In ConsoleOne:

- 1 Right-click the GWIA object, then click *Properties*.
- 2 Click *GroupWise > Gateway Administrators*.



- 3 Select a user to receive the gateway files.
Use yourself at this point for testing purposes.
- 4 Select *Accountant*.
- 5 Click *OK*.
- 6 Continue with [Receiving and Forwarding the Accounting Files](#).

71.5.6 Receiving and Forwarding the Accounting Files

Each GWIA sends the accounting files to the accountant. The accountant then must forward the accounting files to the external Monitor user.

In the GroupWise client:

- 1 Create a new rule to forward all accounting messages to the external Monitor user in the external Monitor post office.
A typical subject line for an accounting message is Agent Accounting Data File.
- 2 In order to establish the link for the first time, restart the Monitor Agent and the MTA for the domain that the external Monitor domain is linked to.
- 3 Verify that the accounting log files are being received by the Monitor Agent:
 - 3a At the [Monitor Agent Web console](#), click *Log > Gateway Accounting Logs*.
 - 3b Select the GWIA, then click *View Accounting Logs*.
If files are listed, then accounting data is successfully arriving to the Monitor Agent. The Monitor Agent uses the accounting log files to generate Gateway Accounting reports.

The accounting log files are stored on the server where the Monitor Agent is running. The default location varies by platform.

Linux: [/var/log/novell/groupwise/gwmon/acct](#)

Windows: [c:\ProgramData\Novell\GroupWise Server\Monitor\acct](#)

71.5.7 Viewing the Gateway Accounting Report

After accounting log files are being successfully sent to the Monitor Agent for processing, you can view the Gateway Accounting report in your Web browser.

- 1 At the [Monitor Agent Web console](#), click *Reports > Gateway Accounting*.

NOTE: The Gateway Accounting report cannot be generated at the Windows [Monitor Agent server console](#).

- 2 Select the GWIA for which you want to view accounting reports, then click *View Accounting Reports*.

The initial report lists all users who have sent and received messages through the GWIA. It lists the number of messages, the size of the messages, and the number of attachments. You can sort the list by any column heading.

[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)

[Environment](#) | [User Traffic](#) | [Link Traffic](#) | [Message Tracking](#) | [Performance Testing](#) | [Connected Users](#) | [Gateway Accounting](#) | [Trends](#) | [Down Time](#)

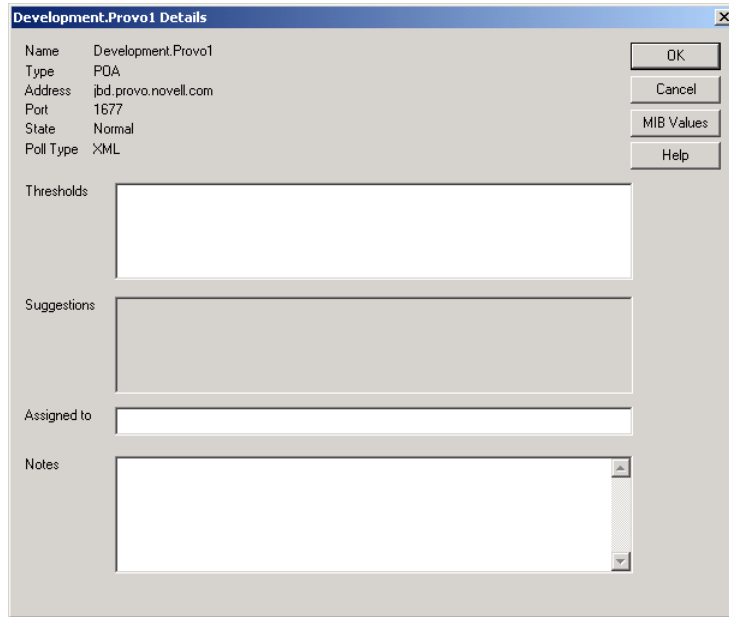
GWIA.Provo1		Jul 12 - Jul 12								
		Inbound			Outbound			Total		
Name	Messages	Size	Attachments	Messages	Size	Attachments	Messages	Size	Attachments	
jsuml	15	108420	15	9	18909	3	24	127329	18	
mpalu	3	21855	3	0	0	0	3	21855	3	

- 3 In the Users list, click a user to list all messages sent to and from the user.
- 4 In the list of messages, click a message ID to run a Message Tracking report for that message, as described in [Section 71.3.7, "Message Tracking Report," on page 987](#).
- 5 In the Users list, click *View Domains* to list the Internet domains associated with the GWIA.
- 6 In the list of domains, click an Internet domain to list all messages sent and received through that Internet domain.

71.6 Assigning Responsibility for Specific Agents

If multiple GroupWise administrators manage the agents throughout your GroupWise system, you can assign a contact for each agent. Or, in a help desk environment, a person can be assigned to an agent when a problem occurs. The person assigned to the agent can record notes about the functioning of the agent, which are then available to other administrators.

- 1 On Windows, at the [Monitor Agent server console](#), right-click an agent in the agent status window, then click *Agent Details*.



or

On Linux, at the [Monitor Agent Web console](#), click the agent status link.

[Status](#) | [Preferences](#) | [Link Trace](#) | [Link Configuration](#) | [Reports](#) | [Log](#) | [Map](#)

Name	Provo1
Type	MTA
Address	137.65.67.217:7100
Poll Type	XML
State	Normal
Assigned	<input type="text"/>
Notes	<div style="border: 1px solid #ccc; height: 60px;"></div>

mtaIndex	0
mtaDomainName	Provo1
mtaTotalDomains	7

- 2 In the *Assigned To* field, type the name of the GroupWise administrator who is responsible for this agent.

The name is displayed to the right of the agent status in the status window of the Monitor Agent console and the Monitor Web console.

- 3 In the *Notes* field, type any comments you might have about the agent.

If a problem with the agent occurs, the *Thresholds* field and the *Suggestions* field display helpful information about the problem if you have set up customized thresholds, as described in [Section 69.5.2, “Customizing Notification Thresholds,” on page 959](#).

- 4 Click *OK* to save the information about who is assigned to the agent.

71.7 Searching for Agents

If you monitor a large number of agents, the list displayed in the Monitor Web console can become very long. You can easily search for an individual agent or for a group of related agents.

At the [Monitor Web console](#):

- 1 Click the *Search* icon.



The screenshot shows the 'GroupWise Monitor' interface with a 'Search' tab selected. On the left, there is a tree view under 'Corporate' with sub-items 'OES Agents', 'SLES Agents', and 'Windows Agents'. Below this are buttons for 'Create', 'Rename', 'Move', 'Delete', 'Refresh', and 'Help'. The main area is titled 'Agent Search' and contains an 'Agent Name:' input field. Below it are radio buttons for 'Agent View': 'Problem Agents' (selected), 'Monitored Agents', and 'All Agents'. Under 'Agent Type:', there are checkboxes for MTA, POA, GWIA, WEBACC, PAGER, ASYNC, API, FAX, TAS, GATEWAY, X400, X25, EXCHANGE, and Other. A 'Sort By:' dropdown menu is set to 'Name'. At the bottom are 'Search', 'Cancel', and 'Help' buttons.

NOTE: The Search feature is not available in the Windows [Monitor Agent server console](#) or the [Monitor Agent Web console](#).

- 2 Type the name of an agent.

or

Select *Problems* to list all agents whose status is other than *Normal*.

or

Select one or more types of agent to list.

- 3 Select the number of instances you want listed at one time.

- 4 Click *Search*.

The results display on the Search page with the same functionality as is available on the regular Monitor Web console pages.

72 Comparing the Monitor Consoles

Many aspects of agent monitoring are available in one or more of the Monitor Agent consoles. The table below summarizes agent monitoring features and where they are available.

Task	Windows Monitor Agent Server Console	Monitor Agent Web Console	Monitor Web Console
Selecting Agents to Monitor	Yes	Yes	No
Creating and Managing Agent Groups	Yes	Yes	Yes
Viewing All Agents	Yes	Yes	Yes if not in groups
Viewing Problem Agents	Yes	Yes	Yes
Viewing a Windows Agent Server Console	Yes	No	No
Viewing an Agent Web Console	Yes	Yes	Yes
Searching for Agents	No	No	Yes
Assigning Responsibility for Specific Agents	Yes	Yes	Yes
Configuring the Monitor Agent for HTTP	Yes	Yes	Yes
Configuring the Monitor Agent for SNMP	Yes	Yes	Yes
Configuring Polling of Monitored Agents	Yes	Yes	Yes
Configuring Email Notification for Agent Problems	Yes	Yes	Yes
Configuring Audible Notification for Agent Problems	Yes	No	No
Configuring SNMP Trap Notification for Agent Problems	Yes	Yes	Yes
Configuring Authentication and Intruder Lockout for the Monitor Web Console	Yes	Authentication: Yes Intruder Lockout: No	No
Configuring Monitor Agent Log Settings	Yes	Yes	Yes
Monitoring Messenger Agents	Yes	Yes	Yes
Generating Reports	Yes	Yes	Yes
Link Trace Report	Yes	Yes	Yes
Link Configuration Report	Yes	Yes	Yes
Image Map Report	No	Yes	No

Environment Report	Yes	Yes	No
User Traffic Report	Yes	Yes	No
Link Traffic Report	Yes	Yes	No
Message Tracking Report	Yes	Yes	No
Performance Testing Report	Yes	Yes	No
Connected User Report	No	Yes	No
Gateway Accounting Report	No	Yes	No
Trends Report	No	Yes	No
Down Time Report	No	Yes	No

73 Using Monitor Agent Startup Switches

GroupWise Monitor Agent startup switches must be used on the command line when you start the Monitor Agent, or in a script or batch file created to start the Monitor Agent. The Monitor Agent does not have a startup file for switches.

Linux: If you start the Monitor Agent by running the gwmon executable, you can create a script like the following:

```
/opt/novell/groupwise/agents/bin/gwmon --home /domain_directory
                                         --other_switches &
```

If you start the Monitor Agent by running the grpwise-ma script, you can edit the MA_OPTIONS variable to include any switches you want to set.

Windows: You can create a batch file like the following:

```
c:\Program Files\Novell\GroupWise Server\Monitor\gwmon.exe
                                         /startup_switch /startup_switch ...
```

You can create a desktop icon for your batch file, or you can add startup switches to the Monitor Agent desktop icon that is created when you install the Monitor Agent.

The table below summarizes Monitor Agent startup switches for all platforms and how they correspond to configuration settings in the Windows Monitor Agent Server Console.

Switch starts with: a b c d e f g **h i j k l m n o p** q r s t u v w x y z

Linux Monitor Agent	Windows Monitor Agent	Windows Monitor Agent Server Console
--hapassword	/hapassword	N/A
--hapoll	/hapoll	N/A
--hauser	/hauser	N/A
--help	/help	N/A
--home	/home	N/A
--httpagentpassword	/httpagentpassword	Configuration > Poll Settings > HTTP Password
--httpagentuser	/httpagentuser	Configuration > Poll Settings HTTP User
--httpcertfile	/httpcertfile	N/A
--httpmonpassword	/httpmonpassword	Configuration > HTTP > HTTP Password
--httpmonuser	/httpmonuser	Configuration > HTTP > HTTP User
--httpport	/httpport	Configuration > HTTP > HTTP Port
--httpssl	/httpssl	N/A

Linux Monitor Agent	Windows Monitor Agent	Windows Monitor Agent Server Console
--ipa	/ipa	N/A
--ipp	/ipp	N/A
--lang	/lang	N/A
--log	/log	Log > Log Settings > Log File Path
--monwork	/monwork	N/A
--nmaddress	/nmaddress	Configuration > Add Novell Messenger System > Replica Address
--nmhome	/nmhome	Configuration > Add Novell Messenger System > Novell Messenger System Object
--nmpassword	/nmpassword	Configuration > Add Novell Messenger System > Password
--nmuser	/nmuser	Configuration > Add Novell Messenger System > User Name
--nosnmp	/nosnmp	N/A
--pollthreads	/pollthreads	N/A
--proxy	/proxy	N/A
--tcpwaitconnect	/tcpwaitconnect	N/A

NOTE: The [Monitor Agent Web console](#) does not include any settings comparable to the Monitor Agent startup switches.

73.1 --hapassword

Specifies the password for the Linux user name that the Monitor Agent uses to log in to the Linux server where the GroupWise High Availability service is running. See [Section 69.12, "Supporting the GroupWise High Availability Service on Linux,"](#) on page 968.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--hapassword <i>password</i>	/hapassword- <i>password</i>
Example:	--hapassword high	/hapassword-high

See also [--hauser](#) and [--hapoll](#).

73.2 --hapoll

Specifies in seconds the poll cycle on which the Monitor Agent contacts the GroupWise High Availability service to provide agent status information. The default is 120. The actual duration of the poll cycle can vary from the specified number of seconds because the actual duration includes the

time during which the Monitor Agent is checking agent status and restarting agents as needed. Then the specified poll cycle begins again and continues for the specified number of seconds. See [Section 69.12, “Supporting the GroupWise High Availability Service on Linux,”](#) on page 968.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--hapoll <i>seconds</i></code>	<code>/hapoll-<i>seconds</i></code>
Example:	<code>--hapoll 240</code>	<code>/hapoll-60</code>

See also [--hauser](#) and [--hapassword](#).

73.3 --hauser

Specifies the Linux user name that the Monitor Agent can use to log in to the Linux server where the GroupWise High Availability service is running. See [Section 69.12, “Supporting the GroupWise High Availability Service on Linux,”](#) on page 968.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--hauser <i>user_name</i></code>	<code>/hauser-<i>user_name</i></code>
Example:	<code>--hauser gwha</code>	<code>/hauser-gwha</code>

See also [--hapassword](#) and [--hapoll](#).

73.4 --help

Displays the Monitor Agent startup switch Help information. When this switch is used, the Monitor Agent does not start.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--help</code>	<code>/help</code>

73.5 --home

Specifies a domain directory, where the Monitor Agent can access a domain database ([wpdomain.db](#)). From the domain database, the Monitor Agent can determine which agents to monitor, what user names and passwords are necessary to access them, and so on.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	<code>--home <i>/directory</i></code>	<code>/home-[<i>svr</i>][<i>[vol:]dir</i></code> <code>/home-\\<i>svr</i>\<i>vol</i>\<i>dir</i></code> <code>/home-[<i>drive:</i>]\<i>dir</i></code> <code>/home-\\<i>svr</i>\<i>sharename</i>\<i>dir</i></code>

Linux Monitor Agent	Windows Monitor Agent
Example: --home /gwsystem/provo2	/home-\provo2 /home-mail:\provo2 /home-server2\mail:\provo2 /home-\\server2\mail\provo2 /home-\provo2 /home-m:\provo2 /home-\\server2\c\mail\provo

See also [--ipa](#) and [--ipp](#).

73.6 --httpagentpassword

Specifies the password for the Monitor Agent to prompt for when contacting monitored agents for status information. Providing a password is optional. See [Section 69.3.1, “Configuring the Monitor Agent for HTTP,”](#) on page 953.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --httpagentpassword <i>unique_password</i>	/httpagentpassword- <i>unique_password</i>
Example: --httpagentpassword WatchIt	/httpagentpassword-WatchIt

See also [--httpagentuser](#).

73.7 --httpagentuser

Specifies the user name for the Monitor Agent to use when contacting monitored agents for status information. Providing a user name is optional. See [Section 69.3.1, “Configuring the Monitor Agent for HTTP,”](#) on page 953.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --httpagentuser <i>unique_user_name</i>	/httpagentuser- <i>unique_user_name</i>
Example: --httpagentuser AgentWatcher	/httpagentuser-AgentWatcher

See also [--httpagentpassword](#).

73.8 --httpcertfile

Specifies the full path to the public certificate file used to provide secure SSL communication between the Monitor Agent and the Monitor Web console displayed in your Web browser. See [Section 69.8, “Configuring Authentication and Intruder Lockout for the Monitor Web Console,”](#) on page 964.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --httpcertfile <i>/dir/file</i>	/httpcertfile-[<i>drive:</i>] <i>dir\file</i> /httpcertfile-\\sv\sharename\dir\file

Linux Monitor Agent	Windows Monitor Agent
Example: --httpcertfile /certs/gw.crt	/httpcertfile-\ssl\gw.crt /httpcertfile-m:\ssl\gw.crt /httpcertfile-\\server2\c\ssl\gw.crt

See also [--httpssl](#).

73.9 --httpmonpassword

Specifies the password for the Monitor Web console to prompt for before allowing a user to display the Monitor Web console. Do not use an existing Novell eDirectory password because the information passes over the non-secure connection between your Web browser and the Monitor Agent. See [Section 69.8, “Configuring Authentication and Intruder Lockout for the Monitor Web Console,”](#) on page 964.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --httpmonpassword <i>unique_password</i>	/httpmonpassword- <i>unique_password</i>
Example: --httpmonpassword WatchIt	/httpmonpassword-WatchIt

See also [--httpmonuser](#).

73.10 --httpmonuser

Specifies the user name for the Monitor Web console to prompt for before allowing a user to display the Monitor Web console. Providing a user name is optional. Do not use an existing eDirectory user name because the information passes over the non-secure connection between your Web browser and the Monitor Agent. See [Section 69.8, “Configuring Authentication and Intruder Lockout for the Monitor Web Console,”](#) on page 964.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --httpmonuser <i>unique_user_name</i>	/httpmonuser- <i>unique_user_name</i>
Example: --httpmonuser MonAdmin	/httpmonuser-MonAdmin

See also [--httpmonpassword](#).

73.11 --httpport

Sets the HTTP port number used for the Monitor Agent to communicate with your Web browser. The default is 8200; the setting must be unique. See [Section 69.3.1, “Configuring the Monitor Agent for HTTP,”](#) on page 953.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --httpport <i>port_number</i>	/httpport- <i>port_number</i>

Linux Monitor Agent	Windows Monitor Agent
Example: --httpport 8201	/httpport-9200

73.12 --httpsl

Enables secure SSL communication between the Monitor Agent and the Monitor Web console displayed in your Web browser. See [Section 69.8, “Configuring Authentication and Intruder Lockout for the Monitor Web Console,”](#) on page 964.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --httpsl	/httpsl

See also [--httpcertfile](#).

73.13 --ipa

Specifies the network address (IP address or DNS hostname) of a server where an MTA is running. The Monitor Agent can communicate with the MTA to obtain information about agents to monitor.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --ipa <i>network_address</i>	/ipa- <i>network_address</i>
Example: --ipa 172.16.5.19 --ipa server2	/ipa-172.16.5.20 /ipa-server3

See also [--ipp](#).

73.14 --ipp

Specifies the TCP port number associated with the network address of an MTA with which the Monitor Agent can communicate to obtain information about agents to monitor. Typically, the MTA listens for service requests on port 7100.

Linux Monitor Agent	Windows Monitor Agent
Syntax: --ipp <i>port_number</i>	/ipp- <i>port_number</i>
Example: --ipp 7110	/ipp-7111

See also [--ipa](#).

73.15 --lang

Specifies the language to run the Monitor Agent in, using a two-letter language code. You must install the Monitor Agent in the selected language in order for the Monitor Agent to display in the selected language.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--lang <i>code</i>	/lang- <i>code</i>
Example:	--lang de	/lang-fr

See [Chapter 7, “Multilingual GroupWise Systems,”](#) on page 123 for a list of language codes.

73.16 --log

Specifies the full path of the directory where the Monitor Agent writes its log files. The default location varies by platform:

Linux: `/var/log/novell/groupwise/gwmon`

Windows: `c:\Program Files\Novell\GroupWise Server\Monitor`

See [Section 69.9, “Configuring Monitor Agent Log Settings,”](#) on page 965.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--log <i>/dir/file</i>	/log-[<i>drive:</i>] <i>dir</i> \ <i>file</i> /log-\\sv\ <i>sharename</i> \ <i>dir</i> \ <i>file</i>
Example:	--log /opt/novell/groupwise/agents/logs	/log-gw\logs /log-m:gw\logs /log-\\server2\c\gw\logs

73.17 --monwork

Specifies the location where the Monitor Agent creates its working directory. The default location varies by platform.

Linux: `/tmp/gwmon`

Windows: `c:\Program Files\Novell\GroupWise Server\Monitor`

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--monwork <i>/directory</i>	/monwork-[<i>sv</i>][<i>vol:</i>] <i>dir</i> /monwork-\\sv\ <i>vol</i> \ <i>dir</i> /monwork-[<i>drive:</i>] <i>dir</i> /monwork-\\sv\ <i>sharename</i> \ <i>dir</i>

Linux Monitor Agent	Windows Monitor Agent
Example: --monwork /tmp	/monwork-\\temp /monwork-mail:\\ temp /monwork-server2\\mail:temp /monwork-\\server2\\mail\\ temp /monwork-\\ temp /monwork-m:\\temp /monwork-\\server2\\c\\mail\\temp

73.18 --nmaddress

Specifies the IP address where an eDirectory replica is available, from which the Monitor Agent can obtain the information it needs to monitor Messenger Agents. See [Section 69.11, “Monitoring Messenger Agents,” on page 967](#).

Linux Monitor Agent	Windows Monitor Agent
Syntax: --nmaddress <i>IP_address</i>	/nmaddress- <i>IP_address</i>
Example: --nmaddress 172.16.5.18	/nmaddress-172.16.5.18

See also [--nmuser](#), [--nmpassword](#), and [--nmhome](#).

73.19 --nmhome

Specifies the context of the eDirectory container object where a Novell Messenger system is located. See [Section 69.11, “Monitoring Messenger Agents,” on page 967](#).

Linux Monitor Agent	Windows Monitor Agent
Syntax: --nmhome <i>eDirectory_context</i>	/nmhome- <i>eDirectory_context</i>
Example: --nmhome OU=MessengerService,O=Messenger	/nmhome- OU=MessengerService,OU=Provo,O=Novell

See also [--nmuser](#), [--nmpassword](#), and [--nmaddress](#).

73.20 --nmpassword

Specifies the password for the eDirectory user that the Monitor Agent uses to log into eDirectory to obtain Messenger information. See [Section 69.11, “Monitoring Messenger Agents,” on page 967](#).

Linux Monitor Agent	Windows Monitor Agent
Syntax: --nmpassword <i>password</i>	/nmpassword- <i>password</i>
Example: --nmpassword december	/nmpassword-sailboat

See also [--nmuser](#), [--nmhome](#), and [--nmaddress](#).

73.21 --nmuser

Specifies a user that the Monitor Agent can use to log in to eDirectory to obtain information about the Messenger system from the various Messenger objects. See [Section 69.11, “Monitoring Messenger Agents,”](#) on page 967

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--nmuser <i>eDirectory_context</i>	/nmuser- <i>eDirectory_context</i>
Example:	--nmuser CN=Admin,OU=Users,O=Novell	/nmuser-CN=Admin,OU=Provo,O=Novell

See also [--nmpassword](#), [--nmhome](#), and [--nmaddress](#).

73.22 --nosnmp

Disables SNMP for the Monitor Agent. The default is to have SNMP enabled. See [Section 69.3.2, “Configuring the Monitor Agent for SNMP,”](#) on page 955.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--nosnmp	/nosnmp

73.23 --pollthreads

Specifies the number of threads that the Monitor Agent uses for polling the agents for status information. Valid values range from 1 to 32. The default is 20. See [Section 69.4, “Configuring Polling of Monitored Agents,”](#) on page 956.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--pollthreads <i>number</i>	/pollthreads- <i>number</i>
Example:	--pollthreads 10	/pollthreads-32

73.24 --proxy

Routes all communication through the Monitor Agent and the Monitor Application (on the Web server). As long as the Web server can be accessed through the firewall, the Monitor Web console can receive information about all GroupWise agents that the Monitor Agent knows about. Without `--proxy`, the Monitor Web console cannot communicate with the GroupWise agents through a firewall. See [Section 69.10, “Configuring Proxy Service Support for the Monitor Web Console,”](#) on page 966.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--proxy	/proxy

73.25 --tcpwaitconnect

Sets the maximum number of seconds the Monitor Agent waits for a connection to a monitored agent. The default is 5.

	Linux Monitor Agent	Windows Monitor Agent
Syntax:	--tcpwaitconnect <i>seconds</i>	/tcpwaitconnect- <i>seconds</i>
Example:	--tcpwaitconnect 10	/tcpwaitconnect-15

XVI Client

- ♦ [Chapter 74, “Using GroupWise Windows Client Custom Installation Options,” on page 1015](#)
- ♦ [Chapter 75, “Setting Up GroupWise Client Modes and Accounts,” on page 1017](#)
- ♦ [Chapter 76, “Setting Defaults for the GroupWise Client Options,” on page 1025](#)
- ♦ [Chapter 77, “Distributing the GroupWise Windows Client,” on page 1069](#)
- ♦ [Chapter 78, “Supporting the GroupWise Client in Multiple Languages,” on page 1087](#)
- ♦ [Chapter 79, “Tools for Analyzing and Correcting GroupWise Client Problems,” on page 1089](#)
- ♦ [Chapter 80, “Startup Options for the GroupWise Windows Client,” on page 1091](#)

74 Using GroupWise Windows Client Custom Installation Options

The GroupWise Windows client Setup program provides the following options for customizing the installation of the Windows client:

Languages	If you downloaded the multilanguage version of the GroupWise software image, you can install the Windows client in one or more languages, as listed in Section 7.1, "GroupWise User Languages," on page 123.
Software Integrations	<p>If you use GroupWise Document Management Services (DMS), you can select which third-party applications you want to integrate with the Windows client. By default, no applications are integrated.</p> <p>The Setup program offers the following integrations:</p> <ul style="list-style-type: none">◆ OpenOffice Calc Document◆ OpenOffice Draw Document◆ OpenOffice Writer Document◆ OpenOffice Impress Document <p>Additional document types can be manually integrated with the Windows client, as described in Part VII, "Libraries and Documents," on page 313.</p>
Internet Browser Mail Integration	This option enables GroupWise to be the default email application when you click a <code>mailto</code> link in your Web browser or use the <code>Mail</code> command in your Web browser.
Program Folder	By default, the Setup program creates a Novell GroupWise program folder. You can use a different folder as needed.
Add GroupWise to the Desktop	By default, the Setup program create a GroupWise icon on your Windows desktop.
Add GroupWise to Quick Launch	By default, the Setup program adds a GroupWise icon to the Windows Quick Launch bar
Add Notify to the Startup Folder	By default, the Setup program does not add Notify to the Windows Startup folder. If you want to start Notify automatically, but you do not want to use the Windows Startup folder, you can click <i>Tools > Options > Environment</i> , then select <i>Launch Notify at startup</i> to have GroupWise automatically start Notify.
Add Icons to the Start Menu	By default, the Setup program adds GroupWise to the Windows Start Menu and includes a list of GroupWise tasks that can be performed directly from the Start Menu.

When users install the Windows client for themselves, they can set these options according to their own preferences.

When you, as an administrator, distribute the Windows client software to users' workstations, you can set these options according to your preferences, as described in:

- ♦ [Section 77.1, "Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client," on page 1069](#)
- ♦ [Section 77.2, "Using ZENworks Configuration Management to Distribute the GroupWise Windows Client," on page 1085](#)

75 Setting Up GroupWise Client Modes and Accounts

As a GroupWise administrator, you might need to help users with the various GroupWise modes and account types.

- ◆ [Section 75.1, “GroupWise Client Modes,” on page 1017](#)
- ◆ [Section 75.2, “Email Accounts,” on page 1022](#)

75.1 GroupWise Client Modes

GroupWise provides three different ways to run the GroupWise client: Online mode, Caching mode, and Remote mode.

- ◆ [Section 75.1.1, “Online Mode,” on page 1017](#)
- ◆ [Section 75.1.2, “Caching Mode,” on page 1017](#)
- ◆ [Section 75.1.3, “Remote Mode,” on page 1019](#)

Most GroupWise features are available in all three GroupWise modes, with a few exceptions:

- ◆ Subscribing to other users’ notifications is not available in Caching mode.
- ◆ Subscribing to other users’ notifications and Proxy are not available in Remote mode.

75.1.1 Online Mode

When users use Online mode, they are connected to their post office on the network. The user’s mailbox displays the messages and information stored in the network mailbox, which is called the Online mailbox. Online mode is connected to the Online mailbox continuously. In Online mode, if the Post Office Agent (POA) shuts down or users lose network connection, they temporarily lose the connection to their mailboxes.

Users should use this mode if they do not have a lot of network traffic, or if they use several different workstations and do not want to download a local mailbox to each one.

75.1.2 Caching Mode

Caching mode stores a copy of a user’s Online mailbox, including messages and other information, on the user’s local drive. This allows GroupWise to be used whether or not the network or Post Office Agent is available. Because the user is not connected to the network all the time, this mode cuts down

on network traffic and has the best performance. A connection is made automatically to retrieve and send new messages. All updates are performed in the background so GroupWise work is not interrupted.

Users should use this mode if they have enough disk space on the local drive to store the Caching mailbox. If users run Caching mode and Remote mode on the same computer, the same local mailbox can be used to minimize disk space usage.

By backing up their Caching mailboxes, users can protect items that might be deleted if the system is set up to automatically clean up items (or if the system administrator runs an Expire and Reduce).

Several users can set up their Caching mailboxes on a single shared computer.

The default location for a Caching mailbox varies by client platform:

Windows 7: `c:\Users\user_name\AppData\Roaming\Novell\GroupWise`

Windows Vista: `c:\Users\user_name\AppData\Local\Novell\GroupWise`

Windows XP: `c:\Documents and Settings\user_name\Local Settings\Application Data\Novell\GroupWise`

- ♦ [“Allowing or Forcing Use of Caching Mode” on page 1018](#)
- ♦ [“Downloading the GroupWise Address Book in Caching Mode” on page 1019](#)

Allowing or Forcing Use of Caching Mode

As the GroupWise administrator, you can allow or disallow the use of Caching mode, and can also force users to log in to GroupWise in Caching mode.

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Client Options*.
- 2 Click *Environment > Client Access*.
- 3 Select or deselect *Allow Use of Caching Mode*.
- 4 Select or deselect *Force Use of Caching Mode*.

Specify the number of days before Caching mode will be enforced. This allows the user to continue using Online mode until the grace period has passed. The grace period begins the first time the user connects to the POA. The setting applies per user per workstation.

The *Force Caching Mode* setting is not enforced on a workstation that does not have enough disk space for a Caching mailbox. The amount of disk space that is required is the size of the mailbox + 20 MB + 25% of the mailbox size.

The *Force Caching Mode* setting is also not enforced when a user connects from a shared Windows workstation or terminal server if you configure these workstations to be excluded. You do this by setting a registry key on the Windows workstation. The registry key is in HKEY_LOCAL_MACHINE. Under `Software\Novell\GroupWise\Client`, add a dword value named `No Local Store` with a value of 1. This prevents the user from creating a Caching or Remote mailbox by using the GroupWise Windows client menus. However, the user can still create a Caching or Remote mailbox by using the startup options `/pc`, `/pr`, or `/ps`.

If you force Caching mode and then restrict Online mailbox size so that users have items in their Caching mailboxes that are no longer available online, you need to make sure users understand about doing backups. See [“Backing Up Email”](#) in [“Maintaining GroupWise”](#) in the *GroupWise 2012 Windows Client User Guide*.

Downloading the GroupWise Address Book in Caching Mode

When users prime their Caching mailboxes, they receive a copy of the GroupWise Address Book. After the initial priming of the Caching mailbox, users can re-download the GroupWise Address Book and their personal address books in Caching mode by clicking *View > Retrieve System Address Book* or *View > Retrieve Personal Address Book* in the Address Book. Address books also be re-downloaded in Caching mode when users click *Tools > Retrieve Entire Mailbox*.

Users can also specify to download the GroupWise Address Book (and any rules they have created) on a regular basis.

- 1 In Remote or Caching mode, click *Accounts > Account Options*.
- 2 Select the GroupWise account, then click *Properties > Advanced*.
- 3 Select *Refresh Address Books and Rules Every __ Days*. By default this is set to 0 days, but it can be changed.

If you configure the POA to generate the GroupWise Address Book regularly, Caching mode users always have a current copy to download.

- 1 In ConsoleOne, right-click the POA object, then click *Properties > GroupWise > Maintenance*.

On the Maintenance page, make sure that *Generate Address Book for Remote* is selected. You can choose the time when you want the generation to take place.

If you want to generate the GroupWise Address Book for download more than once a day, you can delete the existing `wprof50.db` file from the `\wpcsout\ofs` subdirectory of each post office. A new downloadable GroupWise Address Book is generated automatically for users on each post office.

75.1.3 Remote Mode

Remote mode is familiar to GroupWise users who use Hit the Road. Similar to Caching mode, a copy of the Online mailbox, or the portion of the mailbox that users specify, is stored on the local drive. Users can periodically retrieve and send messages with the type of connection they specify (modem, network, or TCP/IP). Users can restrict what is retrieved, such as only new messages or only message subject lines.

As a GroupWise administrator, you can allow or disallow the use of Remote mode for client users.

- 1 In ConsoleOne, click *Tools > GroupWise Utilities > Client Options*.
- 2 Click *Environment > Client Access*.
- 3 Select or deselect *Allow Use of Remote Mode*.

The following topics explain the capabilities users have when they are allowed to use Remote mode.

- ♦ [“Hit the Road” on page 1019](#)
- ♦ [“Remote Properties” on page 1020](#)
- ♦ [“Remote Mode Connections” on page 1020](#)

Hit the Road

Users can use *Hit the Road* on the *Tools* menu (or startup option from Online mode to Remote mode) to create, set up, or update the Remote mailbox. A copy of the mailbox is created on the user’s local drive and any current connections are detected and set up. If users have already used Caching mode, the local mailbox has already been created. Users can also use *Hit the Road* to create setup files on a

removable storage device (for example, a flash drive) to set up their Remote mailbox on a computer that is not connected to the network. Several users can set up their Remote mailboxes on a single shared computer.

Hit the Road creates a network connection for the method (direct connection or TCP/IP) GroupWise uses to access the user's post office. GroupWise can then use this connection to connect to the GroupWise system, when running in Remote mode. For example, a network connection lets users of docked laptops run GroupWise in Remote mode and connect to the GroupWise system through the network connection rather than a modem connection.

To use *Hit the Road*:

- 1 In the GroupWise client, click *Tools > Hit the Road*.
- 2 Follow the prompts to create the Remote mailbox on the computer or on a removable storage device.

If *Hit the Road* created the user's Remote mailbox on a removable storage device, the user needs to install the Remote mailbox on the computer that will be running in Remote mode.

- 1 Insert the removable storage device containing the Remote mailbox into the computer.
- 2 Run `setup.exe` on the removable storage device.

Follow the prompts. The Setup program creates a Remote mailbox and copies the required files to the computer's hard drive.

Remote Properties

Users can change the way Remote mode is set up, including the connection, time zone, signature, and so on, in Account Options on the Accounts menu. Remote is listed as an account.

By default, if an item is deleted from the Remote mailbox, the item is deleted from the Online mailbox the next time a connection is made. Deletion options in Remote Properties can be changed so that an item deleted from the Remote mailbox stays in the Online mailbox or vice versa.

Remote Mode Connections

- ♦ ["Setting Up a Network Connection" on page 1020](#)
- ♦ ["Setting Up a TCP/IP Connection" on page 1021](#)

Setting Up a Network Connection

While running in Remote mode, GroupWise can connect to the user's Online mailbox using a network connection. A network connection is useful for laptop users connecting to the network through a docking station, or for remote users connecting through a modem using remote node software.

To create a network connection:

- 1 In the client, log in or change to Remote mode.
- 2 Click *Accounts > Send/Retrieve > GroupWise Options*.
- 3 Click *Network > OK*.
- 4 Type a descriptive name for the network connection in the *Connection Name* box.
- 5 Type the path to any post office directory in the master GroupWise system.

Users can connect to their own post offices or to any post office in the master GroupWise system to access their Online mailboxes.

- 6 Click a disconnect method:

Method	Description
When All Updates Are Received	Disconnects after requests are sent and after all responses to the requests are received (or disconnects automatically when the time allowed by the gateway has expired).
Do Not Wait for Responses	Disconnects immediately after requests are sent and pending responses are received. Pending responses are responses to other requests that are waiting to be downloaded to you.
Manually	Lets you manually control when to disconnect (or disconnects automatically when the time allowed by the gateway has expired).

- 7 Click *OK*.
- 8 Select the connection you want, then click *Select*.
- 9 Select the location you are connecting from in the *Connecting From* box. If none are listed, use the *Default Location* option.

If you need to create a new location, click the *Connect From* button. This is useful for laptop users who are calling into the GroupWise system from different geographic locations.
- 10 Click *OK*, then click *Close*.

Setting Up a TCP/IP Connection

A TCP/IP connection enables GroupWise, while running in Remote mode, to connect to the GroupWise system through a network connection using TCP/IP. A TCP/IP connection can be made through a network connection, such as a laptop connecting to the network through its docking station, or through a modem using remote node software.

To create a TCP/IP connection:

- 1 In the client, log in or change to Remote mode.
- 2 Click *Accounts > Account Options*, then double-click the Remote account.
- 3 Click *Connection > Connect To > New > TCP/IP > OK*.
- 4 Type a descriptive name for the TCP/IP connection.
- 5 Type the IP address or the DNS name.
- 6 Type the IP port for this address.

7 Click a disconnect method:

Method	Description
When All Updates Are Received	Disconnects after requests are sent and after all responses to the requests are received (or disconnects automatically when the time allowed by the gateway has expired).
Do Not Wait for Responses	Disconnects immediately after requests are sent and pending responses are received. Pending responses are responses to other requests that are waiting to be downloaded to you.
Manually	Lets you manually control when to disconnect (or disconnects automatically when the time allowed by the gateway has expired).

8 Click *OK*.

9 Select the connection you want, then click *Select*.

10 Select the location you are connecting from in the *Connecting From* box. If none are listed, use the *Default Location* option.

If you need to create a new location, click the *Connect From* button. This is useful for laptop users who are calling into the GroupWise system from different geographic locations.

11 Click *OK*, then click *Close*.

75.2 Email Accounts

- ♦ [Section 75.2.1, “Accounts Menu,” on page 1022](#)
- ♦ [Section 75.2.2, “Enabling POP3, IMAP4, and NNTP Account Access in Online Mode,” on page 1022](#)

75.2.1 Accounts Menu

In addition to the Remote account, users can access and configure POP3 and IMAP4 Internet email accounts and NNTP News accounts from the *Accounts* menu. While the user is in Remote and Caching mode, POP3, IMAP4, and NNTP accounts are accessed without needing to connect to the GroupWise system. If the system administrator enables it, users can also access and configure their POP3, IMAP4, and NNTP accounts from the Accounts menu in Online mode.

75.2.2 Enabling POP3, IMAP4, and NNTP Account Access in Online Mode

By default, POP3, IMAP4, and NNTP accounts can be added, configured, and accessed by users in Remote and Caching mode only. Account items and information are not accessible in Online mode, nor can items and information be uploaded to the Online mailbox until the system administrator enables it.

To enable POP3, IMAP4, and NNTP account access for clients in Online mode for an entire post office:

- 1 Make sure GroupWise 6.x or later agents have been installed.
For more information, see [Part X, “Message Transfer Agent,” on page 619](#).
- 2 Make sure Internet Addressing is enabled.

For more information, see [Section 4.11, “Internet Addressing,”](#) on page 89.

- 3** In ConsoleOne, select the Post Office object.
- 4** Click *Tools > GroupWise Utilities > Client Options*.
- 5** Click *Environment > General*.
- 6** Select *Allow Use of POP and IMAP Accounts in the Online Mailbox*.
- 7** Select *Allow Use of News (NNTP) Accounts in the Online Mailbox*.
- 8** Click OK.

76 Setting Defaults for the GroupWise Client Options

The GroupWise client includes options (preferences) that can be set by individual users. As a GroupWise administrator, you can determine the default settings for the options. If you don't want users to change the default settings that you have established, you can lock the settings.

- ♦ [Section 76.1, "Client Options Summary," on page 1025](#)
- ♦ [Section 76.2, "Setting Client Options," on page 1030](#)
- ♦ [Section 76.3, "Resetting Client Options to Default Settings," on page 1068](#)

76.1 Client Options Summary

Default settings can be established at the user level, the post office level, or the domain level. User settings override post office settings, and post office settings override domain settings.

If you set a lock on an option at a higher level, the higher level then overrides the lower-level setting. When you change an option and lock it, the new setting is immediately put into effect.

- 1 In ConsoleOne, select a Domain, Post Office, or User object, then click *Tools > GroupWise Utilities > Client Options*.



The client options table in this section summarizes all client options and provides links to descriptions of the options. For more detailed instructions, see [Section 76.2, "Setting Client Options," on page 1030](#).

- ♦ [Environment](#)
- ♦ [Send](#)
- ♦ [Documents](#)
- ♦ [Security](#)
- ♦ [Calendar](#)

Client Options Type	Client Options Tab	Client Options
Environment Click <i>Tools</i> > GroupWise <i>Utilities</i> > Client <i>Options</i> > Environment	<i>General</i>	Refresh Interval Allow Shared Folder Creation Allow Shared Address Book Creation Check Spelling As You Type Check Spelling Before Send Show Messenger Presence Allow Use of POP and IMAP Accounts in the Online Mailbox IMAP Copy Results in a GroupWise Move Allow Use of News (NNTP) Accounts in the Online Mailbox
	<i>Client Access</i>	Client Licensing Full License Mailboxes Limited License Mailboxes Client Login Mode Allow Use of Remote Mode Allow Use of Caching Mode Force Caching Mode after __ Days Show Login Mode Drop-Down List on Client Toolbar
	<i>Views</i>	View Options Read Next After Accept, Decline, or Delete Open New View after Send Allowable Read Views Plain Text HTML Allowable Compose Views Plain Text HTML Disable HTML View
	<i>File Location</i>	Archive Directory Custom Views

Client Options Type	Client Options Tab	Client Options
	<i>Cleanup</i>	Mail and Phone Manual Delete and Archive Auto-Delete After Auto-Archive After Appointment, Task, and Note Manual Delete and Archive Auto-Delete After Auto-Archive After Empty Trash Manual Automatic After Purges Do Not Purge Items Until They Are Backed Up Prompt before Purging Perform Maintenance Purges on Caching/Remote Force Synchronization of Cleanup Options to Caching/Remote
	<i>Appearance</i>	Schemes Default GroupWise 6.5 Simplified Custom Individual Settings Display Main Menu Display Nav Bar Display Main Toolbar Use GroupWise Color Schemes Blue, Olive Green, Silver, Sky Blue, Spring Green, Sterling Silver Display Folder List Favorites Folder List Simple Folder List Full Folder List Long Folder List Display QuickViewer QuickViewer at Bottom QuickViewer at Right
	<i>Retention</i>	Retention
	<i>Junk Mail</i>	Junk Mail Handling Enable Junk Mail Using Junk Mail Lists Enable Junk Mail Using Personal Address Book Enable Junk Calendaring Using Personal Address Book Auto-Delete After Enable Blocked Mail Using Block Mail Lists

Client Options Type	Client Options Tab	Client Options
	<i>Calendar</i>	Web Calendar Publishing Host Enable Calendar Publishing Enable Rules to Move Items to a Published Calendar Enable Publish Free/Busy Search Enable Subscribe to Calendar
	<i>Novell Vibe</i>	Enable Novell Vibe Novell Vibe URL
	<i>Tutorial</i>	Training and Tutorial URL
	<i>Address Book</i>	Enable Auto-Saving Save Addresses of Items That Are Received Save Addresses of Items That Are Sent Allow Creation of User Defined Fields in the Personal Address Book
	<i>Reply Format</i>	Plain Text Reply Format HTML Reply Format
Send	<i>Send Options</i>	Classification Normal, Proprietary, Confidential, Secret, Top Secret, For Your Eyes Only Priority High, Standard, Low Reply Requested When Convenient, Within ___ Days MIME Encoding Allow Use of "Reply to All" in Rules Allow Use of "Internet Mail" Tracking Expiration Date Delay Delivery Wildcard Addressing Notify Recipients Convert Attachments Allow Reply Rules to Loop Maximum Recipients Allowed Restricted Attachment Extensions
Click <i>Tools</i> > GroupWise Utilities > Client Options > Send	<i>Mail</i>	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification When Opened/Deleted None, Mail Receipt, Notify, Notify and Mail
	<i>Appointment</i>	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification When Opened/Accepted/Deleted None, Mail Receipt, Notify, Notify and Mail

Client Options Type	Client Options Tab	Client Options
	<i>Task</i>	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification When Opened/Accepted/Completed/Deleted None, Mail Receipt, Notify, Notify and Mail
	<i>Note</i>	Create a Sent Item to Track Information Delivered, Delivered and Opened, All Information, Auto-Delete Sent Item Return Notification When Opened/Deleted None, Mail Receipt, Notify, Notify and Mail
	<i>Security</i>	Conceal Subject Require Password to Complete Routed Item Secure Items Options Do Not Allow Use of S/MIME URL for Certificate Download Sign Digitally Encrypt for Recipients Encryption Key Size
	<i>Disk Space Management</i>	User Limits Mailbox Size Limit Threshold for Warning Users Maximum Send Message Size Limits Apply to Cache Notify the Administrator When Threshold Limit Is Exceeded Notify the Administrator When Size Limit Is Exceeded
	<i>Global Signature</i>	Global Signature Apply Signature to All Messages Apply Signature to External Messages Only
Documents Click <i>Tools</i> > <i>GroupWise Utilities</i> > <i>Client Options</i> > <i>Documents</i>	<i>Library Configuration</i>	Default Library
Security Click <i>Tools</i> > <i>GroupWise Utilities</i> > <i>Client Options</i> > <i>Security</i>	<i>Password</i>	Enter New Password Clear User's Password Allow Password Caching Allow eDirectory Authentication Instead of Password Enable Single Sign-On Use Collaboration Single Sign-On (CASA)

Client Options Type	Client Options Tab	Client Options
	<i>Macros</i>	View Macro Security Always Play Received Macros Never Play Received Macros Always Prompt Before Playing a Macro
	<i>Notify</i>	Check for Mail Every
Date and Time	<i>Calendar</i>	Month Display Option First of Week Highlight Day Show Week Number Appointment Options Include Myself on New Appointments Display Appointment Length As Duration, End Date and Time Default Length Alarm Options Set Alarm When Accepted Default Alarm Time Work Schedule Start/End Time Work Days
Click <i>Tools</i> > <i>GroupWise Utilities</i> > <i>Client Options</i> > <i>Date and Time</i>	<i>Busy Search</i>	Appointment Length Range and Time to Search Days to Search

76.2 Setting Client Options

Default settings can be established at the user level, the post office level, or the domain level. User settings override post office settings, and post office settings override domain settings.

If you set a lock on an option at a higher level, the higher level then overrides the lower-level setting. When you change an option and lock it, the new setting is immediately put into effect.

To modify the default settings for the GroupWise client:

- 1 In ConsoleOne, click a Domain object if you want to modify the settings for all users in the domain.
or
Click a Post Office object if you want to modify the settings for all users in the post office.
or
Click a User object or GroupWise External Entity object if you want to modify settings for the individual user. To change the same settings for multiple users, select multiple objects.
- 2 With the appropriate GroupWise object selected, click *Tools* > *GroupWise Utilities* > *Client Options* to display the GroupWise Client Options dialog box.



- 3 To set the Environment options, click *Environment*, then continue with [Section 76.2.1, “Modifying Environment Options,”](#) on page 1031.

or

To set the Send options, click *Send*, then skip to [Section 76.2.2, “Modifying Send Options,”](#) on page 1050.

or

To set the Documents options, click *Documents*, then skip to [Section 76.2.3, “Modifying Documents Options,”](#) on page 1061.

or

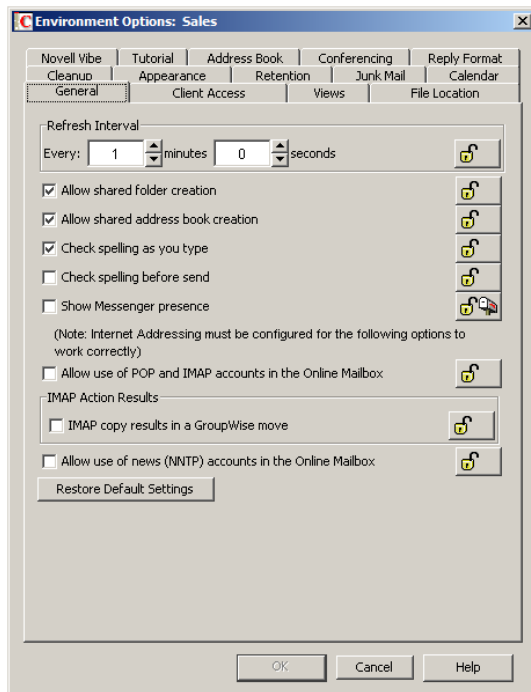
To set the Security options, click *Security*, then skip to [Section 76.2.4, “Modifying Security Options,”](#) on page 1061.

or

To set the Date and Time options, click *Date and Time*, then skip to [Section 76.2.5, “Modifying Calendar Options,”](#) on page 1065.

76.2.1 Modifying Environment Options

- 1 If the Environment Options dialog box is not displayed, follow the instructions in [Section 76, “Setting Defaults for the GroupWise Client Options,”](#) on page 1025 to display the dialog box.



- 2 Click the tab that contains the options you want to change. Refer to the following sections for information about options:

[“Environment Options: General” on page 1033](#)

[“Environment Options: Client Access” on page 1035](#)

[“Environment Options: Views” on page 1037](#)

[“Environment Options: File Location” on page 1038](#)

[“Environment Options: Cleanup” on page 1039](#)

[“Environment Options: Appearance” on page 1041](#)

[“Environment Options: Retention” on page 1042](#)

[“Environment Options: Junk Mail” on page 1043](#)

[“Environment Options: Calendar” on page 1045](#)

[“Environment Options: Novell Vibe” on page 1046](#)

[“Environment Options: Tutorial” on page 1047](#)

[“Environment Options: Address Book” on page 1048](#)

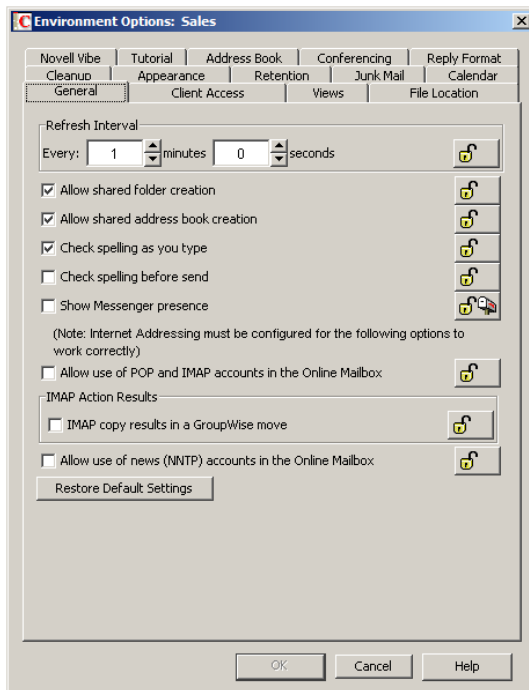
[“Environment Options: Conferencing” on page 1048](#)

[“Environment Options: Reply Format” on page 1049](#)

- 3 If you want to prevent users from changing an option’s setting, click the lock button next to it. After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.
- 4 If you want to return all the options on a tab to their default settings, click *Restore Default Settings*.
- 5 When you are finished, click *OK* to save your changes.

Environment Options: General

The *General* options determine such settings as the refresh interval for new messages, whether users can create shared folders and address books, and which types of accounts can be used in Online mode.



Refresh Interval

Determine how often the GroupWise client lists will be updated to reflect new message status. The default is 1 minute.

Allow Shared Folder Creation

Enables users to share folders with other users. By default, this option is enabled.

Allow Shared Address Book Creation

Enables users to share address books with other users. By default, this option is enabled.

Check Spelling As You Type

Automatically spell checks as text is typed. By default, this option is enabled.

Check Spelling Before Send

Automatically spell checks the message text of each item before the item is sent. By default, this option is disabled.

Show Messenger Presence

Displays the Messenger presence information in the GroupWise Windows client. Messenger presence enables users to easily choose instant messaging as an alternative to email. Messenger presence icons appear in the *From* field of a received message, in the Quick Info for users specified in the *To*, *CC*, and *BC* fields of a new message, and in the Quick Info for users in the Address Book. Messenger presence is enabled by default.

Allow Use of POP and IMAP Accounts in the Online Mailbox

Select this option to enable users to access POP and IMAP accounts while using the GroupWise client in Online mode.

By default, this option is disabled. If you enable this option, an *Accounts* menu is added to the GroupWise client, allowing users to add POP and IMAP accounts to GroupWise, set account properties, and send and retrieve items from their POP and IMAP accounts. In addition, users are allowed to upload POP and IMAP items from the Remote mailbox to the Online mailbox.

IMAP Copy Results in a GroupWise Move

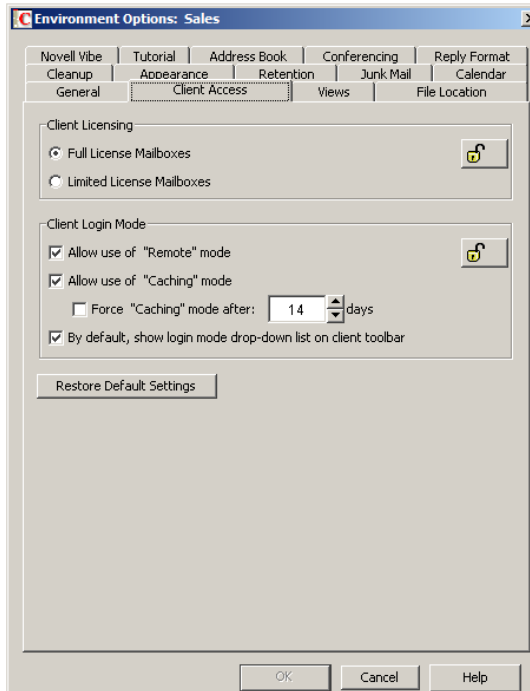
By default, when you move an item from one folder to another in an IMAP email client, the IMAP email client creates a copy of the item in the new location and marks the original item for deletion. The IMAP email client might display the original item with strikethrough markup, to indicate that it will be deleted according to the cleanup schedule you have selected, or the IMAP email client might hide such items until they are automatically cleaned up. When this IMAP behavior synchronizes to your GroupWise mailbox, GroupWise by default displays the original items with the strikethrough markup, and you might have been manually deleting those items from your GroupWise mailbox. Select this option so that items with strikethrough markup no longer display in GroupWise.

Allow Use of News (NNTP) Accounts in the Online Mailbox

Select this option to enable users to set up newsgroup (NNTP) accounts while using the GroupWise client in Online mode.

Environment Options: Client Access

The *Client Access* options allow you to apply a license type (full or limited) to users' mailboxes and enable or disable the Remote and Caching modes in the GroupWise Windows client.



Client Licensing

GroupWise offers two types of mailbox licenses: full client mailbox licenses and limited client mailbox licenses.

A full client mailbox license has no mailbox access restrictions; the mailbox can be accessed by the GroupWise Windows client and by GroupWise WebAccess, as well as any third-party plug-in or POP/IMAP email client.

A limited client mailbox license restricts mailbox access to the following:

- ♦ GroupWise WebAccess (including mobile devices)
- ♦ The GroupWise Windows client or GroupWise WebAccess via the Proxy feature
- ♦ The GroupWise Windows client or GroupWise WebAccess via the Busy Search feature
- ♦ A POP or IMAP client

A limited client license mailbox does not allow access through the GroupWise client for Windows (other than via Proxy or Busy Search).

You can use this option to specify the type of client license that you want applied to users' mailboxes. This enables you to support the type of GroupWise mailbox licenses you purchase. For example, if you only purchased limited client license mailboxes for users on a specific post office, you can mark all mailboxes on that post office as being limited client license mailboxes.

For information about generating an audit report that shows the type of license applied to each mailbox in a post office, see [Section 12.4, "Auditing Mailbox License Usage in the Post Office," on page 207](#).

Client Login Mode

Choose from the following settings to determine which login modes are available to GroupWise users when using the GroupWise client for Windows. These settings apply only if you selected *Full License Mailboxes* for the client licensing.

- ♦ **Allow Use of Remote Mode:** Select this option to enable users to log in with GroupWise in Remote mode. With Remote mode, the GroupWise client uses a Remote mailbox on the user's local drive. The user must initiate a connection (modem, direct, or TCP/IP) to send or retrieve items from the GroupWise system. For more information about Remote mode, see [Section 75.1.3, "Remote Mode," on page 1019](#). By default, this option is enabled.
- ♦ **Allow Use of Caching Mode:** Select this option to enable users to log in with GroupWise in Caching mode. With Caching mode, the GroupWise client uses a Caching mailbox on the user's local drive (this can be the same mailbox as the Remote mailbox). The GroupWise client periodically initiates a connection with the GroupWise system to send and receive items. For more information about Caching mode, see [Section 75.1.2, "Caching Mode," on page 1017](#). By default, this option is enabled.

Select the *Force Caching Mode* option (available only if the *Allow Use of Caching Mode* option is enabled) to force users to run in Caching mode. By default, this option is disabled. Specify the number of days before Caching mode is enforced. This allows the user to continue using Online mode until the grace period has passed. The grace period begins the first time the user connects to the POA. The setting applies per user per workstation.

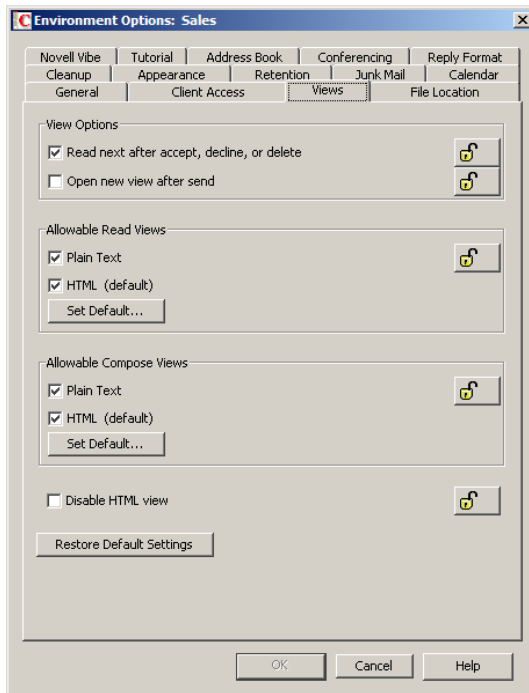
The *Force Caching Mode* setting is not enforced on a workstation that does not have enough disk space for a Caching mailbox. The amount of disk space that is required is: the size of the mailbox + 20 MB + 25% of the mailbox size.

The *Force Caching Mode* setting is also not enforced when a user connects from a shared Windows workstation or terminal server if you configure these workstations to be excluded. You do this by setting a registry key on the Windows workstation. The registry key is in HKEY_LOCAL_MACHINE. Under `Software\Novell\GroupWise\Client`, add a dword value named `No Local Store` with a value of 1. This prevents the user from creating a Caching or Remote mailbox by using the GroupWise Windows client menus. However, the user can still create a Caching or Remote mailbox by using the startup options `/pc`, `/pr`, or `/ps`.

- ♦ **By Default, Show Login Mode Drop-Down List on Client Toolbar:** Select this option to have the *Login Mode* drop-down list displayed on the client's toolbar. This enables users to change the mode themselves and is necessary only if you allow multiple modes to be used. By default, this option is enabled.

Environment Options: Views

The *Views* Environment options determine when items open, and whether or not users can read and compose messages in HTML.



View Options

Choose from the following settings to determine what occurs when the user performs an action that closes the current view.

- ♦ **Read Next after Accept, Decline, or Delete:** Select this option to have the next available received item automatically open after the user accepts, declines, or deletes an appointment, task, or note. By default, this option is enabled.
- ♦ **Open New View after Send:** Select this option to have a new send view open after a user sends a message. By default, this option is disabled.

Allowable Read Views

Choose from the following settings to determine what read views you allow the clients to use.

- ♦ **Plain Text (Default):** Select this option to allow users to read items in plain text.
- ♦ **HTML:** Select this option to allow users to read items in HTML.

Click *Set Default* to select the default read views.

Allowable Compose Views

Choose from the following settings to determine what compose views you allow the clients to use.

- ♦ **Plain Text (Default):** Select this option to allow users to compose items in plain text.
- ♦ **HTML:** Select this option to allow users to compose items in HTML.

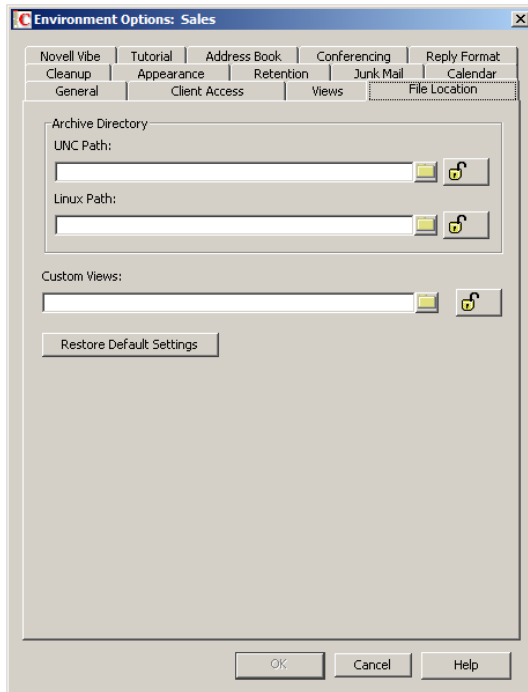
Click *Set Default* to select the default compose views.

Disable HTML View

Turns off the ability to view or compose messages in HTML View.

Environment Options: File Location

The *File Location* options determine the locations of users' archive directories and the custom views directory.



Archive Directory

Select the directory to be used for archiving items for the Windows client. Each user must have his or her own archive directory. You could choose a location similar to the default location for users' Caching mailbox, for example:

Windows XP: `c:\Documents and Settings\user_name\Local Settings\Application Data\Novell\GroupWise\archive`

Windows Vista: `c:\Users\user_name\AppData\Local\Novell\GroupWise\archive`

Windows 7: `c:\Users\user_name\AppData\Roaming\Novell\GroupWise\archive`

Linux: `/home/login_name/gwarchive`

It could also be a personal user directory on a network server. If you select a network drive, make sure users have the necessary rights to access the location.

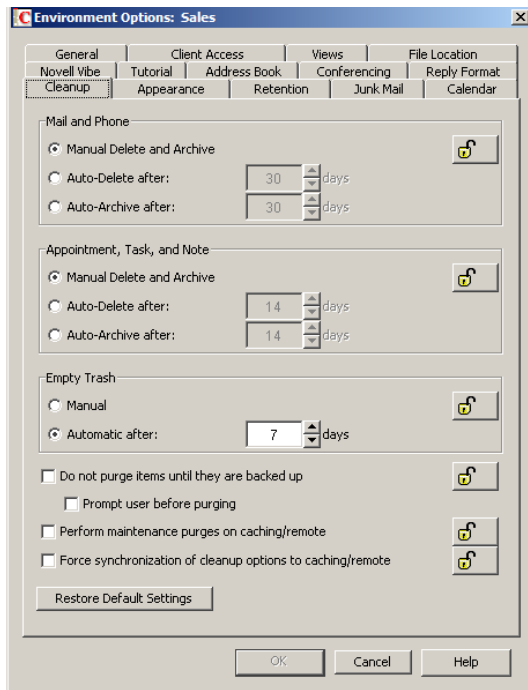
IMPORTANT: If you want to use a network location, do not specify the same directory for users in more than one post office. The names of users' individual archive directories are based on their FIDs. FIDs are unique within a post office, but users in different post offices can have the same FID.

Custom Views

This option applies only if you are using custom views. Select the directory where the views are located. The GroupWise product does not include the capability to design custom views, but third-party products make use of this feature to support their specialized capabilities.

Environment Options: Cleanup

The *Cleanup* options determine the delete and archive settings for GroupWise items (mail messages, phone messages, appointments, tasks, and notes).



Mail and Phone

Choose from the following settings to determine how mail and phone messages are deleted and archived:

- ◆ **Manual Delete and Archive:** Select this option to have mail and phone messages deleted or archived only when users manually do it. This is the default setting.
- ◆ **Auto-Delete After:** Select this option to have GroupWise automatically delete mail and phone messages that are older than the specified number of days. If you use this option, you should notify users so they know they must archive items they want to save.
- ◆ **Auto-Archive After:** Select this option to have GroupWise archive mail and phone messages that are older than the specified number of days. Users must have an archive directory specified in order for items to be archived. See [“Environment Options: File Location” on page 1038](#) for information about setting a default archive directory location.

Appointment, Task, and Note

Choose from the following settings to determine how appointments, tasks, and notes are deleted or archived:

- ♦ **Manual Delete and Archive:** Select this option to have appointments, tasks, and notes deleted or archived only when users manually do it. This is the default setting.
- ♦ **Auto-Delete After:** Select this option to have GroupWise automatically delete appointments, tasks, or notes that are older than the specified number of days. If you use this option, you should notify users so they know they must archive items they want to save.
- ♦ **Auto-Archive After:** Select this option to have GroupWise automatically archive appointments, tasks, and notes older than the specified number of days. Users must have an archive directory specified in order for items to be archived. See [“Environment Options: File Location” on page 1038](#) for information about setting a default archive directory location.

Empty Trash

Deleted items are moved to the Trash folder. They can be retrieved from the Trash until it is emptied. Items in the Trash still take up disk space. Select from the following settings to determine how the Trash folder is emptied:

- ♦ **Manual:** Select this option to require the user to manually empty the Trash. This is the default setting.
- ♦ **Automatic:** Select this option to have GroupWise automatically empty items from the trash after they have been in it for the specified number of days.

Purges

- ♦ **Do Not Purge Items Until They Are Backed Up:** Select this option to prevent items that have not been backed up from being removed from the Trash. This option is disabled by default.

Select the *Prompt Before Purging* option (available only if *Do Not Purge Items Until They Are Backed Up* is disabled) to prompt the user to confirm the purging of any files that have not been backed up.

- ♦ **Perform Maintenance Purges on Caching/Remote:** On the Disk Space Management page (*Tools > GroupWise Utilities > Client Options > Send > Disk Space Management*) in ConsoleOne, you can limit the size of users' Online mailboxes. You can now enforce the same mailbox size limits on users' Caching and Remote mailboxes, wherever those mailboxes are located.

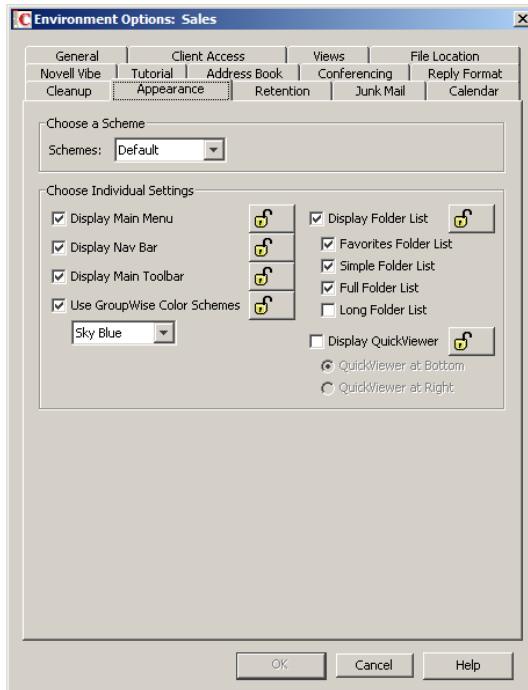
The size limit is applied to users' Caching and Remote mailboxes regardless of the amount of available disk space on users' hard drives. The size limit is applied the next time the GroupWise Windows client synchronizes with users' Online mailboxes. Because users might lose items that they have been storing locally when the size limit is enforced, you should warn users that size limits are going to be placed on their local Caching and Remote mailboxes.

Force Synchronization of Cleanup Options to Caching/Remote

Transfers the cleanup options you set in ConsoleOne to users' Caching and Remote mailboxes and locks them, so that the cleanup options are performed even if users are working in their Caching or Remote mailboxes without being connected to the network.

Environment Options: Appearance

The *Appearance* options determines the appearance of the GroupWise Windows client.



Schemes

There are four available schemes that determine how the GroupWise Windows Client appears.

- ♦ **Default:** The Default scheme has a new color scheme and displays the Nav Bar, Full Folder List, the Main Menu, and two columns with panels.
- ♦ **GroupWise 6.5:** The GroupWise 6.5 scheme has the Folder List, Main Toolbar, and Item List, displaying in the old colors.
- ♦ **Simplified:** The Simplified scheme has a new color scheme and has the Nav Bar, Simple Folder List, and two columns with panels.
- ♦ **Custom:** The Custom scheme allows you to set the appearance settings however you like. If you edit one of the predefined schemes, those settings become your Custom scheme.

Individual Settings

You can also control individual appearance settings for the GroupWise Windows client.

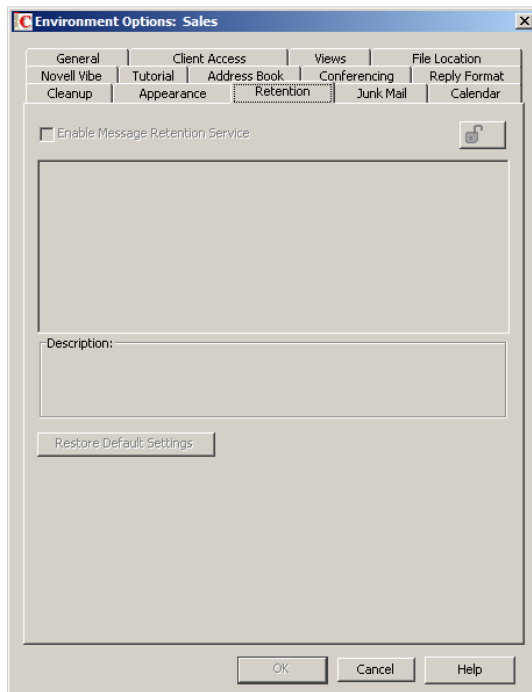
- ♦ **Display Main Menu:** Displays the menu at the top of the window in the GroupWise client.
- ♦ **Display Nav Bar:** Displays the Nav Bar at the top of the window in the GroupWise client.
- ♦ **Display Main Toolbar:** Displays the toolbar underneath the Navigation bar in the GroupWise client.
- ♦ **GroupWise Color Scheme:** Overrides any operating system color schemes for the GroupWise client. You can select Blue, Olive Green, Silver, Sky Blue, Spring Green, or Sterling Silver.

- ♦ **Display Folder List:** Displays the Folder list on the left side of the window in the GroupWise client. You can select from a Favorites Folder List, Simple Folder List, Full Folder List, or Long Folder List. For descriptions, see “[Customizing Individual GroupWise Appearance Settings](#)” in “[Getting Organized](#)” in the *GroupWise 2012 Windows Client User Guide*.
- ♦ **Display QuickViewer:** Displays the QuickViewer in the GroupWise client. You can select to display the QuickViewer on the right side or at the bottom.

Environment Options: Retention

The *Retention* tab is displayed only if the Provides Message Retention Service setting is turned on for a trusted application. For information, see [Section 4.12, “Trusted Applications,”](#) on page 90.

Message retention is configurable only by administrators, not by GroupWise users. The Retention options do not display in the GroupWise client.

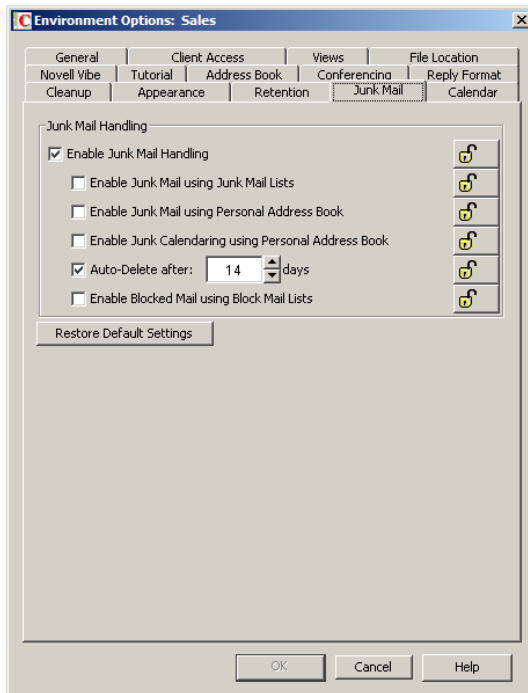


Enable Message Retention Service

Select this option to enable the Message Retention Service. If you are setting client options for a domain, all user mailboxes in the domain support message retention. Likewise, if you are setting options for a post office, all user mailboxes in the post office support message retention. After a user’s mailbox is enabled for message retention, the user cannot perform any action (purging, archiving, etc.) that removes messages from the mailbox until the messages have been copied to another storage location by a trusted application that has been designed to provide the Message Retention Service.

Environment Options: Junk Mail

The Junk Mail Handling Environment options determine the junk mail handling functionality of the GroupWise client.



Junk Mail Handling

Select *Enable Junk Mail Handling* to enable junk mail handling. This setting determines whether or not the Junk Mail Handling feature is available for a user. This setting affects both the client and the POA. Junk Mail Handling allows users to block or “junk” unwanted Internet email. When this setting is disabled, the client does not display any Junk Mail Handling menus or dialog boxes, and the POA does not perform any junk mail handling for the user. When this setting is enabled, the client displays Junk Mail Handling menus and dialog boxes, and the POA performs junk mail handling if the block and junk lists are also enabled.

Enable Junk Mail Using Junk Mail Lists

Select this option to cause junking based on email addresses and domain names available to users. A user can junk email from a specific Internet email address or from an entire Internet domain, when the email addresses and Internet domains are listed in the user’s Junk List. (Initially, there are no entries in a user’s junk list.) Junked items are delivered to the Junk Mail folder in the user’s Mailbox.

When this setting is enabled or disabled and not locked, the user’s initial setting to use the Junk List is enabled or disabled. Users can change the setting. When the setting is enabled and locked, a user’s Enable Junk List setting is enabled and cannot be disabled. When the setting is disabled and locked, the Junk List is unavailable to the user. Client menu options and dialog boxes involving the Junk List are not displayed.

Enable Junk Mail Using Personal Address Book

Select this option to cause junking based on personal address book entries available to users. A user can junk email from all users whose addresses are not in any personal address books (including Frequent Contacts) without building a Junk List.

When this setting is enabled or disabled and not locked, the user's initial setting to use personal address books is enabled or disabled. Users can change the setting. When the setting is enabled and locked, a user's *Enable Junk Mail Using Personal Address Book* setting is enabled and cannot be disabled. When the setting is disabled and locked, this option is unavailable to the user.

Enable Junk Calendaring Using Personal Address Book

Select this option to make junking of calendar items based on personal address book entries available to users. A user can junk calendar items from all users whose addresses are not in any personal address books (including Frequent Contacts) without building a Junk List.

Auto-Delete After

Select this option and specify the number of days after which you want junked items to be automatically deleted from users' mailboxes. The default is 14 days.

When this setting is enabled or disabled and not locked, the user's initial setting to delete junked items is enabled or disabled. Users can change the setting. When the setting is enabled and locked, a user's *Automatically Delete Items* setting is enabled and cannot be disabled. When the setting is disabled and locked, this option is unavailable to the user.

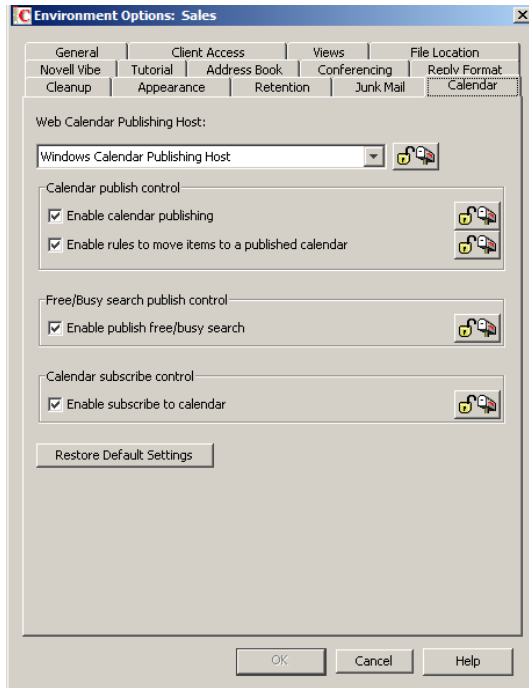
Enable Blocked Mail Using Block Mail Lists

Select this option to make blocking available to users. A user can block email from an Internet email address or Internet domain, when blocked email addresses and Internet domains are listed in the user's Block List. (Initially, there are no entries in a user's Block List.) Blocked items are blocked when the POA processes delivery to the user's mailbox, and the items are never delivered to the user's mailbox. When the POA log uses verbose mode, the log displays information about blocked items.

When this setting is enabled or disabled and not locked, the user's initial setting to use the Block List is enabled or disabled. Users can change the setting. When the setting is enabled and locked, a user's Block List setting is enabled and cannot be disabled. When the setting is disabled and locked, blocking is unavailable to the user. Client menu options and dialog boxes involving the Block List are not displayed.

Environment Options: Calendar

The Calendar options enable various types of calendar publishing for GroupWise users.



Web Calendar Publishing Host

Select the Calendar Publishing Host for this domain or post office from the drop-down list. For setup instructions, see [“Installing the GroupWise Calendar Publishing Host”](#) in the *GroupWise 2012 Installation Guide*.

Enable Calendar Publishing

Select this option to let users publish personal GroupWise calendars on the Internet. When calendar publishing is enabled, users of the GroupWise Windows client and GroupWise WebAccess can right-click a personal calendar, then click *Publish* to select options for publishing a personal calendar.

Enable Rules to Move Items to a Published Calendar

Select this option to allow users to create rules that move specific items to a published GroupWise calendar. Rules are disabled by default.

Enable Publish Free/Busy Search

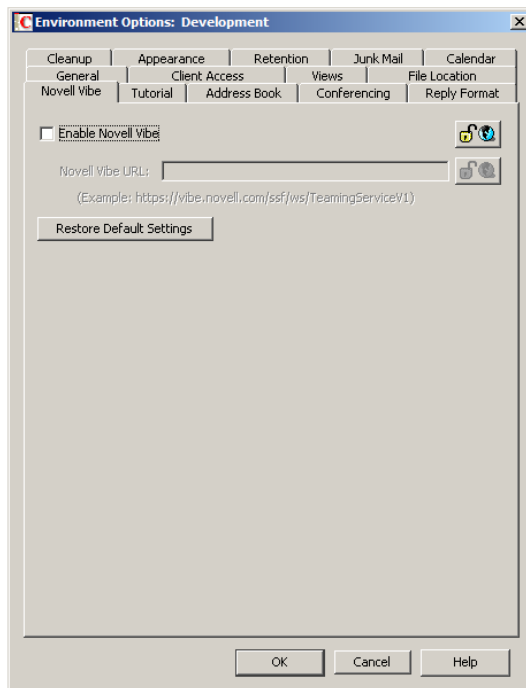
Enable this option to allow users to make their appointment information available to external users, so that external users can perform Free/Busy Searches on users' GroupWise calendars. Free/Busy searching is disabled by default.

Enable Subscribe to Calendar

Select this option to allow users to subscribe to Internet calendars that are updated on a regular basis, such as calendars for sporting events. Calendar subscription is enabled by default. Calendar subscription can be enabled even if no Calendar Publishing Host has been selected.

Environment Options: Novell Vibe

The Novell Vibe options provide access to a Novell Vibe site for GroupWise users. Novell Vibe enhances GroupWise by providing easy document management and sharing, team calendars and task lists, workflows, discussion threads, wikis, blogs, and RSS feeds.



Enable Novell Vibe

Select this option to provide GroupWise Windows client users with a Novell Vibe folder in their mailboxes. The Novell Vibe folder links to the Novell Vibe site associated with your GroupWise system. For more information, see [“Enabling GroupWise/Vibe Integration for GroupWise Windows Client Users”](#) in [“Novell Vibe”](#) in the *GroupWise 2012 Interoperability Guide*.

Novell Vibe URL

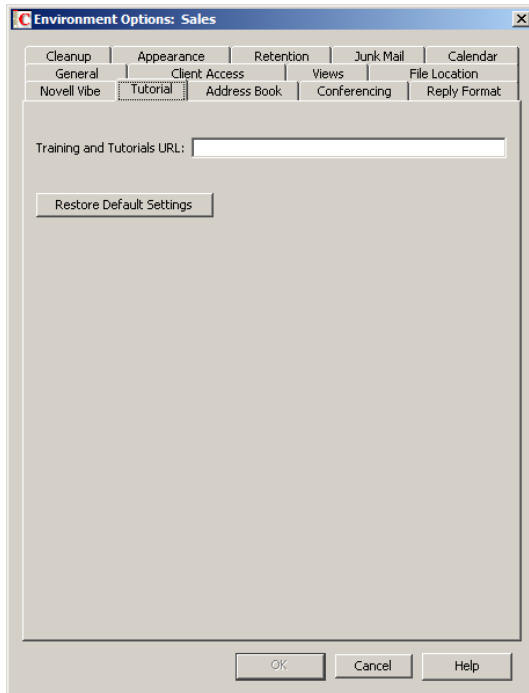
Specify the URL of the Novell Vibe site. The following format is required:

```
http://vibe_server:port_number/ssf/ws/TeamingServiceV1
```

Replace *vibe_server* with the base URL of the server where Novell Vibe is running. If you are using the default port number, specifying *port_number* is optional. The remainder of the URL provides GroupWise with information it needs in order to display the Vibe site correctly within GroupWise

Environment Options: Tutorial

The Tutorial option provides the ability to change the URL that is displayed when the user clicks *Help > Training and Tutorials* in the GroupWise Windows client.



Training and Tutorial URL

The default URL is:

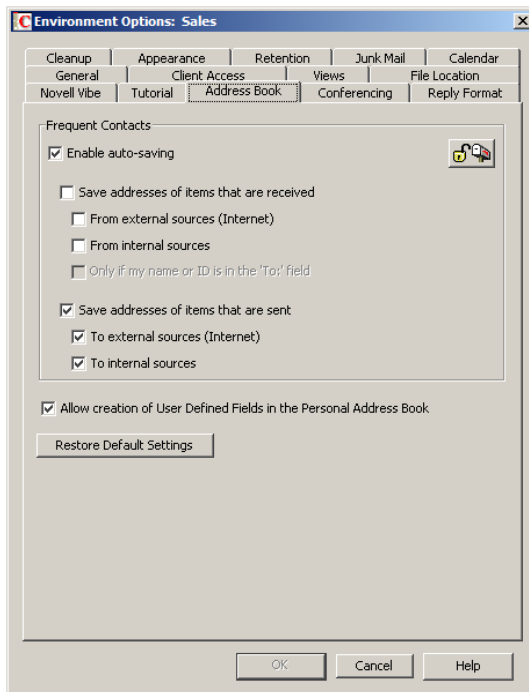
http://www.novell.com/products/groupwise/brainstorm_training/index.html (<http://www.brainstorminc.com/landing/product-integration/novell/gw-2012-quickhelp.aspx>)

If you purchase more in-depth training from BrainStorm, or you want to provide your own customized training materials for your GroupWise users, you can specify the URL that *Help > Training and Tutorials* displays.

Specify the URL for a custom training and tutorial Web page.

Environment Options: Address Book

The Address Book options enable you to control how users configure the functioning of their Frequent Contacts address books. You can also control whether users can create custom columns in their personal address books.



Enable Auto-Saving

By default, email addresses of those to whom users send messages are automatically added to their Frequent Contacts address books. Users can also choose to automatically save email addresses of those from whom they receive messages. Deselect this option if you do not want email addresses to be automatically saved.

- ◆ **Save Addresses of Items That Are Received:** Select this option to allow users to automatically add external and internal email address from items that they receive to their Frequent Contacts address books. If desired, you can restrict users to collecting email addresses only if the user's name or email address appears in the *To* field, as opposed to the *CC* or *BC* fields.
- ◆ **Save Addresses of Items That Are Sent:** Select this option to allow users to automatically add external and internal email address from items that they send to their Frequent Contacts address books.

Allow Creation of User Defined Fields in the Personal Address Book

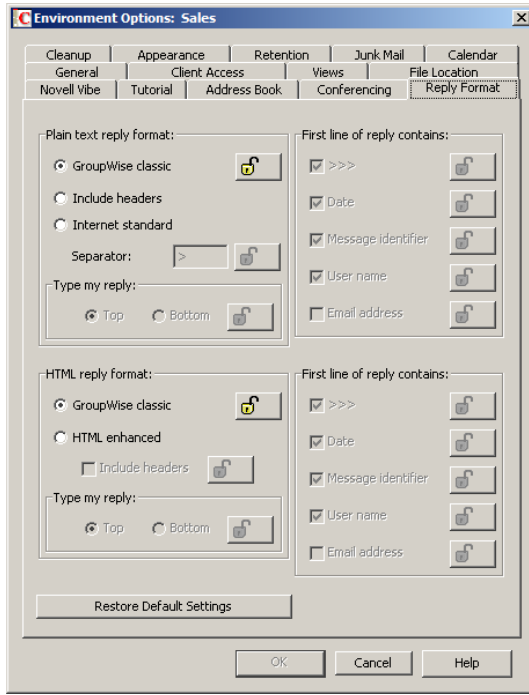
Select this option to allow users to create custom columns in their personal address books.

Environment Options: Conferencing

The Novell Conferencing product is being discontinued.

Environment Options: Reply Format

In the GroupWise Windows client, users can set the format that they want to use for replies to GroupWise items, as described in “[Setting the Default Reply Format](#)” in “[Email](#)” in the *GroupWise 2012 Windows Client User Guide*. The Reply Format options in ConsoleOne control which reply format options are available to users in the GroupWise client.



Plain Text Reply Format

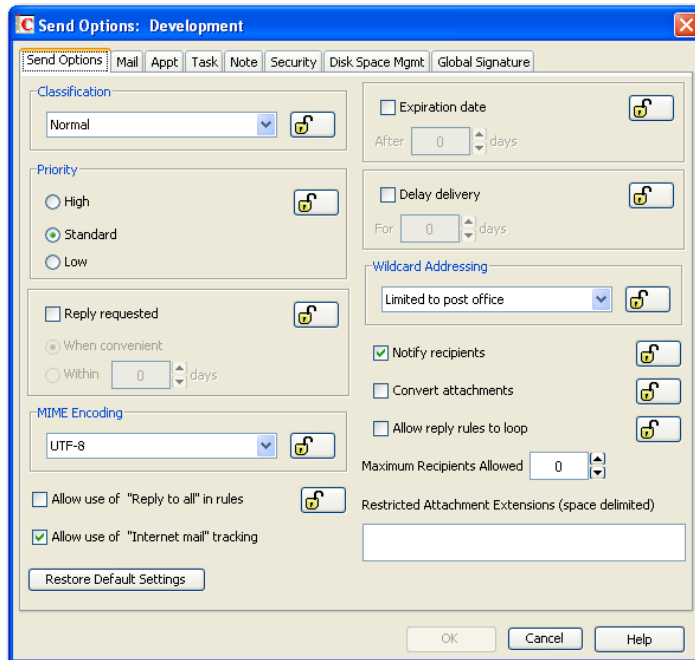
- ◆ **GroupWise Classic:** Provides separator characters, original sender, date, and time.
- ◆ **Include Headers:** Allows the selection of the separator character; provides the original sender, recipient, date, time, and subject.
- ◆ **Internet Standard:** Allows the selection of the separator character; allows you to include the original sender, email address, date, time, and message identifier.
- ◆ **Type My Reply:** Select *Top* or *Bottom* if you selected *Include Headers* or *Internet Standard* above.
- ◆ **First Line of Reply Contains:** Select one or more pieces of information to include in the first line of the reply.

HTML Reply Format

- ◆ **GroupWise Classic:** Provides separator characters, original sender, date, and time.
- ◆ **HTML Enhanced:** Allows the selection of the separator character; allows you to include the original sender, email address, date, time, and message identifier. Select *Include Headers* to provide the original sender, recipient, date, time, and subject instead.
- ◆ **Type My Reply:** Select *Top* or *Bottom* if you selected *Include Headers* above.
- ◆ **First Line of Reply Contains:** Select one or more pieces of information to include in the first line of the reply.

76.2.2 Modifying Send Options

- 1 If the Send Options dialog box is not displayed, follow the instructions in [Section 76, “Setting Defaults for the GroupWise Client Options,”](#) on page 1025 to display the dialog box.



- 2 Click the tab that contains the options you want to change. Refer to the following sections for information about options:

[“Send Options: Send Options”](#) on page 1051

[“Send Options: Mail”](#) on page 1053

[“Send Options: Appointment”](#) on page 1054

[“Send Options: Task”](#) on page 1055

[“Send Options: Note”](#) on page 1056

[“Send Options: Security”](#) on page 1057

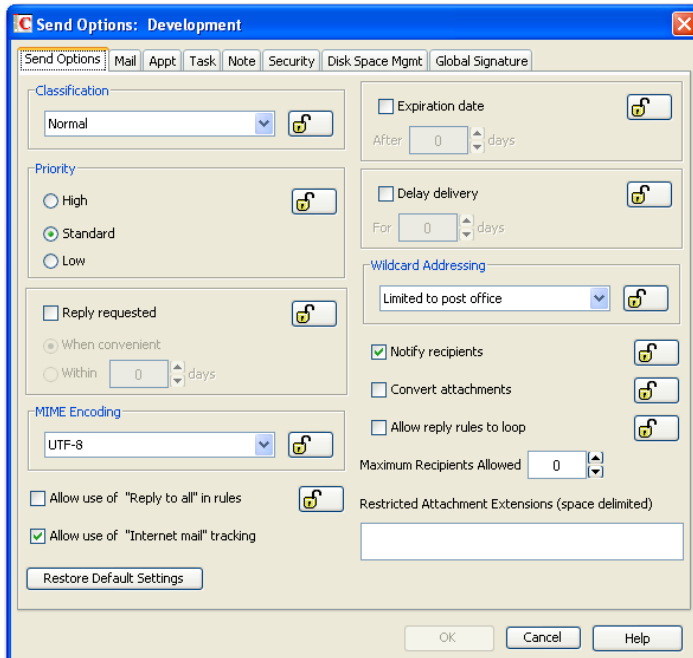
[“Send Options: Disk Space Management”](#) on page 1059

[“Send Options: Global Signature”](#) on page 1060

- 3 If you want to prevent users from changing an option’s setting, click the lock button next to it. After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.
- 4 If you want to return all the options on a tab to their default settings, click *Restore Default Settings*.
- 5 When you are finished, click *OK* to save your changes.

Send Options: Send Options

The *Send Options* determine general settings that apply to all GroupWise item types (mail messages, phone messages, appointments, tasks, and notes).



Classification

Select the default for the security classification label at the top of the message box. The classifications do not provide any encryption or additional security. They are meant to alert the recipient to the relative sensitivity of the item. The options are *Normal*, *Proprietary*, *Confidential*, *Secret*, *Top Secret*, and *For Your Eyes Only*. The default is *Normal*.

Priority

Select *High*, *Standard*, or *Low* as the default item priority. Priority determines which post office directory an item is placed in. This, in turn, determines how quickly items are delivered. High priority items are queued ahead of normal or low priority items.

Reply Requested

Select the *Reply Requested* option to have items always include a reply request. By default, this option is disabled. If you enable the option, select whether the recipient is asked to reply when it is convenient or within a specific number of days.

MIME Encoding

Select the default MIME encoding for all outgoing messages. The MIME encoding is used to specify the character set that is used for all outgoing messages. This is important when your company has users who are using different character sets. For more information, see [Section 7.4, "MIME Encoding,"](#) on page 125.

Allow Use of “Reply to All” in Rules

Select this option to enable users to use the *Reply to All* action when creating rules. By default, this option is disabled, which means that only the *Reply to Sender* action is available.

Allow Use of “Internet Mail” Tracking

Select this option to allow users’ GroupWise clients to automatically embed information in Internet-bound items. The embedded information instructs the receiving system to send back a delivery notification message (if it is supported). By default, this option is enabled.

For this option to work, the Enable Delivery Confirmation option must be enabled in the GroupWise client (*Tools > Options > Send Options > Mail > Enable Delivery Confirmation*). This is the default setting.

Expiration Date

Select this option to have unopened messages expire after the specified number of days. By default, this option is disabled.

Delay Delivery

Select this option to delay the delivery of messages for the specified number of days. For example, if you specify 3 days, a message is not delivered until 3 days after the day it is sent. Messages are delivered at 12:01 a.m. of the appropriate day. By default, this option is disabled.

Wildcard Addressing

Wildcard addressing enables a user to send an item to all users in a post office, domain, GroupWise system, or connected GroupWise system by inserting asterisks (*) as wildcards in email addresses.

- ◆ **Not Allowed:** Select this option to disable wildcard addressing.
- ◆ **Limited to Post Office (Default):** Select this option to limit wildcard addressing to the user’s post office. This means that a user can send an item to all users on the same post office by entering * in the item’s address field.
- ◆ **Limited to Domain:** Select this option to limit wildcard addressing to the user’s domain. This means that a user can send an item to all users in the domain by entering *.* in the item’s address field. A user can also send an item to all users on another post office in the domain by entering *.*post_office_name* in the item’s address field.
- ◆ **Limited to System:** Select this option to limit wildcard addressing to the user’s GroupWise system. This means that a user can send an item to all users in the GroupWise system by entering *.* in the item’s address field. A user can also send an item to all users in another domain by entering *.*domain_name* or to all users in another post office by entering *.*post_office_name*.
- ◆ **Unlimited:** Select this option to allow unlimited use of wildcard addressing. This means that a user can send an item to all users in another GroupWise system by entering *.*post_office_name.domain_name* or *.*domain_name* in the item’s address field.

Notify Recipients

Select this option to have recipients notified when they receive an item, if they are using GroupWise Notify. By default, this option is enabled.

Convert Attachments

Select this option to allow conversion of attachments in items sent to non-GroupWise email systems through a GroupWise gateway.

Allow Reply Rules to Loop

By default, GroupWise does not allow a rule-generated reply to be replied to by another rule-generated reply. This situation, referred to as looping, can quickly increase message traffic. To allow reply rules to loop, select this option.

Maximum Recipients Allowed

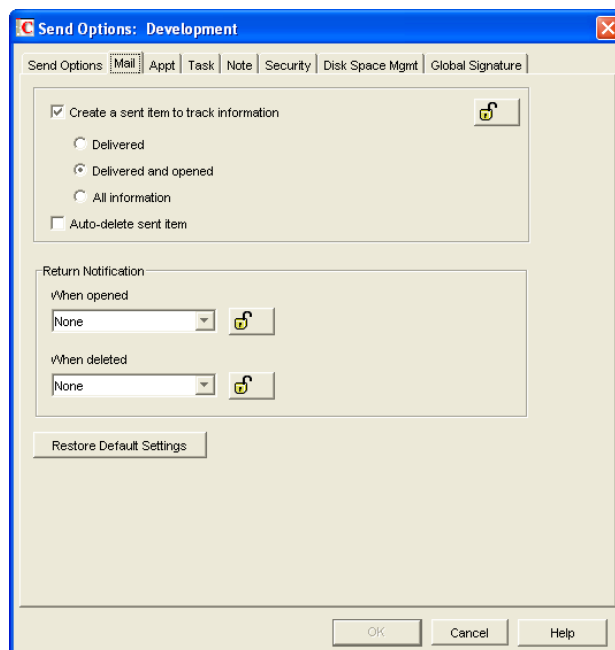
By default, users can send messages to any number of recipients. To prevent users from sending messages to very large numbers of users, perhaps using groups, distribution lists, or wildcard addressing, specify the maximum number of recipients that a message can be sent to. If users exceed the specified maximum, they receive an error instructing them to remove recipients and try again.

Restricted Attachment Extensions

To prevent users from sending specific types of attachments, such as executables, media files, and so on, specify the file extensions that cannot be attached to messages. If users attach a restricted file type, they receive an error indicating the file type restriction, so that they can remove the attachment.

Send Options: Mail

The *Mail* options apply to mail and phone messages only.



Create a Sent Item to Track Information

By default, items the user sends are inserted in the user's Sent Items folder. Deselect this option if you do not want the items placed there. If items are not placed in the Sent Items folder, users cannot check the delivery status of the item. The following options are available only if this option is selected.

- ♦ **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the message to view the status.
- ♦ **Delivered and Opened (Default):** Select this option to track delivered and opened status only. The user can open the Properties window of the sent message to view the status.
- ♦ **All Information:** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the message to view the status.
- ♦ **Auto-Delete Sent Item:** Select this option to automatically delete messages from the user's Mailbox after all the recipients have deleted the messages and emptied them from the Trash.

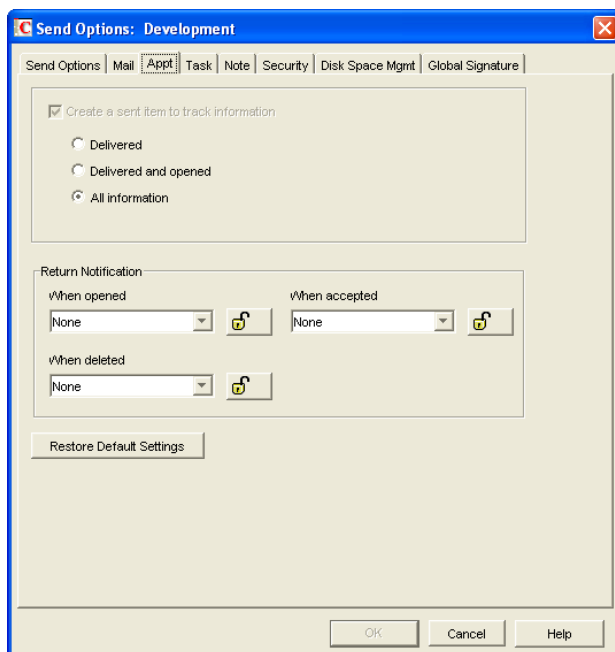
Return Notification

In addition to status tracking information, the user can receive notification when a message is opened or deleted. Choose from the following notification options:

- ♦ **None (Default):** The user does not receive notification.
- ♦ **Mail Receipt:** The user receives a mail message stating that the recipient opened or deleted the message.
- ♦ **Notify:** The user receives notification through GroupWise Notify when the recipient opens or deletes the message.
- ♦ **Notify and Mail:** The user will receive notification through GroupWise Notify and a mail message.

Send Options: Appointment

The *Appointment* options apply to appointments only.



Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the *Mail* tab; it can only be enabled or disabled on the *Mail* tab. If the option is enabled, you can choose from the following status tracking levels:

- ♦ **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the appointment to view the status.
- ♦ **Delivered and Opened:** Select this option to track delivered and opened status only. The user can open the Properties window of the appointment to view the status.
- ♦ **All Information (Default):** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the appointment to view the status.

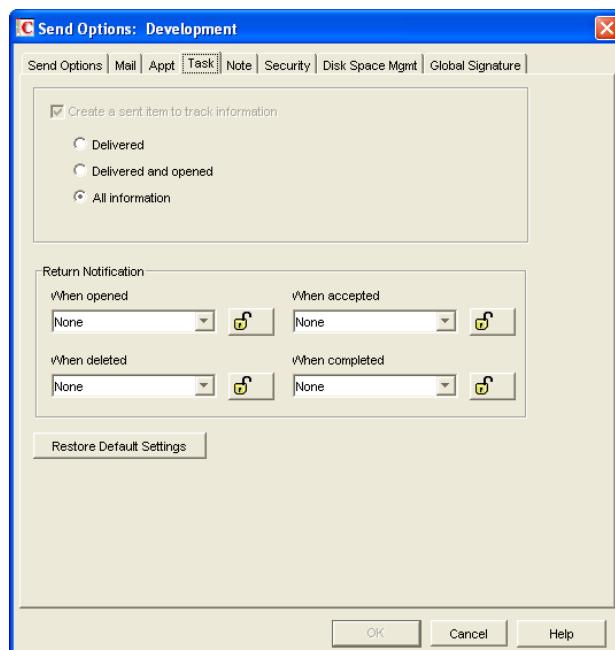
Return Notification

In addition to status tracking information, the user can receive notification when an appointment is opened, accepted, or deleted. Choose from the following notification options:

- ♦ **None (Default):** The user does not receive notification.
- ♦ **Mail Receipt:** The user receives a mail message stating that the recipient opened, accepted, or deleted the appointment.
- ♦ **Notify:** The user receives notification through GroupWise Notify when the recipient opens, accepts, or deletes the appointment.
- ♦ **Notify and Mail:** The user receives notification through GroupWise Notify and a mail message.

Send Options: Task

The *Task* options apply to tasks only.



Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the *Mail* tab; it can only be enabled or disabled on the *Mail* tab. If the option is enabled, you can choose from the following status tracking levels:

- ♦ **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the task to view the status.
- ♦ **Delivered and Opened:** Select this option to track delivered and opened status only. The user can open the Properties window of the task to view the status.
- ♦ **All Information (Default):** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the task to view the status.

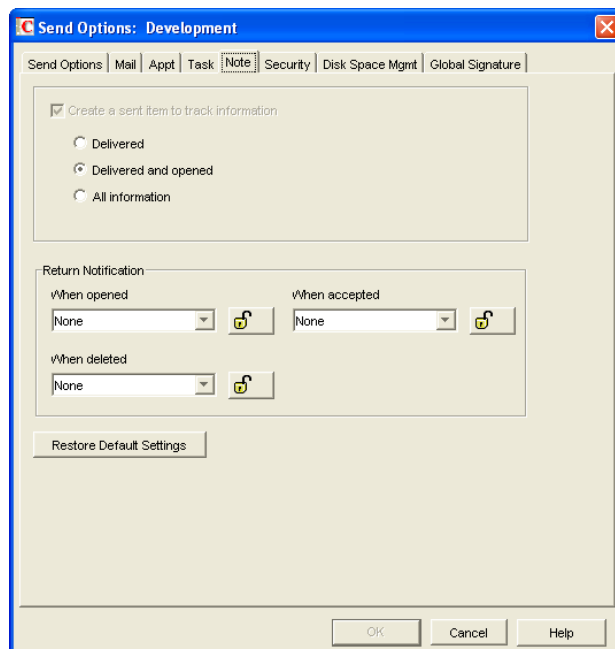
Return Notification

In addition to status tracking information, the user can receive notification when a task is opened, accepted, completed, or deleted. Choose from the following notification options:

- ♦ **None (Default):** The user does not receive notification.
- ♦ **Mail Receipt:** The user receives a mail message stating that the recipient opened, accepted, completed, or deleted the task.
- ♦ **Notify:** The user receives notification through GroupWise Notify when the recipient opens, accepts, completes, or deletes the task.
- ♦ **Notify and Mail:** The user receives notification through GroupWise Notify and a mail message.

Send Options: Note

The *Note* options apply to notes only.



Create a Sent Item to Track Information

The setting for this option is inherited from the setting on the *Mail* tab; it can only be enabled or disabled on the *Mail* tab. If the option is enabled, you can choose from the following status tracking levels:

- ♦ **Delivered:** Select this option to track delivered status only. The user can open the Properties window of the note to view the status.
- ♦ **Delivered and Opened (Default):** Select this option to track delivered and opened status only. The user can open the Properties window of the note to view the status.
- ♦ **All Information:** Select this option to track all status information (delivered, opened, deleted, emptied). The user can open the Properties window of the note to view the status.

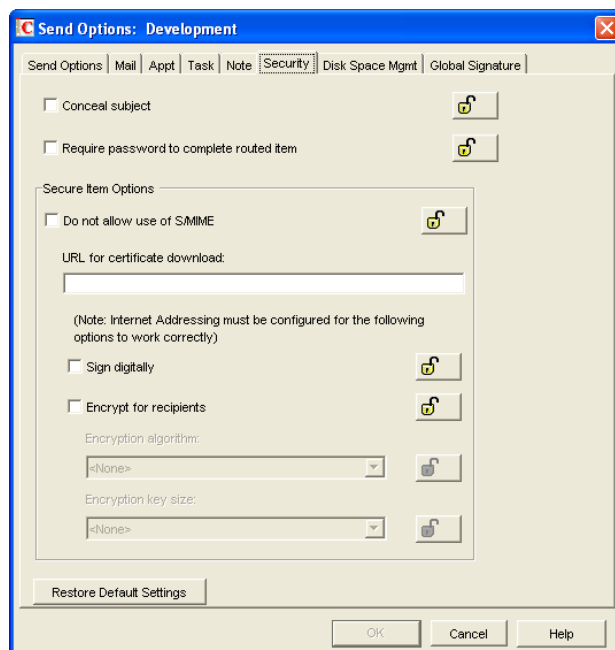
Return Notification

In addition to status tracking information, the user can receive notification when a note is opened or deleted. Choose from the following notification options:

- ♦ **None (Default):** The user does not receive notification.
- ♦ **Mail Receipt:** The user receives a mail message stating that the recipient opened or deleted the note.
- ♦ **Notify:** The user receives notification through GroupWise Notify when the recipient opens or deletes the note.
- ♦ **Notify and Mail:** The user receives notification through GroupWise Notify and a mail message.

Send Options: Security

The *Security* options apply to all GroupWise item types (mail messages, phone messages, appointments, tasks, and notes).



Conceal Subject

Select this option to conceal the item's subject so the notification that appears on the recipient's screen does not include the subject. The subject of the item is also concealed in the recipient's mailbox and the sender's Sent Items folder. It is visible only when the item is being read.

Require Password to Complete Routed Item

Select this option to require a user to enter a password before completing a routed item.

Secure Items Options

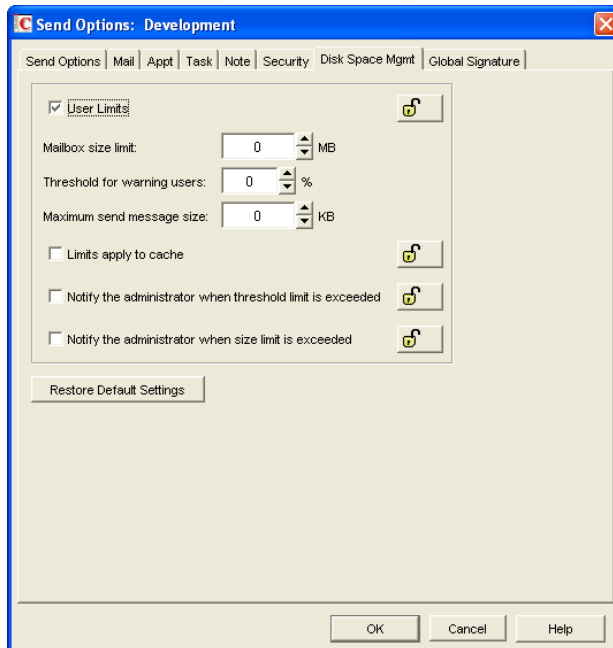
If users have installed security providers on their workstations, select the options you want them to use.

- ♦ **Do Not Allow Use of S/MIME:** Select this option to disable S/MIME functionality. This disables the *Encrypt* and *Digitally Sign* buttons (and other related S/MIME functionality) in the GroupWise client. By default, this option is enabled. When it is enabled, you can modify the rest of the options in the dialog box.
- ♦ **URL for Certificate Download:** Specify the Internet address of your preferred certification authority. If it is not otherwise changed in this field, the GroupWise client accesses <http://www.novell.com/groupwise/certified.html>, which lists several common certification authorities.
- ♦ **Sign Digitally:** Select this option to enable users to add a digital signature to their outgoing messages. Recipients of a digitally signed item who have S/MIME-enabled email products are able to verify that the item is actually from the sender. This setting is not a useful security measure unless you lock it as the default.
- ♦ **Encrypt for Recipients:** Select this option to enable users to encrypt an outgoing item so they can ensure that the intended recipients who have an S/MIME-enabled email product are the only individuals who can read the item. This setting is not a useful security measure unless you lock it as the default.

If you enable the *Encrypt for Recipients* options, you can set the encryption algorithm and key size. The available algorithm methods (RC2, RC4, DES, 3DES) are trusted algorithms that encrypt or transform data to mask the original content. The key size sets the default size (in bits) of the encryption key that is used with the algorithm you select. These settings are not useful security measures unless you lock them.

Send Options: Disk Space Management

The *Disk Space Management* options let you enforce disk space limitations for users on a post office.



User Limits

Select this option if you want to impose limits on the size of users' mailboxes or the size of messages they can send. By default, this option is disabled, so there are no size limits. If you enable it, you can modify the following options:

- ♦ **Mailbox Size Limit:** Specify the maximum amount of post office disk space available to each user for storing message and attachment files. The setting uses logical disk space because attachments are shared by all recipient users on the same post office. Messages in shared folders are counted as disk space only for the owner of the shared folder. If you do not want to limit the mailbox size, set the value to zero (0). The physical maximum size limit for a mailbox is 4 TB.

If users meet or exceed their mailbox size limits, they cannot send items until their mailboxes are under the size limit. Users can reduce the size of their mailboxes by deleting or archiving items.

- ♦ **Threshold for Warning Users:** Select the mailbox capacity (as a percentage) that must be reached before the user is warned that his or her mailbox is reaching its limit. For example, if the mailbox size limit is 200 MB and the threshold is set at 75%, users receive warnings when their mailboxes reach 150 MB. Set the value to 0 or 100 if you do not want users to receive a warning.
- ♦ **Maximum Send Message Size:** Specify the maximum size of a message (in kilobytes) that a user can send using the GroupWise client. If the user sends an item that exceeds this size, a message notifies the user that the item is too large to send.

You can also set message size limits at the post office level through POA configuration, at the domain level through MTA configuration, and at the GroupWise system level through GWIA configuration, as described in [Section 12.3.5, "Restricting the Size of Messages That Users Can Send,"](#) on page 201.

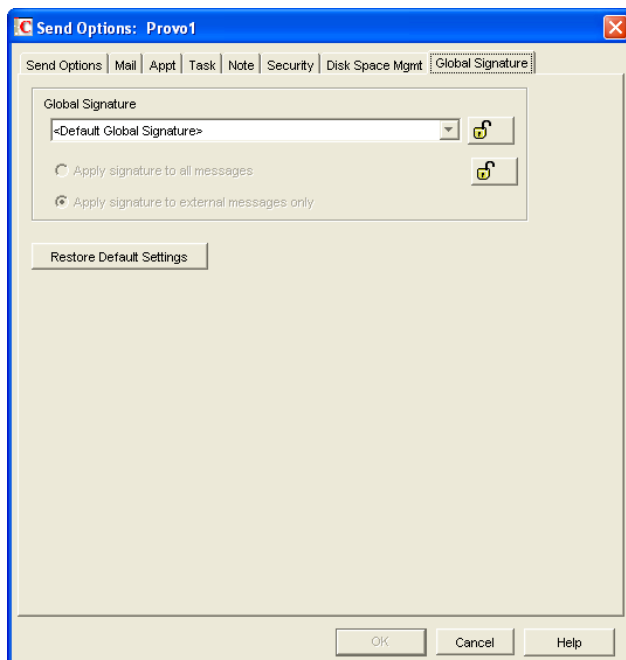
- ♦ **Limits Apply to Cache:** Select this option to prevent users from sending from their Caching or Remote mailboxes when their Caching or Remote mailboxes exceed the limits you have set for Online mailboxes, as described in [Section 12.3.4, “Enforcing Mailbox Size Limits,”](#) on page 200. You can use this option in conjunction with the *Perform Maintenance Purges on Caching/Remote* option to control the size of users’ Caching and Remote mailboxes.

If you impose this limit on users who have existing Caching or Remote mailboxes, their Caching or Remote mailboxes might be reduced in size in order to meet the new disk space limit. Such users should be warned in advance so that they can back up their Caching or Remote mailboxes before the size reduction takes place. Otherwise, users could lose messages that they want to keep.

- ♦ **Notify the Administrator When Threshold Limit Is Exceeded:** Select this option so that the administrator is notified along with the user when the user’s mailbox exceeds the size established in the *Threshold for Warning Users* field. The administrator who receives the notification must be defined on the Identification page of the Domain object.
- ♦ **Notify the Administrator When Size Limit Is Exceeded:** Select this option so that the administrator is notified when the user’s mailbox exceeds the size established in the *Mailbox Size Limit* field. The administrator who receives the notification must be defined on the Identification page of the Domain object.

Send Options: Global Signature

The *Global Signature* option lets you set the global signature. To set options at the domain level, select a domain. To set options at the post office level, select a post office. To set options for individual users, select one or more users.



Global Signature

- 1 Select a global signature to append to users’ messages.

When enabled, global signatures are automatically appended to every message that is sent by the users. For more information, see [Section 4.14, “Global Signatures,”](#) on page 94.

- 2 Select *Apply the signature to all messages* to add the signature to all internal or external messages.

or

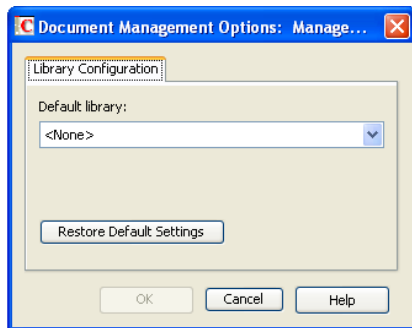
Select *Apply signature to external messages only* to apply the signature to messages that are sent through the GWIA.

If you select *Default Global Signature*, the default signature that is used by the GWIA is applied. If you select *None*, then no signature is applied.

NOTE: All *Global Signature* options pertain only to the Windows client.

76.2.3 Modifying Documents Options

- 1 If the Documents Options dialog box is not displayed, follow the instructions in [Section 76, “Setting Defaults for the GroupWise Client Options,”](#) on page 1025 to display the dialog box.

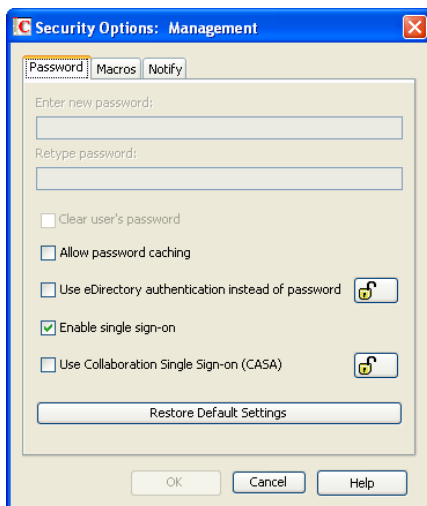


- 2 Select the default library, then click *OK* to save your changes.

For information about libraries and document management, see [Part VII, “Libraries and Documents,”](#) on page 313.

76.2.4 Modifying Security Options

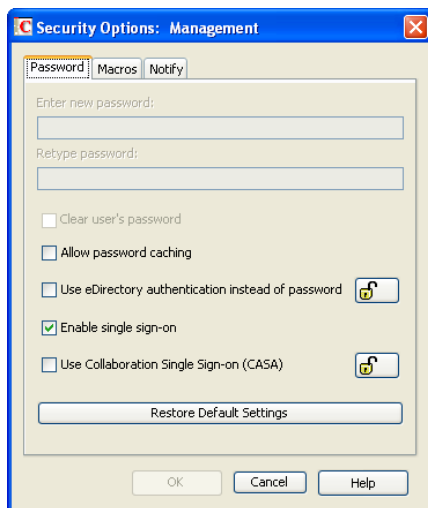
- 1 If the Security Options dialog box is not displayed, follow the instructions in [Section 76, “Setting Defaults for the GroupWise Client Options,”](#) on page 1025 to display the dialog box.



- 2 Click the tab that contains the options you want to change. Refer to the following sections for information about options:
 - “Security Options: Password” on page 1062
 - “Security Options: Macros” on page 1064
 - “Security Options: Notify” on page 1064
- 3 If you want to prevent users from changing an option’s setting, click the lock button next to it. After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.
- 4 If you want to return all the options on a tab to their default settings, click *Restore Default Settings*.
- 5 When you are finished, click *OK* to save your changes.

Security Options: Password

The *Password* options let you reset a user’s password and enable various methods by which a user can set up the GroupWise client so that he or she does not have to enter a password at startup.



For background information about passwords, see [Chapter 82, “GroupWise Passwords,”](#) on [page 1099](#).

Enter New Password

This option is available only when setting client options for an individual user. You can use this option to set or reset a user’s password. You should advise the user to change the password as soon as possible.

Retype Password

This option is available only when setting client options for an individual user. If you enter a new password, verify it by retyping it in this field.

Clear User Password

This option is available only when setting client options for an individual user. If a user forgets his or her personal password, select this option to clear the password. The user can then enter a new password at his or her discretion. In a high security post office, it might be necessary to set a new password after clearing the old one.

Allow Password Caching

Select this option to allow users to enable the *Remember My Password* option under *Security* options in the GroupWise client. The *Remember My Password* option stores the user's password in the workstation's Windows password list so that the user does not need to enter the password when starting GroupWise. This option is disabled by default.

This option applies only to older GroupWise clients running on older Windows versions, such as Windows 2000 and earlier, which are not supported for the GroupWise 2012 Windows client.

Allow eDirectory Authentication Instead of Password

Select this option to allow users to select the *No Password Required with eDirectory* option under *Security* options in the GroupWise client. When this option is selected in the client, the user can access his or her mailbox without requiring a password if he or she is already logged in to Novell eDirectory. Mailbox access is granted based on eDirectory authentication, not on password information. This option is available only if eDirectory authentication is enabled for the post office, as described in [Section 11.2.11, "Selecting a Post Office Security Level," on page 180](#).

NOTE: In versions of GroupWise prior to the GroupWise 5.5 Enhancement Pack, this option was called *Allow NDS Single Sign-on*. The option name has been changed to avoid confusion with the Novell Single Sign-on product.

Enable Single Sign-On

Select this option to give users the *Use Single Sign-on* option under *Security Options* in the GroupWise client. This option lets the user access his or her mailbox without reentering the password. After a user selects *Use Single Sign-On* in the GroupWise client, the GroupWise password is stored in eDirectory for the currently logged-in user.

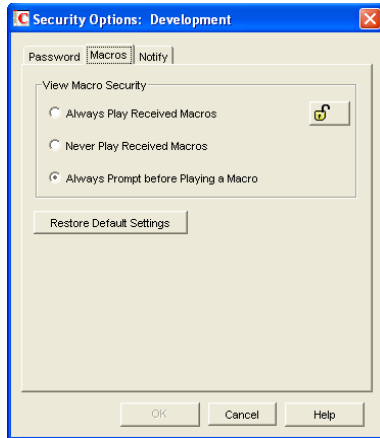
IMPORTANT: Novell Single Sign-on must be installed on the user's workstation in order for this option to take effect.

Use Collaboration Single Sign-on (CASA)

Select this option to give users the *Use Collaboration Single Sign-on (CASA)* option under *Security Options* in the GroupWise Windows client. This option lets the user access his or her mailbox without reentering the password if the *Collaboration Single Sign-on (CASA)* software is installed. After a user selects *Use Collaboration Single Sign-On (CASA)* in the GroupWise client and if the CASA client is installed, the GroupWise password is stored for the currently logged-in user.

Security Options: Macros

The *Macros* option determines how GroupWise handles macros that are included in received messages.



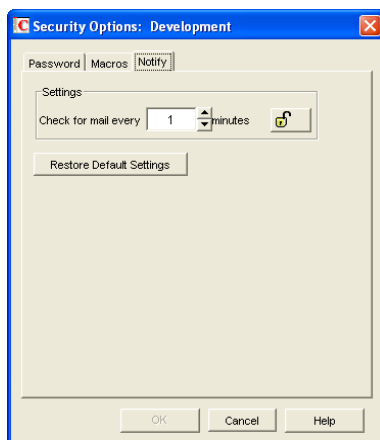
View Macro Security

Choose from the following settings to determine the level of macro security:

- ◆ **Always Play Received Macros:** Select this option to play attached macros when the message is opened.
- ◆ **Never Play Received Macros:** Select this option to ignore attached macros. Macros do not play.
- ◆ **Always Prompt Before Playing a Macro (Default):** Select this option to have the user prompted to play the macro.

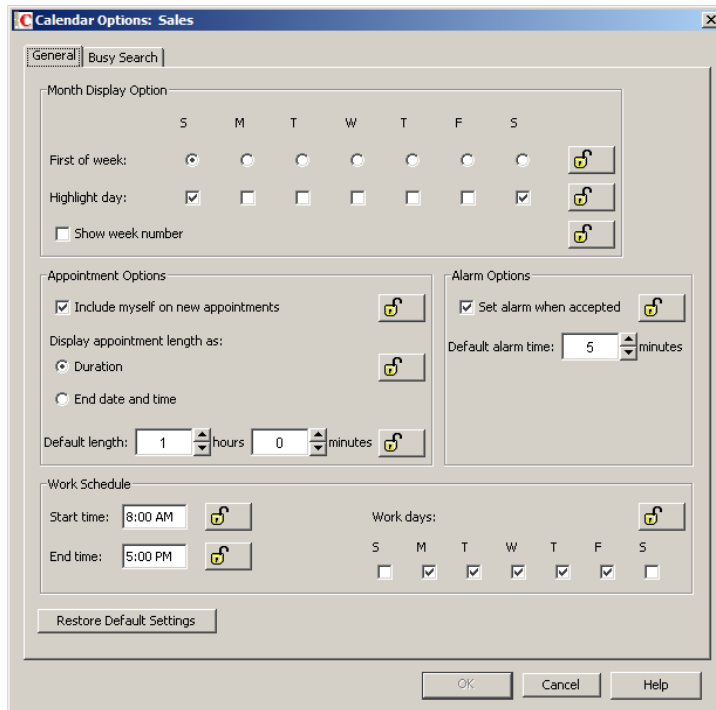
Security Options: Notify

The *Notify* option determines how often GroupWise Notify checks a user's mailbox for newly received items. If new items are detected, the user is notified. The default is every minute.



76.2.5 Modifying Calendar Options

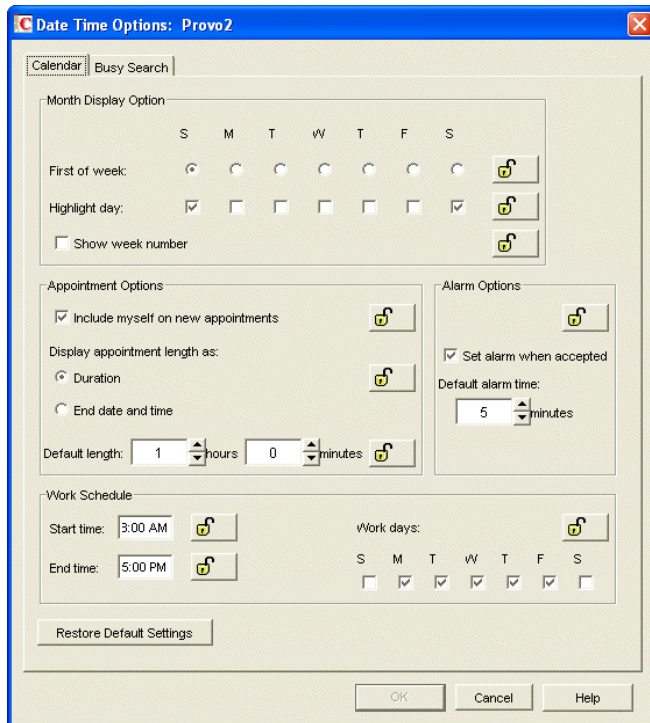
- 1 If the Calendar Options dialog box is not displayed, follow the instructions in [Section 76, “Setting Defaults for the GroupWise Client Options,”](#) on page 1025 to display the dialog box.



- 2 Click the tab that contains the options you want to change. Refer to the following sections for information about options:
 - “[Calendar Options: General](#)” on page 1066
 - “[Calendar Options: Busy Search](#)” on page 1067
- 3 If you want to prevent users from changing an option’s setting, click the lock button next to it. After you click it, the lock button indicates whether the setting is locked at the domain level, the post office level, or the user level.
- 4 If you want to return all the options on a tab to their default settings, click *Restore Default Settings*.
- 5 When you are finished, click *OK* to save your changes.

Calendar Options: General

The *General* options determine basic settings for the GroupWise Calendar.



Month Display Option

Select from the following options to determine how the month calendar is displayed:

- ◆ **First of Week:** Select the day of the week that you want to display as the first day on the calendar.
- ◆ **Highlight Day:** Select any days you want highlighted, such as weekends and holidays.
- ◆ **Show Week Number:** Select this option to display the week number (1 through 52) at the beginning of the calendar week.

Appointment Options

Select from the following options to determine how appointments are handled:

- ◆ **Include Myself on New Appointments:** Select this option to have the sender automatically included in the appointment's To: list. This option is enabled by default.
- ◆ **Display Appointment Length As:** When creating an appointment, the sender must specify the appointment's length. You can use this option to determine whether the sender enters a duration for the appointment or an end time for the appointment. Select the *Duration* setting to have appointments display a *Duration* field that the sender must fill in (for example, 30 minutes, 1 hour, or 10 hours). Select the *End Date and Time* setting to have appointments display *End Date and Time* fields that the sender must fill in (for example, June 3, 2010 and 10:00 a.m.). The default setting is *Duration*.

- ♦ **Default Length:** Select the default length for appointments. Users can change the length. If the appointment's length is displayed as a duration, the duration defaults to this length. If it is displayed as an end date and time, the end time defaults to the start time plus the default length (for example, if the start time is 9:00 a.m. and the default length is 1 hour, the end time defaults to 10:00 a.m).

Alarm Options

Users can set appointment alarms so that they are notified prior to an appointment time. Select from the following options to determine the default settings for an alarms:

- ♦ **Set Alarm When Accepted:** Select this option to have an alarm automatically set when the user accepts an appointment. By default, this option is enabled.
- ♦ **Default Alarm Time:** Select the number of minutes before an appointment to notify the user. The default is 5 minutes.

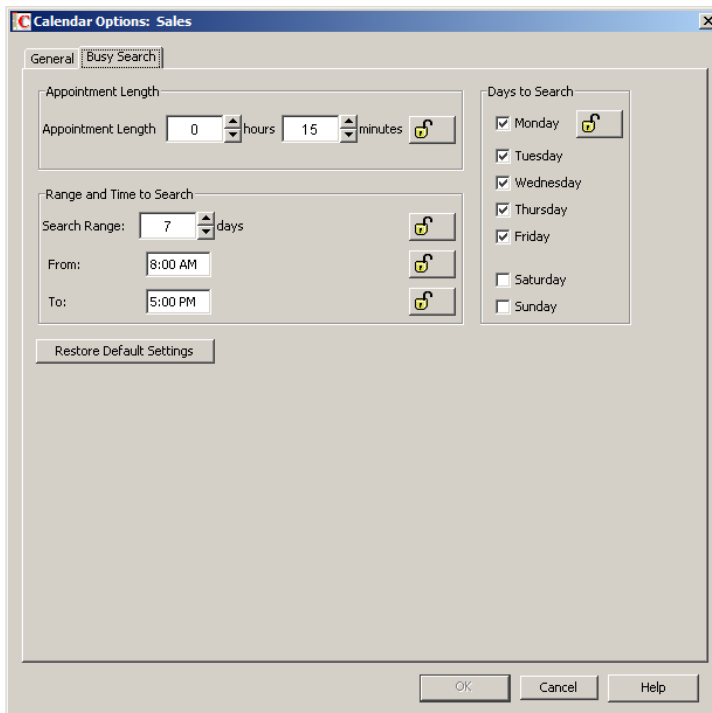
Work Schedule

The work schedule determines the user's normal work days and hours. In the calendar and during busy searches, any days or hours outside of the work schedule are represented by gray squares (Out of Office). Users can still be scheduled for appointments during non-work hours.

- ♦ **Start Time:** Select the daily start time. The default is 8:00 a.m.
- ♦ **End Time:** Select the daily end time. The default is 5:00 p.m.
- ♦ **Work Days:** Select the work days. The start time and end time are applied to each work day.

Calendar Options: Busy Search

The *Busy Search* options determine the amount of free time required for the appointment and the range of dates to search.



Appointment Length

Set the default appointment length to search. You can set the length in 15-minute increments. The default is 15 minutes. This setting is used only when the user does a busy search through the *Busy Search* option on the *Tools* menu. Otherwise, the default appointment length defined on the *Calendar* tab is used (see “[Calendar Options: General](#)” on page 1066).

Range and Time to Search

Specify the number of days to include in the search, then set the daily start and end times for the search.

Days to Search

Select the days to search. By default, the typical work days (Monday through Friday) are selected.

76.3 Resetting Client Options to Default Settings

You can reset client options to the defaults for one or more users. This enables you to establish your preferred settings, and then lock those settings so that users cannot change them in the future.

- 1 In ConsoleOne, select one or more User objects (or GroupWise External Entity objects).
- 2 Click *Tools > GroupWise Utilities > Mailbox/Library Maintenance*.
- 3 In the GroupWise Objects list, select *Users/Resources*.
- 4 In the *Actions* list, select *Reset Client Options*, then click *Run*.

77 Distributing the GroupWise Windows Client

You can distribute the GroupWise Windows client software in various ways:

- ♦ [Section 77.1, “Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client,” on page 1069](#)
- ♦ [Section 77.2, “Using ZENworks Configuration Management to Distribute the GroupWise Windows Client,” on page 1085](#)

For information about client licensing requirements, see [Section 12.4, “Auditing Mailbox License Usage in the Post Office,” on page 207](#).

77.1 Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client

The GroupWise Windows client Setup program (`setup.exe`) includes an AutoUpdate feature that helps you keep users’ Windows client software up to date. Each time the GroupWise Windows client starts, it checks with the POA for the user’s post office to find out if new Windows client software is available in the post office’s software distribution directory. When new software is available and AutoUpdate is enabled, the Setup program can prompt the user to install the updated software.

By default, AutoUpdate checks for a mapped drive to a software distribution directory from which to install the client software. This requires that users have rights to directly access the software distribution directory. To eliminate the need to give users rights to the software distribution directory, you can configure the SetupIP feature to download the client software from a Web server, so that the client installation can run locally on users’ workstations.

After AutoUpdate locates the software, either across a mapped drive or by downloading it from a Web server, the installation of the client software by the client Setup program is controlled by the setup configuration file (`setup.cfg`).

- ♦ [Section 77.1.1, “Preparing for AutoUpdate,” on page 1070](#)
- ♦ [Section 77.1.2, “Working with the Setup Configuration File,” on page 1076](#)
- ♦ [Section 77.1.3, “Enabling AutoUpdate in ConsoleOne,” on page 1082](#)
- ♦ [Section 77.1.4, “Understanding the User’s AutoUpdate Experience,” on page 1083](#)
- ♦ [Section 77.1.5, “Using the AutoUpdate Error Log Files,” on page 1084](#)
- ♦ [Section 77.1.6, “Disabling Your AutoUpdate Customizations,” on page 1084](#)

77.1.1 Preparing for AutoUpdate

- ♦ [“Preparing Your Software Distribution Directory to Support AutoUpdate” on page 1070](#)
- ♦ [“Preparing for Windows Client Installation from a Mapped Drive” on page 1071](#)
- ♦ [“Preparing for Windows Client Installation from a Web Server” on page 1071](#)

Preparing Your Software Distribution Directory to Support AutoUpdate

During the installation of GroupWise Administration, you had the opportunity to plan and set up a software distribution directory, as described in [“GroupWise Software Distribution Directory”](#) in [“Installing a Basic GroupWise System”](#) in the *GroupWise 2012 Installation Guide*.

On Windows, if you selected *GroupWise Client for Windows* when you initially created your software distribution directory, the GroupWise Windows client software was copied from the downloaded *GroupWise 2012* software image into the `client` subdirectory of the software distribution directory.

On Linux, the GroupWise Windows client software is always copied into the software distribution directory, because the Linux GroupWise Installation program does not include an option for selecting *GroupWise Client for Windows*.

The default location of the software distribution directory varies by platform:

Linux: `/opt/novell/groupwise/software`

Windows: `c:\grpwise\software`

If the software distribution directory already contains the Windows client software, follow the instructions for the type of client installation you want to perform:

- ♦ [“Preparing for Windows Client Installation from a Mapped Drive” on page 1071](#)
- ♦ [“Preparing for Windows Client Installation from a Web Server” on page 1071](#)

If you have not yet copied the Windows client software to the software distribution directory:

- 1 Start the [Windows GroupWise Installation program](#).
- 2 Click *Install GroupWise System*, click *Yes* to accept the License Agreement, then click *Next* to accept a standard installation.
- 3 Select *Install Individual Components* and deselect *GroupWise Agents*, so that only *GroupWise Administration* is selected, then click *Next*.
- 4 Deselect *Install Administration Files*, so that only *Copy Files to a Software Distribution Directory* is selected, then click *Next*.
- 5 Specify or browse to and select your software distribution directory, then click *Next*.
- 6 Select *GroupWise Client for Windows*, then click *Next*.
- 7 Review your selections, then click *Install*.
- 8 When the Windows client software files have been copied to the software distribution directory, click *Finish*.

- 9 If you want to distribute the Windows client software from a mapped network drive, continue with [Preparing for Windows Client Installation from a Mapped Drive](#).

or

If you want to distribute the Windows client software from a Web server, so that the Windows client users do not need access rights to the software distribution directory, skip to “[Preparing for Windows Client Installation from a Web Server](#)” on page 1071.

Preparing for Windows Client Installation from a Mapped Drive

- 1 Make sure that Windows client users have a drive mapped to the software distribution directory.

If the software distribution directory is on Linux and you need assistance with this task, you can follow the same basic procedure described in “[Installing the GroupWise Windows Client from the Linux GroupWise 2012 Software Image](#)” in “[Installation](#)” in the *GroupWise 2012 Installation Guide* to set up the connection.

- 2 (Conditional) If the software distribution directory is on Linux, modify the configuration of the software distribution directory to make it available from the point of view of users’ Windows workstations:

- 2a In Windows ConsoleOne, click *Tools > GroupWise System Operations > Software Directory Management*.

- 2b Select the software distribution directory on the Linux server where the Windows client software is located, then click *Edit*.

- 2c In the *UNC Path* field, change the Linux path provided by the Linux GroupWise Installation program or Linux ConsoleOne to the UNC path required to access the location from the point of view of Windows, then click *OK*.

IMPORTANT: Do not edit this software distribution directory in Linux ConsoleOne in the future. Doing so would change the location back to a Linux path and cause the AutoUpdate process to fail.

- 2d Click *Close* to close the Software Distribution Directory Management dialog box.

- 3 Make sure that users have Read and Scan rights to the following locations in the software distribution directory:

`software_distribution_directory\client`

`software_distribution_directory\client\win32`

- 4 Skip to “[Customizing the Setup Configuration File](#)” on page 1079.

Preparing for Windows Client Installation from a Web Server

When the Windows client software was copied to the software distribution directory, the files required for installing the Windows client from a Web server were copied to:

`software_distribution_directory/admin/utility/setupip`

This applies to software distribution directories on Linux and on Windows. SetupIP can be configured to install the Windows client software from the Apache Web server on Linux or from the Internet Information Service (IIS) Web server on Windows.

- 1 Create a directory in the document root directory of your Web server for the GroupWise client software files used by SetupIP, for example:

Apache on Linux: `/srv/www/htdocs/gwclient`

IIS on Windows: `c:\InetPub\wwwroot\gwclient`

- 2 Create a win32 subdirectory under the client software directory that you created in [Step 1](#).

After you customize the setup configuration file (`setup.cfg`), as described in [“Customizing the Setup Configuration File” on page 1079](#), you will copy it to the win32 subdirectory.

- 3 Browse to the following subdirectory in your software distribution directory:

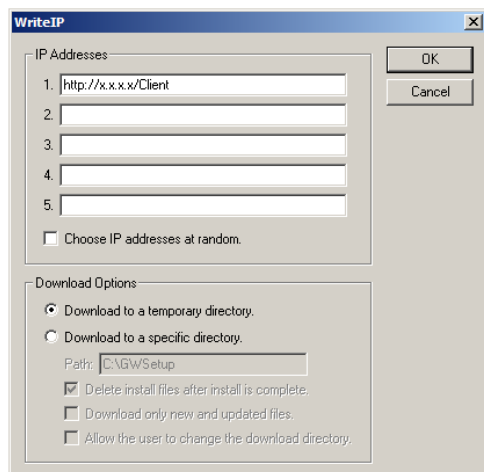
`software_distribution_directory/admin/utility/setupip`

- 4 Copy the `setupip.fil` file and any language-specific `setupip.language_code` files for languages you want to install, from the `utility/setupip` directory to the client software directory that you created in [Step 1](#).

All language-independent Windows client software files are included in the `setupip.fil` file. The `setupip.language_code` file for each client language (`setupip.en`, `setupip.de`, `setupip.fr`, and so on) contains all client software files for the specific language indicated by the language code. If you copy multiple `setupip.language_code` files to the Web server, users are prompted for which languages they want to install.

- 5 On Windows, in the `utility/setupip` directory, run the WriteIP program (`writeip.exe`).

If the WriteIP program is located on a Linux server, you can use the same procedure for creating a connection from Windows to Linux when setting up SetupIP as you use when setting up ConsoleOne for use from Windows to Linux. For assistance, see [Section 2.3, “ConsoleOne in a Multiple-Platform Environment,” on page 48](#).



The WriteIP program (`writeip.exe`) creates a customized SetupIP program (`setupip.exe`) designed to work with the local Web server.

- 6 Specify the IP address location for the local `setupip.fil` file.

For example, you can specify:

`http://172.16.5.18/gwclient`

or

`http://intranet.yourcompanyname.com/gwclient`

You can include proxy and port information, for example:

`http://name.yourcompanyname.com/gwclient;proxy.place.mycompany:1690`

You can specify as many as five locations where you have made the GroupWise client software available on Web servers. During AutoUpdate, each location is checked, in order, until a connection is made.

- 7 (Optional) If you specify multiple locations, select *Choose IP Address at Random* so that the order in which the locations are checked is selected randomly when AutoUpdate occurs.

This balances the load on the Web servers.

- 8 (Optional) Select download options:

Download to a Temporary Directory: Select this option to download the Windows client software into a temporary directory that is automatically deleted after the user installs the updated client software.

Download to a Specific Directory: Select this option to control where and how the Windows client software is downloaded.

- ♦ **Path:** Specify the directory where you want SetupIP to download the Windows client software.
- ♦ **Delete Install Files after Install Is Complete:** Select this option to clean up the user's workstation after the Windows client software is installed.
- ♦ **Download Only New and Updated Files:** Select this option to shorten download time by downloading only new and modified software files.
- ♦ **Allow the User to Change the Download Directory:** Select this option to prompt the user for the location to download the software files.

- 9 Click *OK* to create a customized `setupip.exe` file based on the settings you selected, then click *OK* again to exit the WriteIP program.

The `writeip.ini` file is also created, which stores the options you selected when running the WriteIP program.

- 10 Copy the custom `setupip.exe` file from the `utility/setupip` directory to the `software_distribution_directory/client/win32` directory, so that it is in the same directory with the Windows client Setup program (`setup.exe`).

- 11 Configure your Web server to support SetupIP:

- ♦ ["Apache on Linux" on page 1073](#)
- ♦ ["IIS on Windows Server 2008" on page 1074](#)
- ♦ ["IIS on Windows Server 2003" on page 1075](#)

Apache on Linux

- 1 Open the Apache configuration file (`/etc/apache2/httpd.conf`) in a text editor.
- 2 Search for the following section:

```
<Directory />
```

- 3 After the default `Directory` section, add the following section for the GroupWise client software:

```
<Directory /srv/www/htdocs/gwclient>
  Options Indexes
</Directory>
```

- 4 On the `Directory` line, specify the client software directory that you created in [Step 1](#) in “[Preparing for Windows Client Installation from a Web Server](#)” on page 1071.
- 5 Save the file.
- 6 Restart Apache:

```
rcapache2 restart
```

- 7 Test the availability of the client software on the Web server by displaying the following URL and verifying the contents of the `win32` directory:

```
http://web_server_address/gwclient
```

Index of /gwclient

Name	Last modified	Size	Description
 Parent Directory		-	
 setupip.en	12-Apr-2012 19:49	4.7M	
 setupip.fil	12-Apr-2012 19:49	87M	
 win32/	12-Apr-2012 19:50	-	

- 8 Skip to [Working with the Setup Configuration File](#).

IIS on Windows Server 2008

- 1 On Windows Server 2008, click *Start > Administrative Tools > Internet Information Services (IIS) Manager*.
- 2 Expand the Local Computer object, expand the Sites folder, expand your Web site, then select the client software directory that you created in [Step 1](#) in “[Preparing for Windows Client Installation from a Web Server](#)” on page 1071.
- 3 Enable directory browsing so that the `gwclient` directory can be accessed:
 - 3a In the Features View, double-click *Directory Browsing*.
 - 3b In the *Actions* pane, click *Enable*.
 - 3c Click the client software directory to return to the Features View.
- 4 Configure IIS to allow the download of the client software files:
 - 4a In the Features View, double-click *MIME Types*.
 - 4b In the *Actions* pane, click *Add*.
 - 4c In the *File name extension* field, type `.*` (a period followed by an asterisk).
 - 4d In the *MIME type* field, type `application/octet-stream`.
 - 4e Click *OK*.
 - 4f Click the client software directory to return to the Features View.
- 5 (Conditional) If you have configured file filtering at a higher level in this Web site, configure IIS to not filter out files in the client software directory:
 - 5a In the Features View, double-click *Request Filtering*.
 - 5b Click *Allow File Name Extension*.

- 5c In the *File name extension* field, type `.*` (a period followed by an asterisk).
- 5d Click *OK*.
- 6 Close IIS Manager.
- 7 Restart IIS:
 - 7a Click *Start > Administrative Tools > Services*.
 - 7b Right-click *World Wide Web Publishing Service*, then click *Restart*.
- 8 Test the availability of the client software on the Web server by displaying the following URL and verifying the contents of the `win32` directory:

`http://web_server_address/gwclient`

Index of /gwclient

Name	Last modified	Size	Description
 Parent Directory		-	
 setupip.en	12-Apr-2012 19:49	4.7M	
 setupip.fil	12-Apr-2012 19:49	87M	
 win32/	12-Apr-2012 19:50	-	

- 9 Skip to [Working with the Setup Configuration File](#).

IIS on Windows Server 2003

- 1 On Windows Server 2003, click *Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager*.
- 2 Expand the *Local Computer* object, then expand the *Web Sites* folder.
- 3 Right-click your *Web site*, then click *Properties*.
- 4 On the *Home Directory* tab, select *Directory Browsing*, then click *OK*.
- 5 Restart IIS:
 - 5a Click *Start > Administrative Tools > Services*.
 - 5b Right-click *World Wide Web Publishing Service*, then click *Restart*.
- 6 Test the availability of the client software on the Web server by displaying the following URL:

`http://web_server_address/gwclient`

Index of /gwclient

Name	Last modified	Size	Description
 Parent Directory		-	
 setupip.en	12-Apr-2012 19:49	4.7M	
 setupip.fil	12-Apr-2012 19:49	87M	
 win32/	12-Apr-2012 19:50	-	

- 7 Continue with [Working with the Setup Configuration File](#).

77.1.2 Working with the Setup Configuration File

The AutoUpdate process is controlled by the setup configuration file (`setup.cfg`).

- ♦ [“Understanding the Setup Configuration File” on page 1076](#)
- ♦ [“Customizing the Setup Configuration File” on page 1079](#)
- ♦ [“Adding LDAP Directory Service Accounts to the Setup Configuration File” on page 1081](#)

Understanding the Setup Configuration File

A default setup configuration file (`setup.cfg`) is provided in the following directory:

`software_distribution_directory\client`

The setup configuration file is an ASCII text file that supports extended ASCII characters. The file contains the responses normally provided by the user during the installation of the Windows client software. For example, the path for the Windows client software and the folder for the GroupWise desktop icon are specified in this file. In addition, information can be added to the setup configuration file to add predefined LDAP directory service accounts to the GroupWise Address Book in the Windows client during installation.

When the GroupWise Windows client Setup program (`setup.exe`) is executed, it looks in the same directory for a `setup.cfg` file. If none is found, the installation proceeds, prompting the user for the needed information. If the `setup.cfg` file is found, the Windows client Setup program proceeds, using the information specified in the setup configuration file. Depending on the entries in the setup configuration file, the user might or might not be prompted to provide information during the installation.

The setup configuration file is divided into the following sections. In the setup configuration file, each section head must be enclosed in brackets [] as shown.

- ♦ [“\[GroupWiseSetup\]” on page 1076](#)
- ♦ [“\[ShowSetup\]” on page 1077](#)
- ♦ [“\[AutoUpdate\]” on page 1078](#)
- ♦ [“\[Startup\]” on page 1078](#)
- ♦ [“\[GWCheck\]” on page 1078](#)
- ♦ [“\[IntegrationApps\]” on page 1079](#)
- ♦ [“\[Languages\]” on page 1079](#)

[GroupWiseSetup]

Version=	This entry must match the version being installed; otherwise, the Setup program does not use <code>setup.cfg</code> . The default is 8.0.
Path=	This entry specifies the path where you want the GroupWise Windows client to be installed. The default path for GroupWise 2012 is <code>c:\Program Files\Novell\Groupwise</code> . Earlier versions of GroupWise defaulted to <code>c:\novell\groupwise</code> .
Folder=	This entry creates and installs the GroupWise Windows client shortcuts to the specified folder in the user's <i>Start</i> menu. The default folder is <code>Novell GroupWise</code> .

LaunchMessenger=	This optional entry specifies whether Novell Messenger should be launched when GroupWise starts. The default is No.
LaunchNotify=	This optional entry specifies whether GroupWise Notify should be launched when GroupWise starts. The default is No.
GWMailTo=	This entry specifies whether the GroupWise Windows client should be the default email application in your Web browser. The default is Yes, so that the Internet Browser Mail Integration is installed along with the GroupWise client.
IPAddress=	This optional entry specifies the IP address for the Windows client to always use. Use this setting to set the IP address per post office when using multiple post offices.
IPPort=	This optional entry specifies the IP port for the Windows client to always use.
DefaultIPAddress=	This optional entry specifies the default IP address for the Windows client to use the first time it is started. This should be an IP address that everyone on the system has access to.
DefaultIPPort=	This optional entry specifies the default IP port for the Windows client to use the first time it is started.
StopService=	Use this entry when you are running integrated third-party software along with the GroupWise Windows client, and that software might be locking some GroupWise Windows client DLLs. If client DLLs are locked, the client software cannot be installed. Specify the service for the client Setup program to stop before it installs the client software. Use the name as it appears in the list provided by <i>Control Panel > Administrative Tools > Services</i> . You can stop only one service before installing the client software.

[ShowSetup]

ShowDialogs=	Specify No to hide dialog boxes during the installation. Specify Yes to show the dialog boxes. The default is Yes. If an entry is missing from the <code>setup.cfg</code> file and <code>ShowDialogs=Yes</code> , the Setup program selects the default setting. If <code>ShowDialogs=No</code> , the Setup program prompts the user for a selection. NOTE: This option does not suppress the language selection dialog box that appears when you install the GroupWise Windows client from the multilanguage software image. For more information, see the GroupWise 2012 Readme (http://www.novell.com/documentation/groupwise2012/gw2012_readme_full/data/gw2012_readme_full.html) .
ShowProgress=	Specify Yes to show the progress indicator during the installation. Specify No to hide the progress indicator during installation. The default is Yes.
ShowFinish=	Specify Yes to display the Finish dialog box after the installation. Specify No to hide this dialog box. The default is Yes.

[AutoUpdate]

When you enable AutoUpdate, you can configure the AutoUpdate process to prompt the user to update or to install the software automatically, thus forcing the user to update.

Enabled=	Specify <i>Yes</i> if you want users to be prompted to update their GroupWise Windows client software as soon as a newer version is available. Specify <i>No</i> if you want to disable the AutoUpdate feature. The <i>ForceUpdate=</i> entry is then ignored. This can be useful if you intend to distribute the client software by using a different method such as ZENworks Configuration Management , or if you want to disable AutoUpdates at the post office level during a migration to a newer version of GroupWise. The default is <i>Yes</i> .
SetupIPEnabled=	Specify <i>Yes</i> if you want to use AutoUpdate over an IP connection to a Web server instead of a mapped drive to a software distribution directory. The default is <i>No</i> .
ForceUpdate=	<p>When this entry is set to <i>Yes</i>, GroupWise automatically updates the users' Windows client software. The default is <i>No</i>.</p> <p>Users can still click <i>Cancel</i> to cancel the update; however, they cannot run the Windows client software to access their mailboxes until they update the software.</p>
GraceLoginCount=	Specify the number of grace logins allowed before you require the users to update their Windows client software. If <i>ForceUpdate=No</i> , this entry is ignored.
PromptUntilUpdated=	When <i>PromptUntilUpdated=Yes</i> , the user is prompted to update the Windows client software each time the client starts. The user can choose not to install the new software when prompted and still run the currently installed version of the client. The AutoUpdate reminder appears the next time the user starts the client. The default is <i>No</i> .

[Startup]

Notify=	If you specify <i>Yes</i> , the Setup program places <i>Notify</i> in the Windows Startup folder to be started automatically when the computer starts. The default is <i>No</i> .
---------	---

[GWCheck]

This section installs and enables GroupWise Check (GWCheck). GWCheck is a tool that performs maintenance and repair tasks on users' mailboxes to keep GroupWise operating efficiently. It is essentially a standalone version of the Mailbox/Library Maintenance feature available in GroupWise Administration in ConsoleOne. GWCheck checks and repairs GroupWise user, message, library, and

resource databases without having ConsoleOne and the GroupWise snap-in loaded. In addition to checking post office, user, and library databases, it also checks Caching, Remote, and archive databases.

InstallGWCheck=	Specify <i>Yes</i> to install GWCheck files to the workstation. Specify <i>No</i> to not install GWCheck. The default is <i>Yes</i> .
GWCheckEnabled=	Specify <i>Yes</i> to install the files to the same directory as the GroupWise Windows client, which results in the <i>Repair Mailbox</i> option being enabled under the <i>Tools</i> menu in the client. Specify <i>No</i> to install the files in a GWCheck subdirectory below the <code>client</code> directory, which disables the <i>Repair Mailbox</i> option until the files are manually copied into the GroupWise directory. The default is <i>No</i> .

[IntegrationApps]

GroupWise installs integration for the following applications, if found, unless the entry is set to *No*.

- ◆ Microsoft Excel
- ◆ Microsoft Word
- ◆ Microsoft PowerPoint
- ◆ Corel Presentations
- ◆ Corel Quattro Pro
- ◆ Corel WordPerfect
- ◆ OpenOffice Calc
- ◆ OpenOffice Draw
- ◆ OpenOffice Writer
- ◆ OpenOffice Impress

[Languages]

The default language is set to *English*, and all other languages are set to *No*, meaning they are not installed. See the `setup.cfg` file for a listing of the different languages.

Customizing the Setup Configuration File

- 1 On the server from which you want to distribute the client software, browse to the following directory:
`software_distribution_directory/client`
- 2 Copy the `setup.cfg` file to the `win32` subdirectory, so that it is in the same directory with the `setup.exe` file that it provides the configuration settings for.
- 3 (Conditional) If you are installing from the multilanguage version of GroupWise and you do not want users to be prompted for the languages to install, copy the `setup.ini` file down to the `win32` subdirectory.
- 4 Change to the `win32` subdirectory.
- 5 Use an ASCII text editor to edit the copied `setup.cfg` file and add the settings that you want to use when AutoUpdate installs the client software on users' workstations:
 - 5a Under the `[AutoUpdate]` heading, specify:
`Enabled=Yes`

- 5b** If you want the Windows client software to be automatically updated, so that users are required to update their client software, specify:

`ForceUpdate=Yes`

or

If you want users to be prompted for whether they want to update their Windows client software, specify:

`ForceUpdate=No`

- 5c** (Conditional) If you are forcing users to update, set the number of grace logins you want to allow before forcing an AutoUpdate, for example:

`GraceLoginCount=3`

- 5d** (Conditional) If you are using SetupIP to distribute the client software from a Web server, as described in [“Preparing for Windows Client Installation from a Web Server” on page 1071](#), specify:

`SetupIPEnabled=Yes`

- 5e** (Conditional) If you want to reduce or eliminate interaction between the client Setup program and users, specify one or more of the following options:

`ShowDialogs=No`
`ShowProgress=No`
`ShowFinish=No`

- 6** Change other setup configuration entries as described in [“Understanding the Setup Configuration File” on page 1076](#).

- 7** Save the customized `setup.cfg` file.

- 8** (Conditional) If you are installing from the multilanguage version and you do not want users to be prompted for the languages to install:

- 8a** Open the `setup.ini` file in a text editor.

- 8b** In the `[Startup]` section, specify:

`EnableLangDlg=N`

- 8c** Save the customized `setup.ini` file.

- 9** (Conditional) If you are using SetupIP to distribute the client software from a Web server:

- 9a** Copy the customized `setup.cfg` file to the client software directory that you created in [Step 1](#) in [“Preparing for Windows Client Installation from a Web Server” on page 1071](#).

- 9b** (Conditional) If you customized the `setup.ini` file in [Step 8](#), copy it to the client software directory on the Web server.

- 9c** Test the availability of the files in the `win32` directory on the Web server by displaying the following URL and verifying the contents of the `win32` directory:

`http://web_server_address/gwclient`

Index of /gwclient

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 setupip.en	12-Apr-2012 19:49	4.7M	
 setupip.fil	12-Apr-2012 19:49	87M	
 win32/	12-Apr-2012 19:50	-	

When the `setupip.fil` file and `setupip.en` file are extracted on users' workstations prior to the client software installation, the files in the `win32` directory on the Web server replace the standard files.

- 10 (Optional) Continue with [Adding LDAP Directory Service Accounts to the Setup Configuration File](#).

or

Skip to [Section 77.1.3, "Enabling AutoUpdate in ConsoleOne,"](#) on page 1082.

Adding LDAP Directory Service Accounts to the Setup Configuration File

LDAP directory service accounts provide users with the ability to search directory services such as Bigfoot for names and email addresses of people. Each search can check potentially millions of names. After locating a name through a directory service search, users can add those names and email addresses to their personal address books.

You can add predefined LDAP directory service accounts to the Address Book by adding information to `setup.cfg`. This information can be added even after the initial installation. After the accounts are added, this information does not need to be removed from `setup.cfg`. During subsequent installations, GroupWise adds any new accounts listed but does not update or duplicate existing LDAP accounts.

The user can also choose to add LDAP directory service accounts after the GroupWise Windows client is installed, as described in "Using the LDAP Address Book" in "Contacts and Address Books" in the *GroupWise 2012 Windows Client User Guide*.

To add an LDAP address book during installation, add the following lines to the `setup.cfg` file, providing information that is specific to the LDAP account:

```
[LDAP Account 1]
Description=Ldap Server1
Server=ldap.server1.com
Port=389
SearchRoot=c=us
Login=TRUE
```

You can add multiple accounts:

```
[LDAP Account 2]
Description=Ldap Server2
Server=ldap.server2.com
Port=389
SearchRoot=0=widget, c=us
Login=FALSE
```

Parameter	Description
-----------	-------------

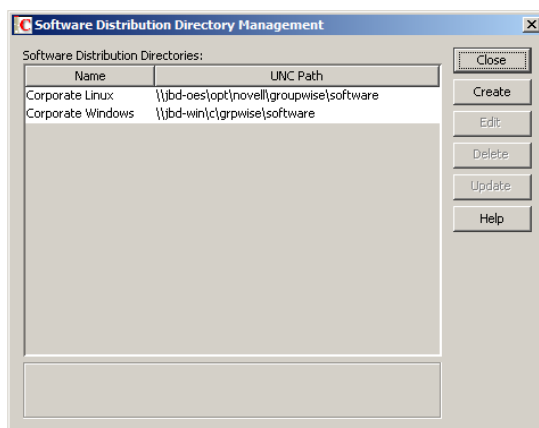
Description=	The name that displays in the list of LDAP directory services in the Address Book.
--------------	--

Parameter	Description
Server=	The LDAP server name or IP address.
Port=	The LDAP directory service's port number. The number is usually 389.
SearchRoot=	The base or root of the LDAP directory service where the user searches for names. For example, the base could be a country, organization, or other type of grouping. This is not required for all LDAP directory services. If a search root is required, the LDAP directory service provides the information.
Login=	TRUE means users are prompted for a user name and password when they use that LDAP directory service.

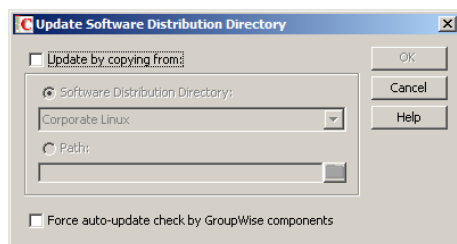
Continue with [Enabling AutoUpdate in ConsoleOne](#).

77.1.3 Enabling AutoUpdate in ConsoleOne

- 1 Log in to ConsoleOne as an Admin equivalent.
- 2 Connect to a domain.
- 3 Click *Tools > GroupWise System Operations > Software Directory Management*.



- 4 Select the software distribution directory for the post offices where you want to update the Windows client software, then click *Update*.



- 5 (Conditional) If the Windows client software is being installed from a mapped drive, select *Update by Copying From*, then select *Software Distribution Directory* or browse to and select another location.

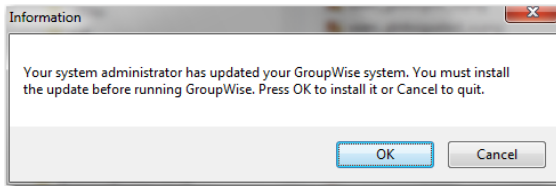
If the Windows client software is being installed from a Web server, the updated software has already been made available, as described in [“Preparing for Windows Client Installation from a Web Server”](#) on page 1071.

- 6 Select *Force Auto-Update Check by GroupWise Components*, then click *OK*.
- 7 Continue with [Section 77.1.4, “Understanding the User’s AutoUpdate Experience,”](#) on page 1083.

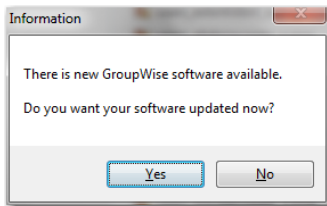
77.1.4 Understanding the User’s AutoUpdate Experience

The next time each client user starts the Windows client, the client detects that the software version in the software distribution directory has been updated. It launches the Windows client Setup program (`setup.exe`), which runs according to the settings you have provided in the `setup.cfg` file.

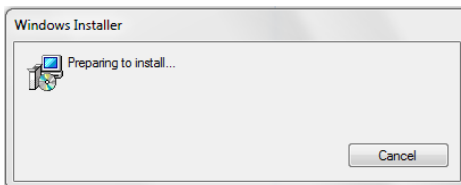
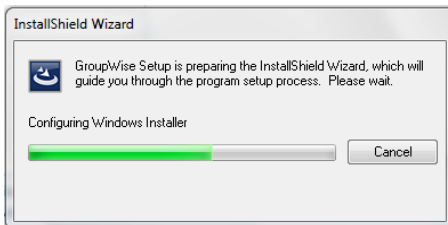
If you are forcing the user to update (`ForceUpdate=Yes` in the `setup.cfg` file), the following message appears:



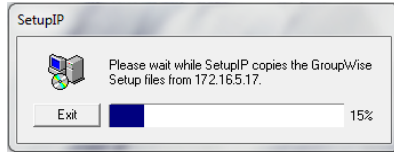
If you are not forcing the user to update (`ForceUpdate=No` in the `setup.cfg` file), the following message appears:



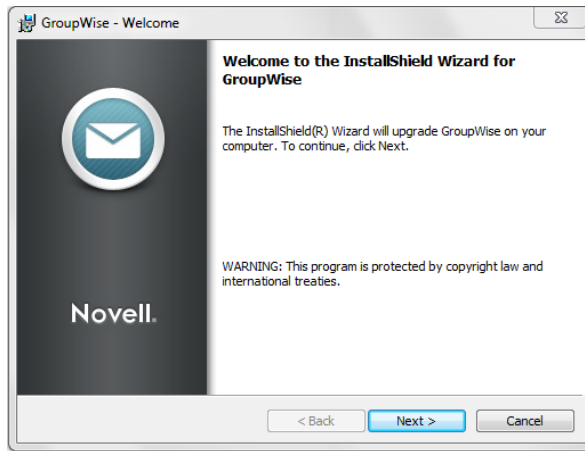
If a mapped drive to the software distribution directory is found, the Windows client software is installed from the mapped drive by the client Setup program (`setup.exe`).



If a mapped drive to the software distribution directory is not found and you have enabled SetupIP (`SetupIPEnabled=Yes` in the `setup.cfg` file), the user sees the software being downloaded from the Web server:



The installation then proceeds based on your choices in the `[ShowSetup]` section of the `setup.cfg` file.



If you turned off all dialog boxes, users do not see the Setup program running.

77.1.5 Using the AutoUpdate Error Log Files

If no connection to a software distribution directory can be made, the `setupip.err` file is created in `c:\windows` on the user's workstation. This file explains why none of the connections could be made.

If an error occurs during the software update and `ShowDialogs` is set to `No` in the `setup.cfg` file, the error message is logged in the `gwsetup.err` file in the user's `c:\windows` directory.

If you add `ErrorMessage=error_text` as the last entry under the `[GroupWiseSetup]` section in the `setup.cfg` file, the specified error text is displayed. Otherwise, a generic error message is displayed, notifying the user to contact the system administrator.

77.1.6 Disabling Your AutoUpdate Customizations

To stop the Windows client Setup program (`setup.exe`) from using the setup configuration file (`setup.cfg`), delete `setup.cfg` from the `client/win32` directory where `setup.exe` resides. Without a `setup.cfg` file, the Setup program offers the user all client installation options to choose from.

77.2 Using ZENworks Configuration Management to Distribute the GroupWise Windows Client

You can use ZENworks Configuration Management to automatically distribute the GroupWise Windows client software to users' workstations. For instructions, see "[Novell ZENworks](#)" in the *GroupWise 2012 Interoperability Guide*.

78 Supporting the GroupWise Client in Multiple Languages

The GroupWise client software is available in a broad range of languages to meet the needs of users in many countries. If your GroupWise system services users who speak more than one language, the following tasks help you meet your multilingual users' needs:

- ♦ [Section 78.1, "Providing the GroupWise Client Software in Multiple Languages," on page 1087](#)
- ♦ [Section 78.2, "Providing Post Office Support for Multiple Languages," on page 1087](#)

78.1 Providing the GroupWise Client Software in Multiple Languages

- 1 Ensure that you have the multilanguage version of GroupWise.

The name of the downloaded GroupWise software image includes `multi` when it is the multilanguage version

- 2 Install the client software in the languages you need in one or more software distribution directories, following the instructions in [Section 4.9, "Software Directory Management," on page 84](#).
- 3 Distribute the client software to users, as described in [Chapter 77, "Distributing the GroupWise Windows Client," on page 1069](#).

By installing the GroupWise client software in their language of choice, users can begin using GroupWise in that language immediately. However, there are a few language-related details of GroupWise functionality that are not taken care of by the client software running on users' workstations. For a fuller multilanguage implementation, continue with [Section 78.2, "Providing Post Office Support for Multiple Languages," on page 1087](#).

78.2 Providing Post Office Support for Multiple Languages

A few aspects of GroupWise functionality are affected by the language in use by the POA running for the post office to which users belong. The POA returns certain text in the language in which it is running, not the language in use on users' workstations.

- ♦ The status information (Delivered, Opened, and so on) displayed in the Properties page of items
- ♦ The text of return notification mail receipts (if the user has enabled this type of notification)
- ♦ The sort order in the Address Book

In some circumstances, these issues can be resolved by grouping users who speak the same language into the same post office and then installing the POA in the same language that the users are using. For more information, see [Section 11, "Creating a New Post Office," on page 173](#).

At present, the POA is available in fewer languages than the GroupWise client, so this solution helps only those client users who are somewhat familiar with the language in use by the POA. For more information, see [Chapter 7, “Multilingual GroupWise Systems,”](#) on page 123.

79 Tools for Analyzing and Correcting GroupWise Client Problems

The following tools can assist you in analyzing and correcting GroupWise client problems.

- ♦ [Section 79.1, “GroupWise Exception Handler for the Windows Client,” on page 1089](#)
- ♦ [Section 79.2, “GroupWise Check,” on page 1089](#)

79.1 GroupWise Exception Handler for the Windows Client

If the GroupWise Windows client causes an exception (or “crashes”), GroupWise generates a GroupWise Exception Report. This report contains information that is useful in analyzing the problem that the client is having so that it can be solved.

The report is saved in `\temp\grpwise.rpt`. The `\temp` directory used is the one specified by the `TMP` environment variable, or if not defined by `TMP`, the one specified by the `TEMP` environment variable. If neither environment variable is defined, GroupWise uses the current the `windows` directory.

Each time an exception or crash occurs, a new report is appended to `grpwise.rpt`. If the file reaches 100 KB, the oldest reports (at the beginning of the file) are deleted.

The GroupWise Exception Report contains information such as the date and time the report was generated, the exception code, fault address, date of `grpwise.exe`, computer and user name where the exception occurred, hardware and operating system information, process modules, raw stack dumps, and call stacks.

79.2 GroupWise Check

GroupWise Check (GWCheck) is a tool that performs maintenance and repair tasks to keep GroupWise operating efficiently. It is essentially a standalone version of the Mailbox/Library Maintenance feature available in ConsoleOne. GroupWise Check checks and repairs GroupWise

user, message, library, and resource databases without having ConsoleOne and the GroupWise snap-in loaded. In addition to checking post office, user, and library databases, it also checks remote and archive databases.

- ♦ [Section 79.2.1, “Enabling GroupWise Check in the Windows Client,”](#) on page 1090

79.2.1 Enabling GroupWise Check in the Windows Client

GroupWise Check can be installed with the GroupWise Windows client (unless you have specified in `setup.cfg` that it not be installed), and is available by clicking *Tools > Repair Mailbox* in the client in Caching and Remote modes after you complete the following:

- 1 Locate the directory named `gwcheck`. This is a subdirectory of the directory where the client is installed (usually `c:\Program Files\Novell\GroupWise`).
- 2 Locate `grpwise.exe`. It is usually in `c:\Program Files\Novell\GroupWise`.
- 3 Copy all the files in `gwcheck` to the directory where `grpwise.exe` is located.

You can now run GroupWise Check in Caching and Remote mode. The GroupWise Check dialog box is titled GroupWise Mailbox Maintenance. You can also use Ctrl+Shift when accessing a Caching or Remote mailbox to run GroupWise Check before opening the mailbox.

For detailed information about GroupWise Check, click Help or see [Section 34.1, “GroupWise Check,”](#) on page 447.

80 Startup Options for the GroupWise Windows Client

The GroupWise Windows client has optional startup options that you can use when you start the program. Some of these startup options are for your convenience, while others are necessary to run GroupWise on your particular hardware.

Windows Client Startup Options

/@u-?

/@u-user_ID

/bl

/c

/cm

/iabs

/ipa-IP_address_or_hostname

/ipp-port_number

/l-xx

/la-network_ID

/nu

/ph-path_name

/pc-path_to_caching_mailbox

/pr-path_to_remote_mailbox

80.1 /@u-?

Displays a login dialog box whenever you open the GroupWise client, allowing you to supply any necessary login information.

Syntax: */@u-?*

Example: `grpwise.exe /@u-?`

80.2 /@u-user_ID

Lets you use your GroupWise user ID to use the GroupWise client as yourself on another user's computer. The other user remains logged on to the network.

Syntax: /@u-user_ID

Example: grpwise.exe /@u-ltanaka

80.3 /bl

Prevents the GroupWise client logo screen from being displayed when you start the GroupWise client.

Syntax: /bl

Example: grpwise.exe /bl

80.4 /c

Checks for unopened items. If there are unopened items, the GroupWise client opens as usual. Otherwise, the GroupWise client does not start.

Syntax: /c

Example: grpwise.exe /c

80.5 /cm

Checks for unopened items. If there are unopened items, the GroupWise client opens minimized and a beep sounds. Otherwise, the GroupWise client does not start.

Syntax: /cm

Example: grpwise.exe /cm

80.6 /iabs

Initializes the Address Book when the GroupWise client starts.

Syntax: /iabs

Example: grpwise.exe /iabs

80.7 /ipa-IP_address_or_hostname

Lets you specify the IP address or the hostname when you are running in client/server mode.

Syntax: /ipa-IP_address

Example: grpwise.exe /ipa=127.65.45.1

80.8 ***/ipp-port_number***

Lets you specify the IP port number when you are running in client/server mode.

Syntax: */ipp-port_number*

Example: `grpwise.exe /ipp-1677`

80.9 ***/l-xx***

Applies only if you have two or more language versions or language modules. This option instructs GroupWise to override the default environment language (under Environment in Options) with the language specified by the language code *xx*. This table lists the language codes used by all Novell products. GroupWise might not yet be available in some of the listed languages. For current information, contact your local reseller.

For a list of language codes, see [Section 7.1, "GroupWise User Languages,"](#) on page 123.

Syntax: */l-xx*

Example: `grpwise.exe /l-ES`

80.10 ***/la-network_ID***

Lets you use your network ID to use the GroupWise client as yourself on another user's computer. The other user remains logged on to the network.

Syntax: */la-network_ID*

Example: `grpwise.exe /la-jgrey`

80.11 ***/nu***

Turns off AutoRefresh. If this option is selected, click *View > Refresh* whenever you want to update the display to see the items currently in your mailbox.

Syntax: */nu*

Example: `grpwise.exe /nu`

80.12 ***/ph-path_name***

Lets you specify the path to the post office.

Syntax: */ph-path_name*

Example: `grpwise.exe /ph-j:\mail\denver1`

80.13 ***/pc-path_to_caching_mailbox***

Opens GroupWise in Caching mode. GroupWise must be restarted when you change from Online to Caching.

Syntax: `/pc-path_to_caching_mailbox`

Example: `grpwise.exe /pc-c:\novell\groupwise\cache`

80.14 ***/pr-path_to_remote_mailbox***

Opens the GroupWise client in Remote mode. This startup option can be used in the *Target* text box only.

Syntax: `/pr-path_to_remote_mailbox`

Example: `grpwise.exe /pr-c:\novell\groupwise\remote`

XVI Security Administration

- ♦ Chapter 81, “Native GroupWise Security,” on page 1097
- ♦ Chapter 82, “GroupWise Passwords,” on page 1099
- ♦ Chapter 83, “Encryption and Certificates,” on page 1105
- ♦ Chapter 84, “LDAP Directories,” on page 1119
- ♦ Chapter 85, “Message Security,” on page 1123
- ♦ Chapter 86, “Address Book Security,” on page 1125
- ♦ Chapter 87, “GroupWise Administrator Rights,” on page 1127
- ♦ Chapter 88, “GroupWise Agent Rights,” on page 1139
- ♦ Chapter 89, “GroupWise User Rights,” on page 1141
- ♦ Chapter 90, “Spam Protection,” on page 1145
- ♦ Chapter 91, “Virus Protection,” on page 1147

See also Part XVIII, “Security Policies,” on page 1149.

For additional assistance in managing your GroupWise system, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

81 Native GroupWise Security

By default, GroupWise native encryption is employed throughout your GroupWise system. This means that all files related to GroupWise items are automatically encrypted when they are stored on disk. In addition, all connections between the GroupWise client and GroupWise agents use a proprietary, encrypted protocol.

By default, the GroupWise client runs in Online mode, so that all files related to mailboxes are stored on the GroupWise server where the POA for the post office runs. As an administrator, you can choose whether to allow users to set up their mailboxes to use Caching mode or Remote mode, where mailboxes are located on users' workstations.

If you decide to allow users to use Caching mode or Remote mode, the mailbox files on users' workstations are all protected by GroupWise native encryption.

The following sections help you configure your GroupWise system for even tighter security:

- ♦ [Section 82.1, "Mailbox Passwords," on page 1099](#)
- ♦ [Section 82.2, "Agent Passwords," on page 1103](#)
- ♦ [Section 83.1, "Personal Digital Certificates, Digital Signatures, and S/MIME Encryption," on page 1105](#)
- ♦ [Section 83.2, "Server Certificates and SSL Encryption," on page 1107](#)
- ♦ [Section 83.3, "Trusted Root Certificates and LDAP Authentication," on page 1115](#)

See also [Part XVIII, "Security Policies," on page 1149](#).

82 GroupWise Passwords

Access to GroupWise mailboxes is protected by post office security settings or GroupWise passwords. Agent passwords grant access to remote servers and to Novell eDirectory, and protect access to GroupWise agent status information.

- ♦ [Section 82.1, “Mailbox Passwords,” on page 1099](#)
- ♦ [Section 82.2, “Agent Passwords,” on page 1103](#)

See also [Part XVIII, “Security Policies,” on page 1149](#).

82.1 Mailbox Passwords

When you are setting up a new GroupWise system, you need to determine what kind of password protection you want to have on users’ GroupWise mailboxes before users start running GroupWise. In ConsoleOne, you can choose where password information is obtained when users log in to GroupWise and you can set defaults under Client Options to enforce your choices. You and GroupWise client users should keep in mind that GroupWise passwords are case sensitive.

- ♦ [Section 82.1.1, “Using Post Office Security Instead of GroupWise Passwords,” on page 1099](#)
- ♦ [Section 82.1.2, “Requiring GroupWise Passwords,” on page 1100](#)
- ♦ [Section 82.1.3, “Managing GroupWise Passwords,” on page 1100](#)
- ♦ [Section 82.1.4, “Using LDAP Passwords Instead of GroupWise Passwords,” on page 1102](#)
- ♦ [Section 82.1.5, “Bypassing Mailbox Passwords to Respond to Corporate Mandates,” on page 1103](#)

82.1.1 Using Post Office Security Instead of GroupWise Passwords

When you create a new post office, you must select a security level for it.

If you select *Low Security* for the post office, users are not required to set passwords on their GroupWise mailboxes. However, passwordless mailboxes are completely unprotected from other users who know how to use the `@u-user_ID` startup switch.

If you select *High Security* for the post office, users are still not required to set passwords on their GroupWise mailboxes, but they are required to be successfully logged in to a network before they can access their own passwordless mailboxes. Users cannot access other users’ passwordless mailboxes.

After you select *High Security*, you can further enhance post office security by requiring specific types of authentication before users can access their passwordless GroupWise mailboxes. You can require eDirectory authentication so that users must be logged in to eDirectory before they can access their passwordless GroupWise mailboxes.

In spite of these passwordless solutions to GroupWise mailbox security, users are always free to set their own GroupWise passwords on their mailboxes. When they do, the post office security settings no longer apply (except for LDAP authentication as discussed below) and users are regularly faced with both logins unless some additional password options are selected for them, as described in the following sections.

82.1.2 Requiring GroupWise Passwords

Users are required to set passwords on their GroupWise mailboxes if they want to access their GroupWise mailboxes in any of the following ways:

- ♦ Using Caching mode or Remote mode in the GroupWise Windows client
- ♦ Using their Web browsers and GroupWise WebAccess
- ♦ Using an IMAP email client
- ♦ Accessing a GroupWise mailbox as an external entity rather than as an eDirectory user

82.1.3 Managing GroupWise Passwords

When GroupWise passwords are used in addition to network passwords, there are a variety of things you can do to make GroupWise password management easier for you and to make the additional GroupWise password essentially transparent for your GroupWise users.

- ♦ [“Establishing a Default GroupWise Password for New Accounts” on page 1100](#)
- ♦ [“Accepting eDirectory Authentication Instead of GroupWise Passwords” on page 1101](#)
- ♦ [“Using Novell SecureLogin to Handle GroupWise Passwords” on page 1101](#)
- ♦ [“Allowing Windows to Cache GroupWise Passwords” on page 1101](#)
- ♦ [“Using Intruder Detection” on page 1101](#)
- ♦ [“Resetting GroupWise Passwords” on page 1102](#)
- ♦ [“Synchronizing GroupWise Passwords and LDAP Passwords” on page 1102](#)
- ♦ [“Helping Users Who Forget Their Passwords” on page 1102](#)

NOTE: A GroupWise password can contain as many as 64 characters and can contain any typeable characters.

Establishing a Default GroupWise Password for New Accounts

If you want to require users to have GroupWise passwords on their mailboxes, you can establish the initial passwords when you create the GroupWise accounts. In ConsoleOne, you can establish a default mailbox password to use automatically on all new GroupWise accounts, as described in [Section 13.1, “Establishing a Default Password for All New GroupWise Accounts,” on page 219](#). Or you can set the password on each new GroupWise account as you create it.

Keep in mind that some situations require users to have passwords on their GroupWise mailboxes, as listed in [Section 82.1.2, “Requiring GroupWise Passwords,” on page 1100](#).

Accepting eDirectory Authentication Instead of GroupWise Passwords

When you create users in eDirectory, you typically assign them network passwords, which users must provide when they log in to the network. If you want to make it easy for client users to access their GroupWise mailboxes, you can select *Allow eDirectory Authentication Instead of Password* (ConsoleOne > Tools > GroupWise Utilities > Client Options > Security > Password). This allows GroupWise users to select *No Password Required with eDirectory* (Windows client > Tools > Options > Security > Password).

NOTE: This option is not available in GroupWise WebAccess.

As long as users who select this option are logged into eDirectory as part of their network login, they are not prompted by GroupWise for a password when they access their GroupWise mailboxes. If they are not logged in to eDirectory, they must provide their GroupWise passwords in order to access their GroupWise mailboxes.

Using Novell SecureLogin to Handle GroupWise Passwords

If users have Novell SecureLogin installed on their workstations, you can select *Enable single sign-on* (ConsoleOne > Tools > GroupWise Utilities > Client Options > Security > Password). This allows GroupWise users to select *Use Single Sign-On* (Windows client > Tools > Options > Security > Password). Users need to provide their GroupWise mailbox password only once and thereafter SecureLogin provides it for them as long as they are logged in to eDirectory.

NOTE: This option is not available in GroupWise WebAccess.

Allowing Windows to Cache GroupWise Passwords

If you want to allow password information to be stored on Windows workstations, you can select *Allow password caching* (ConsoleOne > Tools > GroupWise Utilities > Client Options > Security > Password). This allows GroupWise users to select *Remember My Password* (Windows client > Tools > Options > Security > Password). Users need to provide their GroupWise mailbox passwords only once and thereafter Windows provides them automatically.

This option applies only to older GroupWise clients running on older Windows versions, such as Windows 2000 and earlier, which are not supported for the GroupWise 2012 Windows client.

NOTE: This option is not available in GroupWise WebAccess.

Using Intruder Detection

Intruder detection identifies system break-in attempts in the form of repeated unsuccessful logins. If someone cannot provide a valid user name and password combination within a reasonable time, then that person probably does not belong in your GroupWise system.

Intruder detection for the GroupWise Windows client is performed by the POA and is configurable. You can set the number of failed login attempts before lockout, the length of the lockout, and so on. If a user is locked out, you can re-enable his or her account in ConsoleOne. See [Section 36.3.5, "Enabling Intruder Detection,"](#) on page 516.

Intruder detection for the GroupWise WebAccess is built in and is not configurable. After five failed login attempts, the user is locked out for 10 minutes. If a user is locked out, the user must wait for the lockout period to end.

Resetting GroupWise Passwords

In ConsoleOne, you can remove a user's password from his or her mailbox if the password has been forgotten and needs to be reset (User object > *Tools* > *GroupWise Utilities* > *Client Options* > *Security* > *Password*). If necessary, you can remove the passwords from all mailboxes in a post office (Post Office object > *Tools* > *GroupWise Utilities* > *Mailbox/Library Maintenance* > *Reset Client Options*) This resets all or users' client options settings, not just the passwords.

It is easy for GroupWise users to reset their own passwords (Windows client > *Tools* > *Options* > *Security* > *Password*). However, if this method is used when users are in Caching or Remote mode, this changes the password on the local Caching or Remote mailboxes, but does not change the password on the Online mailboxes. To change the Online mailbox password while in Caching or Remote mode, users must use a method they might not be familiar with (Windows client > *Accounts* > *Account Options* > *Novell GroupWise Account* > *Properties* > *Advanced* > *Online Mailbox Password*).

It is also easy for GroupWise WebAccess users to reset their own passwords (WebAccess > *Options* > *Password*). However, you might not want users to be able to reset their GroupWise passwords from Web browsers. See [Section 62.2.3, "Preventing Users from Changing Their GroupWise Passwords in WebAccess," on page 908](#). Windows client users cannot be prevented from changing their GroupWise passwords.

Synchronizing GroupWise Passwords and LDAP Passwords

There is no automatic procedure for synchronizing GroupWise passwords and eDirectory passwords. However, if you use LDAP authentication, synchronization becomes a moot point because GroupWise users are authenticated through an LDAP directory (such as eDirectory) rather than by using GroupWise passwords. See [Section 82.1.4, "Using LDAP Passwords Instead of GroupWise Passwords," on page 1102](#).

Helping Users Who Forget Their Passwords

The WebAccess Login page includes a *Can't log in* link, which provides the following information to WebAccess users by default:

If you have forgotten your GroupWise password, contact your local GroupWise administrator.

For your convenience and for the convenience of your WebAccess users, you can customize the information that is provided by the *Can't log in* link. For set instructions, see ["Helping Users Who Forget Their GroupWise Passwords"](#) in ["WebAccess"](#) in the *GroupWise 2012 Administration Guide*.

82.1.4 Using LDAP Passwords Instead of GroupWise Passwords

Instead of using GroupWise passwords, users' password information can be validated using an LDAP directory. In order for users to use their LDAP passwords to access their GroupWise mailboxes, you must define one or more LDAP servers in your GroupWise system and configure the POA for each post office to perform LDAP authentication, as described in [Section 36.3.4, "Providing LDAP Authentication for GroupWise Users," on page 510](#).

When LDAP authentication is enabled, you can control whether users can use the GroupWise client to change their LDAP passwords (ConsoleOne > Post Office object > *Properties* > *GroupWise* > *Security*). If you allow them to, GroupWise users can change their passwords through the Security Options dialog box (Windows client > *Tools* > *Options* > *Security*) or on the Passwords page (GroupWise WebAccess > *Options* > *Password*). If you do not allow them to change their LDAP passwords in the GroupWise client, users must use a different application in order to change their LDAP passwords.

You and users can use some of the same methods to bypass LDAP passwords as you can use for bypassing GroupWise passwords. See [“Accepting eDirectory Authentication Instead of GroupWise Passwords”](#) on page 1101 and [“Allowing Windows to Cache GroupWise Passwords”](#) on page 1101.

For more information about LDAP passwords, see [Section 84.3, “Authenticating to GroupWise with Passwords Stored in an LDAP Directory,”](#) on page 1120.

82.1.5 Bypassing Mailbox Passwords to Respond to Corporate Mandates

Sometimes it is necessary to access user mailboxes to meet corporate mandates such as virus scanning, content filtering, or email auditing that might be required during litigation. These types of mailbox access are obtain using trusted applications, which are third-party programs that can log into Post Office Agents (POAs) in order to access GroupWise mailboxes. For more information about a using trusted application to bypass mailbox passwords, see [Section 4.12, “Trusted Applications,”](#) on page 90

82.2 Agent Passwords

Agent passwords facilitate access to remote servers where domains, post office, and document storage areas are located and access to eDirectory for synchronization of user information between GroupWise and eDirectory. They also protect GroupWise Monitor and the agent Web consoles from unauthorized access.

- ♦ [Section 82.2.1, “Facilitating Access to Remote Servers,”](#) on page 1103
- ♦ [Section 82.2.2, “Facilitating Access to eDirectory,”](#) on page 1103
- ♦ [Section 82.2.3, “Protecting the Agent Web Consoles,”](#) on page 1104
- ♦ [Section 82.2.4, “Protecting the GroupWise Monitor Web Console,”](#) on page 1104

82.2.1 Facilitating Access to Remote Servers

The Windows POA needs user name and password information in order to access a document storage area on a server other than the one where the post office database and directory structure are located. There are two ways to provide this information:

- ♦ Fill in the *Remote User Name* and *Remote Password* fields on the Post Office Settings page of the Post Office object in ConsoleOne
- ♦ Add the `/user` and `/password` startup switches to the POA startup file to provide a user name and password

Providing passwords in clear text in a startup file might seem like a security risk. However, the servers where the agents run should be kept physically secure. If an unauthorized person did gain physical access, they would not be doing so for the purpose of obtaining these particular passwords. The passwords are encrypted as they pass over the wire between servers, so the security risk is minimal.

82.2.2 Facilitating Access to eDirectory

If you have enabled eDirectory user synchronization, the MTA must be able to log in to eDirectory in order to obtain the updated user information. An eDirectory-enabled MTA should be installed on a server where a local eDirectory replica is located. For more information, see [Section 42.4.1, “Using eDirectory User Synchronization,”](#) on page 652.

82.2.3 Protecting the Agent Web Consoles

When you install the POA, the MTA, and the GWIA, they are automatically configured with an agent Web console and no password protection is provided. When you install the GWIA, you can choose whether to enable the agent Web console during installation. If you do, you can provide password protection at that time. For WebAccess, you must manually enable its Web console, so you can provide password protection when you enable it.

If you do not want agent Web console status information available to anyone who knows the agent network address and port number, you should set passwords on your agent Web console, as described in the following sections:

- ♦ [Section 37.2, “Using the POA Web Console,” on page 539](#)
- ♦ [Section 43.2, “Using the MTA Web Console,” on page 669](#)
- ♦ [Section 49.2, “Using the DVA Web Console,” on page 725](#)
- ♦ [Section 56.2, “Using the GWIA Web Console,” on page 827](#)
- ♦ [Section 63.1, “Using the WebAccess Application Web Console,” on page 917](#)

If you plan to access the GroupWise Monitor Web consoles, it is most convenient if you use the same password on all agent Web consoles. That way, you can provide the agent Web console password once in GroupWise Monitor, rather than having to provide various passwords as you view the Web consoles for various agents. For information about providing the agent Web console password in GroupWise Monitor, see [Section 69.4, “Configuring Polling of Monitored Agents,” on page 956](#).

82.2.4 Protecting the GroupWise Monitor Web Console

Along with the agent Web consoles, you can also provide password protection for the Monitor Web console itself, from which all the agent Web consoles can be accessed. For instructions, see [Section 69.8, “Configuring Authentication and Intruder Lockout for the Monitor Web Console,” on page 964](#).

83 Encryption and Certificates

GroupWise native encryption is employed throughout your GroupWise system. For background information, see [Chapter 81, “Native GroupWise Security,” on page 1097](#). Additional security measures should also be utilized to secure your GroupWise data.

- ♦ [Section 83.1, “Personal Digital Certificates, Digital Signatures, and S/MIME Encryption,” on page 1105](#)
- ♦ [Section 83.2, “Server Certificates and SSL Encryption,” on page 1107](#)
- ♦ [Section 83.3, “Trusted Root Certificates and LDAP Authentication,” on page 1115](#)

See also [Part XVIII, “Security Policies,” on page 1149](#).

83.1 Personal Digital Certificates, Digital Signatures, and S/MIME Encryption

If desired, you can implement S/MIME encryption for GroupWise client users by installing various security providers on users' workstations, including:

- ♦ [Entrust 4.0 or later \(http://www.entrust.com\)](http://www.entrust.com)
- ♦ Microsoft Base Cryptographic Provider 1.0 or later (included with Internet Explorer 4.0 or later)
- ♦ [Microsoft Enhanced Cryptographic Provider 1.0 or later \(http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp\)](http://www.microsoft.com/windows/ie/downloads/recommended/128bit/default.asp)
- ♦ [Microsoft Strong Cryptographic Provider \(http://www.siliconprairies.com/spsckb/EncryptAll/strong_cryptographic_provider.htm\)](http://www.siliconprairies.com/spsckb/EncryptAll/strong_cryptographic_provider.htm)
- ♦ [Gemplus GemSAFE Card CSP 1.0 or later \(http://www.gemplus.com\)](http://www.gemplus.com)
- ♦ [Schlumberger Cryptographic Provider \(http://www.slb.com\)](http://www.slb.com)

For additional providers, consult the [Novell Partner Product Guide \(http://www.novell.com/partnerguides\)](http://www.novell.com/partnerguides).

These products enable users to digitally sign and encrypt their messages using S/MIME encryption. When a sender digitally signs a message, the recipient is able to verify that the item was not modified en route and that it originated from the sender specified. When a sender encrypts a message, the sender ensures that the intended recipient is the only one who can read it. Digitally signed and encrypted messages are protected as they travel across the Internet, but native GroupWise encryption is removed as messages leave your GroupWise system.

After users have installed an S/MIME security provider on their workstations, you can configure default functionality for it in ConsoleOne (Domain, Post Office, or User object > *Tools* > *GroupWise Utilities* > *Client Options* > *Send* > *Security* > *Secure Item Options*). You can specify a URL from which you want users to obtain their S/MIME certificates. You can require the use of digital signatures and encryption, rather than letting users decide when to use them. You can even select the encryption algorithm and encryption key size if necessary. For more information, see [Section 76.2.2, “Modifying Send Options,” on page 1050](#).

After you have configured S/MIME functionality in ConsoleOne, GroupWise users must select the security provider (Windows client > *Tools > Options > Security > Send Options*) and then obtain a personal digital certificate. Unless you installed Entrust, users can request certificates (Windows client > *Tools > Options > Certificates > Get Certificate*). If you provided a URL, users are taken to the certificate authority of your choice. Otherwise, certificates for use with GroupWise can be obtained from various certificate providers, including:

- ◆ Novell, Inc. (if you have installed [Novell Certificate Server 2 or later](http://www.novell.com/products/certserver) (<http://www.novell.com/products/certserver>))
- ◆ VeriSign, Inc. (<http://www.verisign.com>)
- ◆ Thawte Certification (<http://www.thawte.com>)
- ◆ GlobalSign (<http://www.globalsign.com>)

NOTE: Some certificate providers charge a fee for certificates and some do not.

After users have selected the appropriate security provider and obtained a personal digital certificate, they can protect their messages with S/MIME encryption by digitally signing them (Windows client > *Actions > Sign Digitally*) and encrypting them (Windows client > *Actions > Encrypt*). Buttons are added to the GroupWise toolbar for convenient use on individual messages, or users can configure GroupWise to always use digital signatures and encryption (Windows client > *Tools > Options > Security > Send Options*). The messages they send with digital signatures and encryption can be read by recipients using any other S/MIME-enabled email product.

GroupWise Windows client users are responsible for managing their personal digital certificates. Users can have multiple personal digital certificates. In the GroupWise client, users can view their own certificates, view the certificates they have received from their contacts, access recipient certificates from LDAP directories (see [Section 84.4, "Accessing S/MIME Certificates in an LDAP Directory," on page 1121](#) for details), change the trust level on certificates, import and export certificates, and so on.

The certificates are stored in the local certificate store on the user's workstation. They are not stored in GroupWise. Therefore, if a user moves to a different workstation, he or she must import the personal digital certificate into the certificate store on the new workstation, even though the same GroupWise account is being accessed.

If your system includes smart card readers on users' workstations, certificates can also be retrieved from this source, so that after composing a message, users can sign them by inserting their smart cards into the card readers. The GroupWise client picks up the digital signature and adds it to the message.

The GroupWise Windows client verifies the user certificate to ensure that it has not been revoked. It also verifies the certificate authority. If a certificate has expired, the GroupWise user receives a warning message.

For complete details about using S/MIME encryption in the GroupWise Windows client, see ["Sending S/MIME Secure Messages"](#) in ["Email"](#) in the [GroupWise 2012 Windows Client User Guide](#).

NOTE: S/MIME encryption is not available in GroupWise WebAccess.

Any messages that are not digitally signed or encrypted are still protected by native GroupWise encryption as long as they are within your GroupWise system.

83.2 Server Certificates and SSL Encryption

You should strengthen native GroupWise encryption with Secure Sockets Layer (SSL) communication between servers where GroupWise agents are installed. You can choose to purchase a server certificate from a commercial certificate authority (CA) or you can generate a self-signed certificate.

The advantage of using a self-signed certificate is that you can proceed to set up SSL immediately, without waiting to the certificate from a certificate authority. However, the first time the GroupWise client encounters the self-signed certificate, it prompts the user to accept the certificate. The advantage of a commercially generated certificate is that the GroupWise client accepts it automatically. You might choose to use a self-signed certificate initially, while you are waiting to obtain a commercially generated certificate.

If you have not already set up SSL on your system, complete the following tasks:

- ♦ [Section 83.2.1, “Purchasing a Commercially Generated Certificate,” on page 1107](#)
- ♦ [Section 83.2.2, “Generating a Self-Signed Certificate,” on page 1111](#)
- ♦ [Section 83.2.3, “Installing the Certificate on the Server,” on page 1114](#)
- ♦ [Section 83.2.4, “Configuring the Agents to Use SSL,” on page 1115](#)

If you have already set up SSL on your system and are using it with other applications in addition to GroupWise, skip to [Section 83.2.4, “Configuring the Agents to Use SSL,” on page 1115](#).

83.2.1 Purchasing a Commercially Generated Certificate

In order to purchase a commercially generated certificate, you must create a certificate signing request (CSR).

- ♦ [“Generating a Certificate Signing Request” on page 1107](#)
- ♦ [“Submitting the Certificate Signing Request to a Certificate Authority” on page 1111](#)

Generating a Certificate Signing Request

The certificate signing request (CSR) includes the hostname of the server where the agents run. Therefore, you must create a CSR for every server where you want the GroupWise agents to use SSL. However, all GroupWise agents running on the same server can all use the same certificate, so you do not need separate CSRs for different agents. The CSR also includes your choice of name and password for the private key file that must be used with each certificate. This information is needed when configuring the agents to use SSL.

- ♦ [“Using the GroupWise Generate CSR Utility \(GWCSRGEN\)” on page 1107](#)
- ♦ [“Linux: Using OpenSSL” on page 1109](#)
- ♦ [“Windows Server 2008: Using IIS Manager” on page 1110](#)
- ♦ [“Windows Server 2003: Using Internet Information Services” on page 1111](#)

Using the GroupWise Generate CSR Utility (GWCSRGEN)

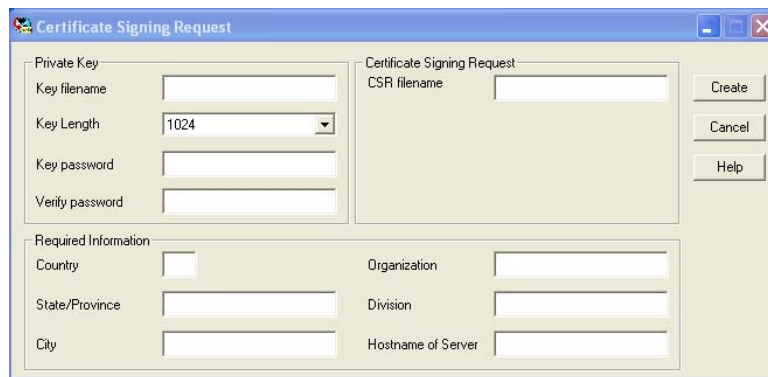
One way to create a CSR is to use the GroupWise Generate CSR utility (GWCSRGEN). This utility takes the information you provide and creates a .csr file from which a public certificate file can be generated.

IMPORTANT: Starting in GroupWise 2012 SP1, GWCSRGEN is no longer a recommended method for creating CSRs. You can still use it for convenience, but for optimum security, use a standard CSR generation method native to your operating system.

1 Start the GroupWise Generate CSR utility.

Linux: The utility (`gwcsrgen`) is installed to the `/opt/novell/groupwise/agents/bin` directory. You must be logged in as `root` to start the utility.

Windows: The utility (`gwcsrgen.exe`) is located in the `\admin\utility\gwcsrgen` directory either in downloaded *GroupWise 2012* software image or in the GroupWise software distribution directory.



2 Fill in the fields in the *Private Key* box. The private key information is used to create both the Private Key file and the certificate signing request file.

Key Filename: Specify a name for the Private Key file (for example, `server1.key`). If you do not want the file stored in the same directory as the GWCSRGEN utility, specify a full path with the file name (for example, `c:\certs\server1.key` or `/opt/novell/groupwise/certs/server1.key`). The directory where you want to create the `.key` file must already exist.

Linux: Use only lowercase characters.

Windows: No limitations

Key Length: The key length can be 1024, 2048, or 4096. The default is 1024.

Key Password: Specify the password for the private key. The password can be up to 256 characters (single-byte environments).

Verify Password: Specify the password again.

3 Fill in the fields in the *Certificate Signing Request* box.

CSR Filename: Specify a name for the certificate signing request file (for example, `server1.csr`). If you don't want the file created in the same directory as the GWCSRGEN utility, specify a full path with the file name (for example, `c:\certs\server1.csr` or `/opt/novell/groupwise/certs/server1.csr`). The directory where you want to create the `.csr` file must already exist.

Linux: Use only lowercase characters.

Windows: No limitations

- 4 Fill in the fields in the *Required Information* box. This information is used to create the certificate signing request file. You must fill in all fields to generate a valid CSR file.
 - Country:** Specify the two-letter abbreviation for your country (for example, US).
 - State/Province:** Specify the name of your state or province (for example, Utah). Use the full name. Do not abbreviate it.
 - City:** Specify the name of your city (for example, Provo).
 - Organization:** Specify the name of your organization (for example, Novell, Inc.).
 - Division:** Specify your organization's division that this certificate is being issued to (for example, Novell Product Development).
 - Hostname of Server:** Specify the DNS hostname of the server where the server certificate will be used (for example, dev.provo.novell.com).
- 5 Click *Create* to generate the CSR file and Private Key file.
 - The CSR and Private Key files are created with the names and in the locations you specified in the *Key Filename* and *CSR Filename* fields.
- 6 Skip to "[Submitting the Certificate Signing Request to a Certificate Authority](#)" on page 1111.

For convenience, if you need to generate multiple certificates, you can record the information for the fields listed in "[Using the GroupWise Generate CSR Utility \(GWCSRGEN\)](#)" on page 1107 in a configuration file so that the information is automatically provided whenever you run the GroupWise Generate CSR utility. The configuration file must have the following format:

```
[Private Key]
Location =
Extension = key

[CSR]
Location =
Extension = csr

[Required Information]
Country =
State =
City =
Organization =
Division =
Hostname =
```

If you do not want to provide a default for a certain field, insert a comment character (#) at the beginning of that line. Name the file `gwcsrgen.cnf`. Save the file in the same directory where the utility is installed:

```
Linux:    /opt/novell/groupwise/agents/bin
Windows:  \grpwise\software\admin\utility\gwcsrgen
```

Linux: Using OpenSSL

For background information, see [HOWTO Certificates \(http://www.openssl.org/docs/HOWTO/certificates.txt\)](http://www.openssl.org/docs/HOWTO/certificates.txt).

- 1 Open a terminal window, become `root`, and change to a convenient directory where you want to create the CSR.
- 2 Enter the following command to create a private key file:

```
openssl genrsa -out -key key_file_name.key 2048
```

Replace `key_file_name.key` with a convenient name for the private key file, such as `gw.key`.

3 Create the CSR:

3a Enter the following command:

```
openssl req -new -key key_file_name.key -out csr_file_name.csr
```

Replace `key_file_name.key` with the key file that you created in [Step 2](#).

3b Enter the two-letter code for your country, such as `US` for the United States, `DE` for Germany, and so on.

3c Enter your state or province.

3d Enter your city.

3e Enter the name of your company or organization.

3f Enter your department or other organizational unit.

3g Enter the fully qualified domain name of the server for which you are obtaining a certificate, such as `gw3.novell.com`.

3h Enter the email address of a contact person for that server.

3i (Optional) Enter a password for the CSR.

3j (Optional) Enter a secondary name for your company or organization.

4 Skip to [“Submitting the Certificate Signing Request to a Certificate Authority”](#) on page 1111.

Windows Server 2008: Using IIS Manager

1 Open IIS Manager.

2 In the *Connections* pane, click the server to display the server Home view.

3 In the *Features View*, double-click *Server Certificate*.

4 In the *Actions* pane, click *Create Certificate Request*.

The screenshot shows a 'Request Certificate' dialog box with the following fields:

- Common name: [Empty text box]
- Organization: [Empty text box]
- Organizational unit: [Empty text box]
- City/locality: [Empty text box]
- State/province: [Empty text box]
- Country/region: [US (dropdown menu)]

Buttons at the bottom: Previous, Next, Finish, Cancel.

5 In the *Common Name* field, specify the fully qualified domain name of the server for which you are obtaining a certificate, such as `gw3.novell.com`.

6 Fill in the rest of the fields with the requested information, then click *Next*.

7 The default cryptographic service provider and bit length are acceptable, so click *Next*.

- 8 Specify a name for the CSR file, such as `gw.csr`, then click *Finish*.
If you do not specify a full path name, the CSR file is created in the `c:\Windows\System32` directory.
- 9 Skip to [“Submitting the Certificate Signing Request to a Certificate Authority”](#) on page 1111.

Windows Server 2003: Using Internet Information Services

- 1 In the Control Panel, click *Administrative Tools > Internet Information Services*.
- 2 Right-click a Web site, then click *Properties*.
- 3 On the *Directory Security* tab, click *Server Certificate*, then click *Next*.
- 4 Select *Create a new certificate*, then click *Next*.
- 5 Select *Prepare the request now, but send it later*, then click *Next*.
- 6 Specify an identifying name for the certificate, then click *Next*.
- 7 Specify your company name and department name, then click *Next*.
- 8 Specify the fully qualified domain name of the server for which you are obtaining a certificate, such as `gw3.novell.com`, then click *Next*.
- 9 Specify the location of your company, then click *Next*.
- 10 Specify a name for the CSR file, such as `gw.csr`, then click *Next*.
If you do not specify a full path name, the CSR file is created in the `c:\Windows\System32` directory.
- 11 Review the information that you have provided, then click *Next* to create the CSR file.
- 12 Continue with [Submitting the Certificate Signing Request to a Certificate Authority](#).

Submitting the Certificate Signing Request to a Certificate Authority

To obtain a server certificate, you can submit the certificate signing request (`server_name.csr` file) to a certificate authority. If you have not previously used a certificate authority, you can use the keywords “certificate authority” to search the Web for certificate authority companies.

The process of submitting the CSR varies from company to company. Most provide online submission of the request. Follow their instructions for submitting the request. The certificate authority must be able to provide the certificate in Base64/Pem or PFX format.

83.2.2 Generating a Self-Signed Certificate

There are several ways to generate a self-signed certificate:

- ♦ [“Using ConsoleOne on Windows or Linux”](#) on page 1111
- ♦ [“Using YaST on Linux”](#) on page 1113
- ♦ [“Using the openssl Command on Linux”](#) on page 1114

Using ConsoleOne on Windows or Linux

The NetIQ Certificate Server, which runs on a Linux server with NetIQ eDirectory, enables you to establish your own certificate authority and issue server certificates for yourself. For complete information, see the [NetIQ Certificate Server Web site \(https://www.netiq.com/documentation/crt33\)](https://www.netiq.com/documentation/crt33).

To quickly create your own public certificate in ConsoleOne:

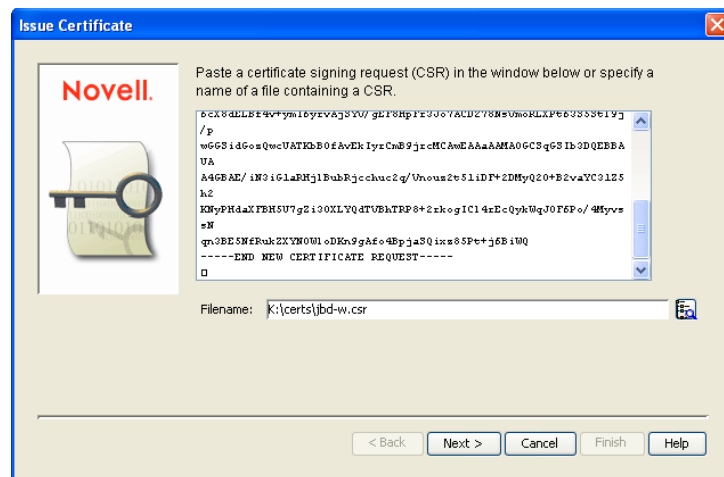
- 1 Click *Help > About Snapins* to see if the Certificate Server snap-in to ConsoleOne is installed.

If you need to install the snap-in on Linux, it is available in the version of ConsoleOne provided in the `consoleone` subdirectory in the downloaded *GroupWise 2012* software image. It is called the PKI Snapin.

If you need to install the snap-in on Windows, you can download the snap-ins for Windows ConsoleOne from the [Novell Downloads site \(http://download.novell.com/Download?buildid=FCT5LqrhcGI~\)](http://download.novell.com/Download?buildid=FCT5LqrhcGI~).

NOTE: You can create a server certificate in Novell iManager, as well as in ConsoleOne, using steps similar to those provided below.

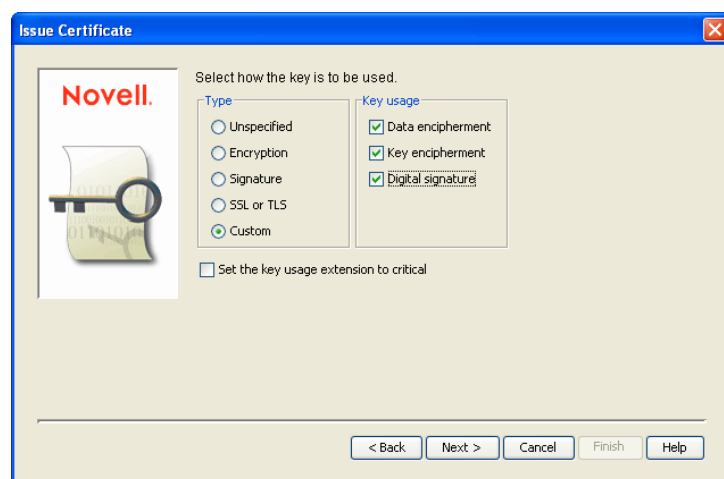
- 2 Browse to and select the container where your Server object is located.
- 3 Click *Tools > Issue Certificate*, then in the *Filename* field, browse to and select the CSR file created by GroupWise Generate CSR utility (GWCSRGEN) in “[Generating a Certificate Signing Request](#)” on page 1107.



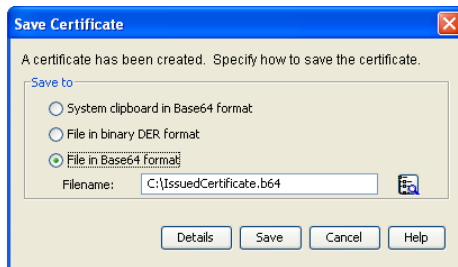
- 4 Click *Next*.

By default, your own organizational certificate authority signs the request.

- 5 Click *Next*.



- 6 In the *Type* box, select *Custom*.
- 7 In the *Key Usage* box, select all three usage options.
- 8 Click *Next*.
- 9 In the *Validity Period* field, select the length of time you want the certificate to be valid.
You might want to change the setting to a longer period of time to best meet the needs of your organization.
- 10 Click *Next*, view the summary information, then click *Finish*.
- 11 Select *File in Base64 Format*.



- 12 Specify the path and file name for the certificate.

Linux: Use only lowercase characters.

Windows: No limitations

You can retain the `.b64` extension or use the more general `.crt` extension.

- 13 Click *Save*.

Using YaST on Linux

- 1 On the Linux server desktop, click *Computer* > *YaST*, then enter the `root` password.
- 2 Click *Security and Users* > *CA Management*.
- 3 If you did not create the `YaST_Default_CA` during the installation of Linux on the server:
 - 3a Click *Import CA*, specify the name and location of an existing CA, click *OK*, then skip to [Step 4](#).
 - or
 - Click *Create Root CA*, then continue with [Step 3b](#).
 - 3b Fill in the following fields:
 - CA Name:** Specify the name of the CA certificate.
 - Common Name:** Specify the name of the certificate authority.
 - Organization:** Specify the name of your organization (for example, Novell, Inc.).
 - Organizational Unit:** Specify your organization's division that this certificate is being issued to (for example, Novell Product Development).
 - Locality:** Specify the name of your city or other regional division (for example, Provo).
 - State:** Specify the name of your state (for example, Utah). Use the full name. Do not abbreviate it.
 - Country:** Select the name of your country (for example, USA).

- 3c Click *Next*.
- 3d Specify and verify the certificate password, then click *Next*.
- 3e Click *Create* to create the root certificate authority on the server.
- 4 After you have a certificate authority on the Linux server:
 - 4a Select *YaST_Default_CA* or the CA you just created, click *Enter CA*, specify the CA password, then click *OK*.
 - 4b On the *Certificates* tab, click *Export > Export to File*.
 - 4c Select *Certificate and the Key Encrypted in PEM Format*.
 - 4d Specify the certificate password and, if desired, specify and verify a new password for the new certificate file.
 - 4e Browse to and select the directory where you want to create the certificate file, then specify the file name for the certificate, adding a `.pem` extension.
 - 4f Click *OK* to create the certificate file, then click *OK* again to confirm.
 - 4g Exit from YaST.
- 5 In a terminal window, log in as `root`, then separate the `.pem` file created by YaST into a `.crt` file and a `.key` file, as required by GroupWise:
 - 5a Use a text editor such as `gedit` to open the `.pem` file.
 - 5b Select and copy the `BEGIN CERTIFICATE` line through the `END CERTIFICATE` line into a new file, name it the same as the server name, and add a `.crt` extension to the file name when you save it.
 - 5c Select and copy the `BEGIN RSA PRIVATE KEY` line through the `END RSA PRIVATE KEY` line into a new file, name it the same as the server name, and add a `.key` extension to the file name when you save it.
 - 5d Exit the text editor.

Using the openssl Command on Linux

A convenient way to create a certificate from the Linux command line is to use the `openssl` command, as described in [HOWTO Keys \(http://www.openssl.org/docs/HOWTO/keys.txt\)](http://www.openssl.org/docs/HOWTO/keys.txt).

83.2.3 Installing the Certificate on the Server

After processing your CSRs, the certificate authority sends you a public certificate (`server_name.b64`) file for each CSR. You might need to extract the private key from the public certificate. The private key file might have an extension such as `.pem` or `.pfx`. The extension is unimportant as long as the file format is correct.

If you used the Issue Certificate feature in ConsoleOne, as described in [Section 83.2.2, "Generating a Self-Signed Certificate," on page 1111](#), it generated the public certificate file (`server_name.b64`) and private key file (`server_name.key`).

Copy the files to any convenient location on each server. The location must be accessible to the GroupWise agents that run on the server.

83.2.4 Configuring the Agents to Use SSL

To configure the agents to use SSL you must first enable them for SSL and then provide certificate and key file information. For detailed instructions, see the following sections:

- ♦ “Securing the Post Office with SSL Connections to the POA” on page 508
- ♦ “Securing the Domain with SSL Connections to the MTA” on page 643
- ♦ Section 48.2.3, “Securing Document Conversion with SSL Connections,” on page 721
- ♦ Securing GWIA Connections with SSL

83.3 Trusted Root Certificates and LDAP Authentication

LDAP authentication, as described in Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510, relies on the presence of a trusted root certificate (often named `rootcert.der`) located on your LDAP server. A trusted root certificate is automatically created for a server when you install eDirectory on that server. However, circumstances might arise where you need to create one manually. You can do this in ConsoleOne.

- 1 Make sure that Novell International Cryptography Infrastructure (NICI) is installed on the workstation where you run ConsoleOne.

If necessary, you can download NICI from the [Novell Product Downloads site \(http://download.novell.com\)](http://download.novell.com).

- 2 In ConsoleOne, click *Help > About Snapins* and verify that the following snap-ins are installed:

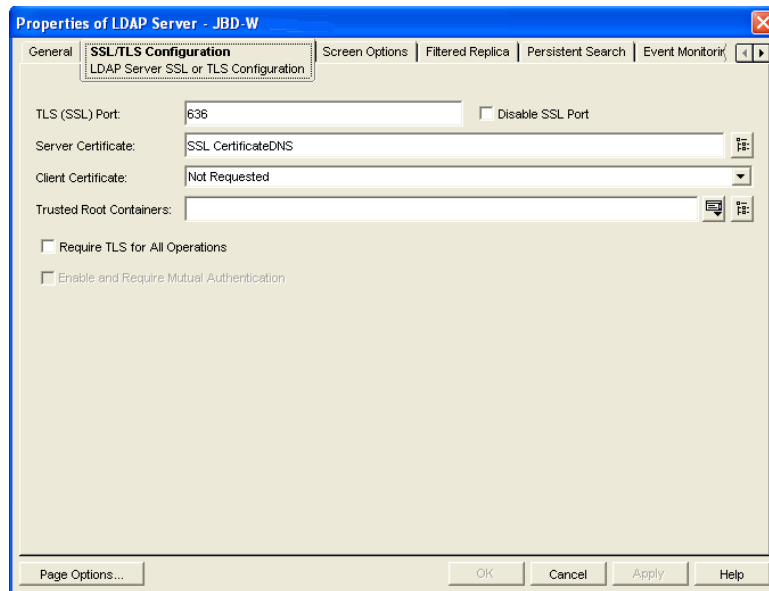
- ♦ Novell LDAP
- ♦ Novell Certificate Server
- ♦ Novell Modular Authentication Services (NMAS)

You can download these snap-ins from the [Novell Product Downloads site \(http://download.novell.com\)](http://download.novell.com). After these snap-ins are installed, you can generate a trusted root certificate for the LDAP server.

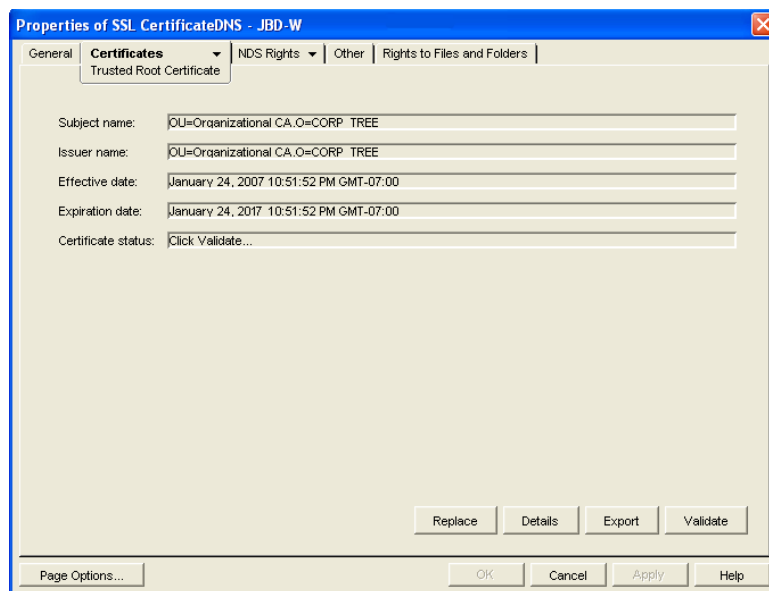
- 3 In ConsoleOne, check current SSL/TLS configuration of the LDAP server:

3a Browse to and right-click the LDAP Server object in your eDirectory tree (typically named `LDAP Server - server_name`), then click *Properties*.

3b Click *SSL/TLS Configuration*.



- 3c Note the name of the server certificate (typically `SSL.CertificateDNS`).
- 3d Make sure that *Disable SSL Port* is not selected.
- 4 Export a trusted root certificate:
 - 4a Browse to and right-click the SSL Certificate object identified in [Step 3c](#), then click *Properties*.
 - 4b Click *Certificates*.



- 5 Click *Validate*, then click *OK*.
- 6 Click *Export*.
- 7 When asked if you want to export the private key with the certificate, select *No*, then click *Next*.
- 8 In the *Output Format* box, select *File in Binary DER Format*.
- 9 In the *Filename* field, specify the full path and file name for the trusted root certificate.

IMPORTANT: For use with GroupWise, the name of the trusted root certificate file can consist of 8 characters plus the `.der` extension. It cannot be a long file name. The most convenient location for the trusted root certificate for use with GroupWise is in the directory where the POA software is installed. By default, the POA looks for a file named `ngwkey.der`.

10 Click *Next*, then click *Finish*.

You are now ready to configure the POA for LDAP authentication, as described in [Section 36.3.4, "Providing LDAP Authentication for GroupWise Users,"](#) on page 510.

84 LDAP Directories

LDAP (Lightweight Directory Access Protocol) is a standard Internet protocol for accessing commonly used network directories. If you are new to GroupWise or LDAP, you might find it useful to review TID 2955731, "GroupWise and LDAP," in the [Novell Support Knowledgebase](http://www.novell.com/support). (<http://www.novell.com/support>) This TID provides an overview of LDAP and explains the two address-book-related ways that GroupWise makes use of LDAP. This section briefly summarizes the address book usages of LDAP and explains how LDAP can also be used to store security information such as passwords and certificates for use with GroupWise.

- ◆ [Section 84.1, "Accessing Public LDAP Directories from GroupWise," on page 1119](#)
- ◆ [Section 84.2, "Offering the GroupWise Address Book as an LDAP Directory," on page 1119](#)
- ◆ [Section 84.3, "Authenticating to GroupWise with Passwords Stored in an LDAP Directory," on page 1120](#)
- ◆ [Section 84.4, "Accessing S/MIME Certificates in an LDAP Directory," on page 1121](#)

See also [Part XVIII, "Security Policies," on page 1149](#).

84.1 Accessing Public LDAP Directories from GroupWise

The GroupWise client uses LDAP to provide access to directory services such as Bigfoot. This enables GroupWise users to select email addresses from these popular directory services and add them to their personal GroupWise address books. See "[Using the LDAP Address Book](#)" in "[Contacts and Address Books](#)" in the *GroupWise 2012 Windows Client User Guide*.

84.2 Offering the GroupWise Address Book as an LDAP Directory

The GroupWise Internet Agent (GWIA) uses LDAP to make the GroupWise address book available to any LDAP-enabled client. This enables users of other email clients to define GroupWise address books as LDAP directories from which they can select email addresses. See [Section 53.3, "Configuring LDAP Services," on page 782](#). See also [Chapter 86, "Address Book Security," on page 1125](#).

84.3 Authenticating to GroupWise with Passwords Stored in an LDAP Directory

Enabling LDAP authentication for the POA is independent of these LDAP address book features. You need to enable LDAP authentication when you want the POA to authenticate the user's password in an LDAP directory rather than looking for a password in the user's GroupWise account information. The POA can make use of the following LDAP capabilities:

- ♦ [Section 84.3.1, "Access Method," on page 1120](#)
- ♦ [Section 84.3.2, "LDAP User Name," on page 1120](#)

When you understand these LDAP capabilities, you are ready to set up LDAP authentication for your GroupWise users. See [Section 36.3.4, "Providing LDAP Authentication for GroupWise Users," on page 510](#).

84.3.1 Access Method

On a server-by-server basis (ConsoleOne > *Tools* > *GroupWise System Operations* > *LDAP Servers*), you can specify whether you want each LDAP server to respond to authentication requests using a bind or a compare.

- ♦ **Bind:** With a bind, the POA essentially logs in to the LDAP server. When responding to a bind request, most LDAP servers enforce password policies such as grace logins and intruder lockout, if such policies have been implemented by the LDAP directory.
- ♦ **Compare:** With a compare, the POA provides the user password to the LDAP server. When responding to a compare request, the LDAP server compares the password provided by the POA with the user's password in the LDAP directory, and returns the results of the comparison. Using a compare connection can provide faster access because there is typically less overhead involved because password policies are not being enforced.

Regardless of whether the POA is submitting bind requests or compare requests to authenticate GroupWise users, the POA can stay connected to the LDAP server as long as authentication requests continue to occur before the connection times out. This provides quick response as users are accessing their mailboxes.

84.3.2 LDAP User Name

On a post office-by-post office basis (ConsoleOne > Post Office object > *Properties* > *GroupWise* > *Security*), you can decide what user name you want the POA to use when accessing the LDAP server.

- ♦ **LDAP Username Login:** If you want the POA to access the LDAP server with specific rights to the LDAP directory, you can provide a user name for the POA to use when logging in. The rights of the user determine what information in the LDAP directory will be available during the authentication process.
- ♦ **Public or Anonymous Login:** If you do not provide a specific LDAP user name as part of the post office LDAP configuration information, then the POA accesses the LDAP directory with a public or anonymous connection. Only public information is available when using such a login.

84.4 Accessing S/MIME Certificates in an LDAP Directory

Just as the POA can access user password information in an LDAP directory, the GroupWise Windows client can access recipients' digital certificates in an LDAP directory. See ["Using LDAP to Search for Recipient Encryption Certificates"](#) in ["Email"](#) in the *GroupWise 2012 Windows Client User Guide*.

When a certificate is stored on an LDAP server, the GroupWise Windows client searches the LDAP server every time the certificate is used. Certificates from LDAP servers are not downloaded into the local certificate store on the user's workstation.

To facilitate this process, the user must select a default LDAP directory in the LDAP address book (Windows client > *Address Book* > *Novell LDAP Address Book* > *Directories* > *Set as Default*) and enable searching (Windows client > *Tools* > *Options* > *Security* > *Send Options* > *Advanced Options* > *Search for recipient encryption certificates in the default LDAP directory defined in LDAP Address Book*).

An advantage to this is that recipients' certificates are available no matter what workstation the GroupWise user sends the message from.

NOTE: This feature is not available in GroupWise WebAccess.

85 Message Security

The GroupWise client accommodates users' preferences for security and privacy when sending messages. Users can:

- ◆ Sign a message with standardized text (Windows client > *Tools > Options > Environment > Signature*).
- ◆ Sign a message with an electronic business card (vCard) (Windows client > *Tools > Options > Environment > Signature*).
- ◆ Digitally sign and encrypt a message. See [Section 83.1, "Personal Digital Certificates, Digital Signatures, and S/MIME Encryption,"](#) on page 1105.
- ◆ Give a message a security classification (Windows client > *New Mail > Send Options > General > Classification > Normal, Proprietary, Confidential, Secret, Top Secret, or For your eyes only*).
- ◆ Conceal the subject of an email message (Windows client > *New Mail > Send Options > Security > Conceal subject*).
- ◆ Mark messages and appointments private so that proxy users cannot see them. (Windows client > *Actions > Mark Private*).
- ◆ Attach a password-protected document to a message and have the application prompt the recipient to supply the password before the recipient can open the document
- ◆ Require a password in order to mark a Routing Slip completed (Windows client > *Tools > Options > Security > Send Options > Require password to complete routed item*). This can prevent a user who is proxied to the mailbox from marking the item completed, or if multiple users proxy to the mailbox, it can be used to ensure that only the user for whom the item was intended can complete it.

In addition, if the users in your GroupWise system exchange messages with users in other GroupWise systems, you can set preferences to control what types of information pass between the two systems. For example, you can prevent external GroupWise users from performing busy searches or obtaining message delivery status. See [Section 4.2, "System Preferences,"](#) on page 72.

See also [Part XVIII, "Security Policies,"](#) on page 1149.

86 Address Book Security

One of the purposes of the Address Book is to make user information available to all GroupWise users. However, there might be types of information that you do not want to display.

- ♦ [Section 86.1, “eDirectory Information Displayed in the Address Book,” on page 1125](#)
- ♦ [Section 86.2, “Suppressing the Contents of the User Description Field,” on page 1125](#)
- ♦ [Section 86.3, “Controlling GroupWise Object Visibility in the Address Book,” on page 1126](#)
- ♦ [Section 86.4, “Controlling GroupWise Object Visibility between GroupWise Systems,” on page 1126](#)

See also [Part XVIII, “Security Policies,” on page 1149](#).

86.1 eDirectory Information Displayed in the Address Book

The Address Book displays information stored in Novell eDirectory for users, resources, and distribution lists in your GroupWise system. By default, the following information is displayed:

- ♦ Name
- ♦ Office phone number
- ♦ Department
- ♦ Fax number
- ♦ User ID

You can configure the Address Book to display more or less information to meet the needs of your users. See [Section 6.1, “Customizing Address Book Fields,” on page 105](#).

By default, all users, resources, and distribution lists that you create in eDirectory are displayed in the Address Book and are available to all GroupWise users.

86.2 Suppressing the Contents of the User Description Field

By default, when you display details about a user in the Address Book, the information in the Description field of the User object in eDirectory is displayed. If you keep confidential information in the Description field of the User object, you can prevent this information from appearing the GroupWise Address Book. See [Section 6.1.6, “Preventing the User Description Field from Displaying in the Address Book,” on page 109](#).

86.3 Controlling GroupWise Object Visibility in the Address Book

You might need to create users, resources, or distribution lists that are not available to all GroupWise users. You can accomplish this by restricting the set of users that can see such objects in the Address Book. You can make such objects visible only to the members of a domain, only to the members of a post office, or to no one at all. An object does not need to be visible to be addressable. For instructions, see [Section 6.2, “Controlling Object Visibility,”](#) on page 110.

86.4 Controlling GroupWise Object Visibility between GroupWise Systems

If you synchronize your GroupWise system with other GroupWise systems to simplify addressing for users of both systems, you can control what information from your Address Book you want to be available in the Address Books of other GroupWise systems. For instructions, see [“Exchanging Information Between Systems”](#) in [“Connecting to Other GroupWise Systems”](#) in the *GroupWise 2012 Multi-System Administration Guide*.

87 GroupWise Administrator Rights

To administer GroupWise, a user needs the appropriate file system rights and Novell eDirectory rights. The following sections provide information to help you configure GroupWise administrator rights to meet the needs of your environment:

- ♦ [Section 87.1, “Setting Up a GroupWise Administrator as an Admin Equivalent,” on page 1127](#)
- ♦ [Section 87.2, “Assigning Rights Based on Administration Responsibilities,” on page 1127](#)
- ♦ [Section 87.3, “eDirectory Object and Properties Rights,” on page 1135](#)
- ♦ [Section 87.4, “Granting or Removing Object and Property Rights,” on page 1138](#)

See also [Part XVIII, “Security Policies,” on page 1149](#).

87.1 Setting Up a GroupWise Administrator as an Admin Equivalent

The easiest way to ensure that a GroupWise administrator has all necessary eDirectory rights and file system rights is to make the administrator an Admin equivalent in eDirectory. Unless you have implemented multiple administrators who have different roles and access rights (for example, a server administrator, a printer administrator, and a GroupWise administrator), we suggest you make your GroupWise administrator an Admin equivalent.

- 1 In ConsoleOne, right-click the GroupWise administrator’s User object, then click *Properties*.
- 2 Click the *Memberships* tab, then click *Security Equal To* to display the Security Equal To page.
- 3 Click *Add* to display the Select Objects dialog box.
- 4 Browse for and select the Admin object, then click *OK*.
The Admin object should now be displayed in the *Security Equal To* list.
- 5 Click *OK*.

87.2 Assigning Rights Based on Administration Responsibilities

Making a GroupWise administrator an Admin equivalent in eDirectory gives the GroupWise administrator all eDirectory rights required to administer GroupWise. It also gives him or her full file system rights to servers that have associated objects in eDirectory. To increase security or to support a distributed administration model, you can restrict GroupWise administrators’ file system and eDirectory rights to only those required to administer GroupWise and assign rights to your GroupWise administrators based on their administration responsibilities. For example,

- ♦ If you have only one GroupWise administrator (a centralized GroupWise administration model), you can give the administrator rights only to the eDirectory objects and file systems that are used for GroupWise.

- ♦ If you have multiple administrators who are each responsible for a domain (a distributed GroupWise administration model), you can restrict their rights to only those eDirectory objects and file systems associated with their GroupWise domain.
- ♦ If you have one administrator whom you want to control all links between domains, you can assign rights to the eDirectory objects and file systems associated with domain links.

The following two sections, [Section 87.2.1, “File System Rights,” on page 1128](#) and [Section 87.2.2, “eDirectory Rights,” on page 1128](#), provide general information about the file system rights and eDirectory object and property rights needed to perform GroupWise administration tasks.

The final section, [Section 87.2.3, “Common Types of GroupWise Administrators,” on page 1132](#), lists some common types of GroupWise administrators (for example, Domain administrator and Post Office administrator) and the specific file system and eDirectory rights they need.

87.2.1 File System Rights

A GroupWise administrator must have an account (or security equivalence) that provides the following rights to the directories listed below:

Directory	Linux Rights	Windows Permissions
Any GroupWise system directory the administrator is responsible for. This includes: <ul style="list-style-type: none"> ♦ domain directories ♦ post office directories ♦ software distribution directories ♦ library storage area directories 	Read Write Execute	Full Control
Any directory in which the GroupWise agents are installed. For Linux, the default directory is <code>/opt/novell/groupwise/agents</code> . For Windows, the default agent subdirectories are located under <code>c:\Program Files\Novell\GroupWise Server</code> .	Read Write Execute	Full Control

For information about managing the Linux agents as a non-root user, see [“Running the Linux GroupWise Agents as a Non-root User”](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.

87.2.2 eDirectory Rights

The eDirectory object and property rights an administrator must have depend on the administrative tasks he or she needs to perform. In GroupWise administration, there are five basic tasks an administrator can perform:

- ♦ [Create and delete objects](#) (for example, domains, post offices, gateways, agents, libraries, resources, external entities, and distribution lists).
- ♦ [Modify object properties](#) (for example, moving a GroupWise user from one post office to another or deleting a GroupWise user from a distribution list).

- ♦ [Modify link information](#) (for example, defining whether Domain 1 links directly to Domain 3 or indirectly to Domain 3 through Domain 2).
- ♦ [Perform system operations](#) (for example, managing software distribution directories, creating administrator-defined fields, and setting up eDirectory user synchronization).
- ♦ [Perform maintenance operations](#) (for example, rebuilding domain and post office databases, analyzing and fixing user and message databases, and changing a user's client options).

Creating and Deleting Objects

The following rules apply to creating or deleting a GroupWise object (for example, domain, post office, gateway, agent, library, resource, external entity, or distribution list):

- ♦ To create a GroupWise object, the administrator must have Create object rights in the container where he or she is creating the object. To delete a GroupWise object, the administrator must have Delete object rights to the GroupWise object's container.
- ♦ If creating or deleting the object requires modification of a second object's properties, the administrator must have Read and Write rights to the second object's NGW: GroupWise ID property and all other affected properties. For example, when you create a distribution list, the list is assigned to a post office. Therefore, the administrator needs Read and Write rights to the post office object's NGW: GroupWise ID property and NGW: Distribution List Member property.

For information about giving a user rights to an object or an object's properties or restricting a user's rights to an object or an object's properties, see [Section 87.4, "Granting or Removing Object and Property Rights,"](#) on page 1138.

Modifying Object Properties

Each eDirectory object has certain properties that hold information about the object. For example, a User object includes Full Name, Given Name, Last Name, Network Address, and Title properties. The following rules apply to modifying an object's properties:

- ♦ Each object has an NGW: GroupWise ID property. The administrator must always have Read and Write rights to the NGW: GroupWise ID property for the object being modified. Without rights to the NGW: GroupWise ID property, no modifications can be made to any of the object's GroupWise properties.
- ♦ The administrator must have Read and Write rights to the property being modified. For example, to change a user's visibility within the GroupWise system, the administrator must have Read and Write rights to the user object's NGW: GroupWise ID property and NGW: Visibility property.
- ♦ If the modification affects a second object's properties, the administrator must have Read and Write rights to the second object's affected properties. For example, when you move a user from one post office to another, the move affects properties for 1) the User object, 2) the Post Office object from which you are moving the user (the source post office) and 3) the Post Office object to which you are moving the user (the target post office). Therefore, the administrator must have 1) Read and Write rights for the User object's NGW: GroupWise ID property and NGW: Post Office property, 2) Read and Write rights for the source post office object's NGW: GroupWise ID property and Members property, and 3) Read and Write rights for the target post office object's NGW: GroupWise ID property and Members property.

Modifications to an object can fail for the following reasons:

- ♦ The administrator does not have the appropriate rights to the object's properties. For example, to restrict an administrator from moving a user from one post office to another, you could 1) not give the administrator Read and Write rights to the source or target post office object's NGW: Members property or 2) not give the administrator Read and Write rights to the user object's NGW: Post Office property.
- ♦ The administrator, in addition to modifying properties he or she has rights to, attempts to modify a property he or she does not have rights to modify. For example, if an administrator has rights to modify a user's mailbox ID and visibility but does not have rights to modify the mailbox expiration date, any modifications made to the mailbox ID and visibility fail if the administrator tries to modify the mailbox expiration date at the same time.

In general, a GroupWise administrator should have Read and Write rights to all GroupWise properties for the objects he or she needs to administer. This ensures that the administrator can modify all GroupWise information for the objects. In addition, an administrator should also have Read and Write rights to other eDirectory properties used by GroupWise. For example, Full Name is an eDirectory User object property used by GroupWise. For a list of GroupWise objects, GroupWise object properties, associated eDirectory object properties, see [Section 87.3, "eDirectory Object and Properties Rights," on page 1135](#).

For information about giving a user rights to modify an object's properties or restricting a user's rights to modify an object's properties, see [Section 87.4, "Granting or Removing Object and Property Rights," on page 1138](#).

Modifying Link Information

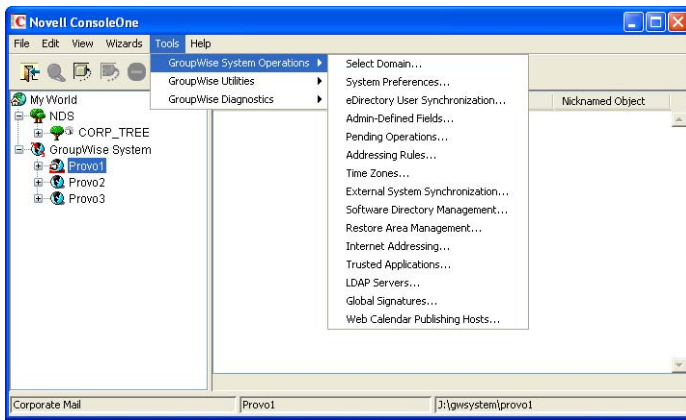
By default, when an administrator creates a domain or post office, the links to other domains or post offices are automatically created. Because there are many different ways you can configure your domain and post office links, you can use the Link Configuration utility to modify how domains and post offices are linked together. You can also use object and property rights to determine which administrators have the ability to modify link information. The following rules apply to modifying link information:

- ♦ To modify the links for post offices within a domain, the administrator must have Read and Write rights to the NGW: GroupWise ID property for the Domain object and the Post Office objects. In addition, the administrator must have Write rights to the NGW: Link Configuration property for the Domain object.
- ♦ To modify the links between domains, the administrator must have Read and Write rights to the NGW: GroupWise ID property for each Domain object, and Write rights to the NGW: Link Configuration property for each Domain object.

Because correct domain and post office links are essential to the proper functioning of your GroupWise system, you might want to assign link configuration tasks to a single administrator and restrict other administrators' abilities to modify link information. Or, if you have a multiple-domain system with multiple administrators, you could have one administrator responsible for all domain links and the other administrators responsible for the post office links for their domains. For information about giving a user rights to an object's properties (or restricting a user's rights to an object's properties), see [Section 87.4, "Granting or Removing Object and Property Rights," on page 1138](#).

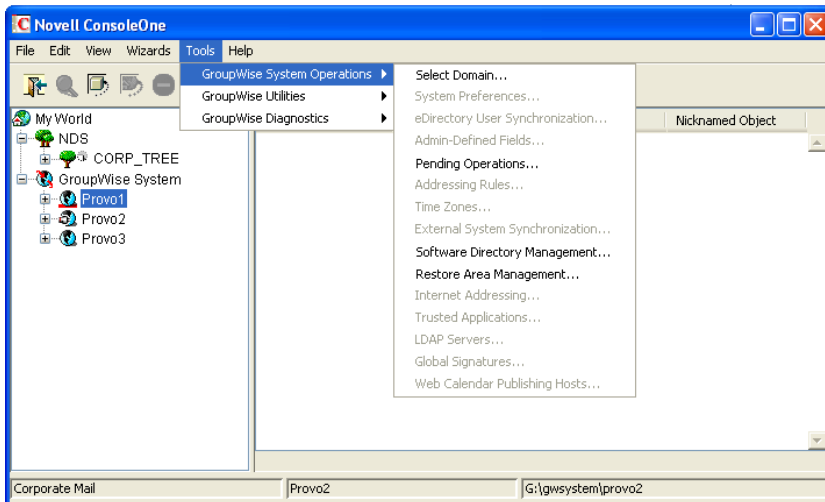
Performing System Operations

The system operations that a GroupWise administrator can perform in ConsoleOne are listed on the *Tools > GroupWise System Operations* menu.



The *Select Domain*, *Pending Operations*, and *Restore Area Management* operations are always available to GroupWise administrators. To perform any of the other system operations, an administrator must have Read and Write rights to the NGW: GroupWise ID property for the primary Domain object. In GroupWise systems that span multiple eDirectory trees, the administrator's current tree must be the tree in which the primary Domain object is located.

You can restrict the ability to perform system operations (other than *Select Domain*, *Pending Operations*, and *Restore Area Management*) to only those GroupWise administrators who connect to the primary domain database. To do so, you use the *Restrict System Operations to Primary Domain* option (*Tools > GroupWise System Operations > System Preferences > Admin Lockout Settings*). Administrators connected to secondary domain databases see the GroupWise System Operations menu with only the *Select Domain*, *Pending Operations*, and *Restore Area Management* options available.



For information about giving a user rights to an object's properties or restricting a user's rights to an object's properties, see [Section 87.4, "Granting or Removing Object and Property Rights,"](#) on page 1138.

Performing Maintenance Operations

To perform maintenance operations such as validating, recovering, or rebuilding domain databases; fixing user, resource, or post office databases; or changing a user's client options, an administrator must have Read and Write rights to the NGW: GroupWise ID property for the object being modified. For example, to rebuild a domain database, an administrator must have Read and Write rights to the

NGW: GroupWise ID property for the Domain object. Or, to change a user's client options, an administrator must have Read and Write rights to the NGW: GroupWise ID property for the User object.

For information about giving a user rights to an object's properties or restricting a user's rights to an object's properties, see [Section 87.4, "Granting or Removing Object and Property Rights,"](#) on page 1138.

87.2.3 Common Types of GroupWise Administrators

The following sections provide information about assigning directory, object, and property rights to some common types of GroupWise administrators:

- ♦ ["Domain Administrator" on page 1132](#)
- ♦ ["Post Office Administrator" on page 1133](#)
- ♦ ["Link Configuration Administrator" on page 1134](#)

Domain Administrator

A Domain administrator is a GroupWise administrator who has all file system and eDirectory rights needed to create and maintain a single GroupWise domain.

File System Rights

A Domain administrator must have the file system rights listed in the following table:

Directory	Linux Rights	Windows Permissions
Any GroupWise system directory the administrator is responsible for. This includes: <ul style="list-style-type: none"> ♦ domain directories ♦ post office directories ♦ software distribution directories ♦ library storage area directories If the domain is not yet created, it is necessary to give the administrator rights to the directories where it will be created.	Read Write Execute	Full Control
The GroupWise agent directories. For Linux, the default directory is <code>/opt/novell/groupwise/agents</code> . For Windows, the default directory is <code>c:\Program Files\Novell\GroupWise Server\Agents</code> .	Read Write Execute	Full Control

eDirectory Rights

A Domain administrator must have Read and Write rights to properties for the objects listed below.

- ♦ **Domain object:** Only the domain that the administrator is responsible for unless he or she will also configure domain links. If so, the administrator also needs rights to the NGW: GroupWise ID and NGW: Link Configuration properties for the other Domain objects.

- ♦ **Post Office objects:** All post offices in the domain.
- ♦ **Gateway objects:** All gateways in the domain.
- ♦ **User objects:** All users in the domain.
- ♦ **Resource objects:** All resources in the domain.
- ♦ **Distribution List objects:** All distribution lists in the domain.
- ♦ **Library objects:** All libraries in the domain.
- ♦ **Agent objects:** All MTAs and POAs in the domain.
- ♦ **External Entity objects:** All resources in the domain.

In most cases, the administrator does not need rights to all of the object properties. After reviewing the list of objects, if you want to restrict an administrator's rights to only the required properties, see [Section 87.3, "eDirectory Object and Properties Rights," on page 1135](#).

In addition, the administrator must have Create and Delete rights in any container in which one of the objects listed above will be created or deleted.

For a listing of the explicit object properties to which the administrator must have rights, see [Section 87.3, "eDirectory Object and Properties Rights," on page 1135](#).

Post Office Administrator

A Post Office administrator is a GroupWise administrator who has all file system and eDirectory rights needed to create and maintain a single GroupWise post office.

File System Rights

A Post Office administrator must have the file system rights listed in the following table:

Directory	Linux Rights	Windows Permissions
The domain directory	Read Write Execute	Full Control
The following directories: <ul style="list-style-type: none"> ♦ post office directory ♦ library storage area directories for libraries assigned to the post office 	Read Write Execute	Full Control
The directory for the Post Office Agent. For Linux, the default directory is <code>/opt/novell/groupwise/agents</code> . For Windows, the default directory is <code>c:\Program Files\Novell\GroupWise Server\Agents</code> .	Read Write Execute	Full Control

eDirectory Rights

A Post Office administrator must have Read and Write rights to properties for the objects listed below.

In most cases, the administrator does not need rights to all of the object properties. After reviewing the list of objects, if you want to restrict an administrator's rights to only the required properties, see [Section 87.3, "eDirectory Object and Properties Rights," on page 1135](#).

- ♦ **Post Office object:** Only the post office that the administrator is responsible for.
- ♦ **User objects:** All users with accounts on the post office.
- ♦ **Resource objects:** All resources assigned to the post office.
- ♦ **Distribution List objects:** All distribution lists assigned to the post office.
- ♦ **Library objects:** All libraries assigned to the post office.
- ♦ **Agent objects:** Only the post office's POA.
- ♦ **External Entity objects:** All external entities with accounts on the post office.

In addition, the administrator must have Create and Delete rights in any container in which one of the objects listed above will be created or deleted.

Link Configuration Administrator

A Link Configuration administrator has all file system and eDirectory rights needed to create and maintain the links between GroupWise domains.

File System Rights

A Link Configuration administrator must have the file system rights listed in the following table:

Directory	Linux Rights	Windows Permissions
ConsoleOne and GroupWise Administrator snap-ins	Read Write Execute	Not applicable
Domain directory	Read Write Execute	Full Control

eDirectory Rights

A Post Office administrator must have Read and Write rights to the properties for the objects listed below.

Object	Property
Domain (all domains)	NGW: GroupWise ID NGW: Link Configuration

87.3 eDirectory Object and Properties Rights

The table in this section lists the GroupWise objects and their properties.

Some properties are specific only to GroupWise. GroupWise-specific properties begin with NGW or ngw. Other properties are common eDirectory properties used by GroupWise objects. Common eDirectory properties do not begin with NGW or ngw.

Object	Property
Domain	NGW: File ID
	NGW: GroupWise ID
	NGW: Language
	NGW: Link Configuration
	NGW: Location
	NGW: Time Zone ID
	NGW: Type
	NGW: Version
	ngwDefaultWebAccess
	CN (Common Name)
	Description Member
Post Office	NDA: Port
	NGW: Access Mode
	NGW: Distribution List Member
	NGW: Domain
	NGW: File ID
	NGW: GroupWise ID
	NGW: Language
	NGW: Library Member
	NGW: Location
	NGW: Resource Member
	NGW: Time Zone ID
	NGW: Version
	ngwDefaultWebAccess
	ngwLDAPServerAddress
	CN (Common Name)
Description Member	

Object	Property
Gateway	NGW: Domain
	NGW: File ID
	NGW: GroupWise ID
	NGW: Language
	NGW: Location
	NGW: Platform
	NGW: Time Zone ID
	NGW: Type
	ngwProviderComm
	ndaReferenceList
	ndaServiceList
	ndaXISettings
	CN (Common Name)
	Description
User	NGW: Account
	NGW: File ID
	NGW: Gateway Access
	NGW: GroupWise ID
	NGW: Mailbox Expiration Date
	NGW: Object ID
	NGW: Post Office
	NGW: Visibility
	ngwNLSInfo
	company
	Department
	Description
	EMail Address
	Fax Number
	General Qualifier
	Given Name
	homePhone (Home Phone)
	Initials
	Internet EMail Address
	L (Location)
	Last Name
	mobile (Mobile Phone)
	otherPhoneNumber (Other Phone)
	pager (Pager Number)
	personalTitle
	Physical Delivery Office Name (City)
	Postal Code (Zip Code)
	Postal Office Box (PO Box)
	S (State)
	SA (Street Address)
	Telephone
Title	

Object	Property
Resource	NGW: File ID NGW: GroupWise ID NGW: Owner NGW: Post Office NGW: Type NGW: Visibility CN (Common Name) Description
Distribution List	NGW: Blind Copy Member NGW: Carbon Copy Member NGW: GroupWise ID NGW: Post Office NGW: Visibility CN (Common Name) Description Member
Library	NGW: Archive Max Size NGW: Document Area Size NGW: File ID NGW: GroupWise ID NGW: Library Display Name NGW: Post Office NGW: Starting Version Number CN (Common Name) Description Member
Agent	NGW: File ID NGW: GroupWise ID NGW: Platform NGW: Type ngwProxyServerAddress ndaServiceList ndaServiceList ndaXISettings CN (Common Name) Description Network Address

Object	Property
External Entity	NGW: Account ID
	NGW: External Net ID
	NGW: File ID
	NGW: GroupWise ID
	NGW: Mailbox Expiration Time
	NGW: Object ID
	NGW: Post Office
	NGW: Visibility
	company
	Department
	Description
	EMail Address
	Fax Number
	Generational Qualifier
	Given Name
	homePhone (Home Phone)
	Initials
	Internet EMail Address
	L (Location)
	Last Name
	mobile (Mobile Phone)
	otherPhoneNumber (Other Phone)
	pager (Pager Number)
	personalTitle
	Physical Delivery Office Name (City)
	Postal Code (Zip Code)
	Postal Office Box (PO Box)
	S (State)
	SA (Street Address)
	Telephone
	Title

87.4 Granting or Removing Object and Property Rights

You can use trustee assignments to grant or restrict rights to an object and its properties. The following steps provide one way to grant or remove a user's rights to an object or its properties. For additional methods, see your eDirectory documentation.

- 1 Right-click the object in the eDirectory tree, then click *Trustees of this Object*.
- 2 Click *Add Trustee* to display the Select Object dialog box.
- 3 Browse for and select the User object, then click *OK* to display the Rights Assigned to Selected Objects dialog box.
- 4 Set the object and property rights you want. If necessary, add additional properties. Click *Help* for additional information.
- 5 Click *OK* when you are finished.



GroupWise Agent Rights

When you create domains and post offices, ConsoleOne creates the directory structures and Agent objects with all the required rights to enable the agents to function properly, regardless of link type between locations and including requirements for Novell eDirectory user synchronization. No manual adjustment of agent rights is necessary in GroupWise 2012.

You can check the POA's rights to the post office directory by starting it using the [/rights](#) switch in the POA startup file.

See also [Part XVIII, "Security Policies,"](#) on page 1149.

89 GroupWise User Rights

GroupWise users require specific Novell eDirectory rights and, in some cases, specific file system rights in order for the GroupWise client to function properly. The following sections provide information about the required rights and how to supply them.

- ♦ [Section 89.1, “eDirectory Rights,” on page 1141](#)
- ♦ [Section 89.2, “File System Rights,” on page 1143](#)

See also [Part XVIII, “Security Policies,” on page 1149](#).

89.1 eDirectory Rights

By default, ConsoleOne is configured to automatically provide a GroupWise user’s required eDirectory rights when you add the user to a post office. You can, however, configure GroupWise Administrator to not assign rights automatically, in which case you would need to manually assign eDirectory rights.

The following sections provide information about how to configure ConsoleOne to automatically set GroupWise users’ eDirectory rights and how to manually set these rights:

- ♦ [Section 89.1.1, “Configuring ConsoleOne to Automatically Set eDirectory Rights When Creating User Accounts,” on page 1141](#)
- ♦ [Section 89.1.2, “Manually Granting eDirectory Rights,” on page 1142](#)

89.1.1 Configuring ConsoleOne to Automatically Set eDirectory Rights When Creating User Accounts

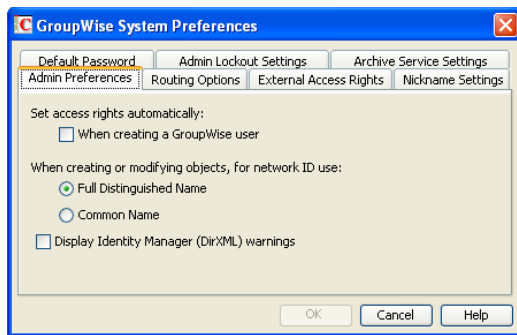
By default, the GroupWise Administrator snap-in for ConsoleOne is configured to automatically set the eDirectory rights required by a GroupWise user. This is done when you create the user’s GroupWise account.

For GroupWise Administrator to be able to set these rights, you must have sufficient administrative rights to eDirectory. If you don’t have sufficient rights to manually set the user’s access rights, GroupWise Administrator does not have sufficient rights to set them automatically. In general, we recommend that you be an Admin equivalent. For more information, see [Chapter 87, “GroupWise Administrator Rights,” on page 1127](#).

If you choose not to grant eDirectory rights automatically, you should manually set the rights to ensure that users have appropriate access. For instructions, see [Section 89.1.2, “Manually Granting eDirectory Rights,” on page 1142](#).

To configure whether or not GroupWise Administrator automatically assigns rights to users when you create GroupWise accounts:

- 1 In ConsoleOne, click *Tools > GroupWise System Operations > System Preferences* to display the GroupWise System Preferences dialog box.



- 2 To have GroupWise Administrator automatically set access rights, select the *Set Access Rights Automatically When Creating a GroupWise User* option.

or

To turn off this option, deselect the *Set Access Rights Automatically When Creating a GroupWise User* option.

- 3 Click *OK* to save your changes.

89.1.2 Manually Granting eDirectory Rights

At startup, the GroupWise client must know the following:

- ♦ The post office where the user has an account.
- ♦ Whether to connect to the user's post office in direct access mode or client/server access mode.

The user can supply this information in the GroupWise Startup dialog box that appears or use the `/ph-path_to_post_office`, `/ipa-IP_address`, `/ipp-TCP_port`, and `/@u-user_ID` startup options.

If you do not want users to be required to supply this information, you can give users rights to the eDirectory objects shown below. When a user has rights to the objects, the GroupWise client can read the object's information in eDirectory to determine the user's post office and access mode. This must have users to be logged in to eDirectory.

Object and Properties	Rights
User object	Browse
NGW:Post Office	Read
Post Office object	Browse
NGW:Location	Read
NGW:Access Mode	Read
POA object	Browse
NGW:Type	Read
Network Address	Read

GroupWise Name Server (ngwnameserver)

The following information applies to users running the GroupWise client in client/server access mode.

If you do not want to provide eDirectory rights to GroupWise users as explained above, or if you have GroupWise users who don't log in to eDirectory, you can set up a GroupWise name server. A GroupWise name server enables users to access their post office without knowing the IP address and port number of the POA.

The GroupWise name server is a DNS host entry for one of the POAs in your GroupWise system. At startup, the GroupWise client automatically looks for the GroupWise name server. When a user reaches the POA designated as the GroupWise name server, the POA redirects the user to the IP address and port number of the POA that services the user's post office.

The primary GroupWise name server must be named `ngwnameserver`. You can set up one backup GroupWise name server and name it `ngwnameserver2`. Both POAs must use the default TCP port of 1677.

To set up a GroupWise name server:

- 1 Use your tool of choice for modifying DNS.
- 2 Create an entry for the IP address of the POA you want to designate as the primary GroupWise name server, then give it the hostname `ngwnameserver`.
- 3 Create an entry for the IP address of the POA you want to designate as the backup GroupWise name server, then give it the hostname `ngwnameserver2`.

89.2 File System Rights

Listed below are the locations you need to consider when assigning file system rights to GroupWise users:

- ♦ **Domain Directory:** Users do not need file system access to the domain directory.
- ♦ **Post Office Directory:** The recommended post office access mode for the GroupWise client is client/server (TCP/IP), which means that the user does not need file system access to the post office. Therefore, ConsoleOne does not assign any file system rights when you add a user to a post office.
- ♦ **GroupWise Software Distribution Directory:** If you want users to have file system rights to a GroupWise software distribution directory to install or run the GroupWise client, you need to manually assign rights. For instructions, see [Section 89.2.1, "Granting File System Rights to the Software Distribution Directory,"](#) on page 1143.
- ♦ **Mailbox Backup Directory:** For users to restore their mailbox from a network backup directory, they need the appropriate file system rights to the directory. For more information, see [Section 89.2.2, "Granting File System Rights to the Mailbox Backup Directory,"](#) on page 1144.

89.2.1 Granting File System Rights to the Software Distribution Directory

The software distribution directory contains the GroupWise client for Windows. To set up and run the GroupWise client, users need the directory rights listed in the table below.

Directories	Linux Rights	Windows Permissions
<i>software distribution directory</i>	Read	Read

Directories	Linux Rights	Windows Permissions
admin	-----	No Access
agents	-----	No Access
client	Read	Read
ofviews	Read	Read
win32	Read	Read
internet	-----	No Access
domain	-----	No Access
po	-----	No Access

IMPORTANT: Users need rights only to the `client` directory and subdirectories. The other directories (`admin`, `agents`, `domain`, `internet`, and `po`) are administration directories that users should not have access to.

89.2.2 Granting File System Rights to the Mailbox Backup Directory

If you back up a user's network mailbox, or a user backs up his or her local mailbox, to a network location, the user needs Read and Write file system rights to the backup directory in order to restore his or her mailbox.

90 Spam Protection

Unwanted Internet email messages (spam) can be a distracting nuisance to GroupWise client users. Your first line of defense against spam is the Internet Agent (GWIA). Your second line of defense is the Junk Mail Handling feature of the GroupWise Windows client.

- ♦ [Section 90.1, “Configuring the GWIA for Spam Protection,” on page 1145](#)
- ♦ [Section 90.2, “Configuring the GroupWise Client for Spam Protection,” on page 1145](#)

See also [Part XVIII, “Security Policies,” on page 1149](#).

90.1 Configuring the GWIA for Spam Protection

In ConsoleOne, you can configure the GWIA to reject messages in certain situations:

- ♦ Messages are received from known open relay hosts or spam hosts (GWIA object > *Access Control* > *Blacklists*).
- ♦ Messages are received from any hosts that you specifically do not want to receive messages from (GWIA object > *Access Control* > *Default Class of Service* > *Edit* > *Allow Incoming Messages, Prevent Incoming Messages, and Exceptions*).
- ♦ Messages are received through an anti-spam service that uses an “X” header field to identify potential spam (GWIA object > *SMTP/MIME* > *Settings* > *Junk Mail*).
- ♦ Thirty messages are received within 10 seconds from the same sending host (GWIA object > *SMTP/MIME Settings* > *Security Settings*). The number of message and the time interval can be modified to identify whatever you consider to be a potential mailbomb.
- ♦ Messages are received from SMTP hosts that are not using the AUTH LOGIN host authentication method (*/forceinboundauth* startup switch).
- ♦ The sender’s identify cannot be verified (GWIA object > *SMTP/MIME Settings* > *Security Settings*).

For detailed setup instructions on these anti-spam security measures, see [Section 54.2, “Blocking Unwanted Email from the Internet,” on page 798](#).

Messages that are identified as spam by the GWIA are not accepted into your GroupWise system.

90.2 Configuring the GroupWise Client for Spam Protection

The Junk Mail Handling feature (Windows client > *Tools* > *Junk Mail Handling*) provides users with the following options for dealing with unwanted messages that have not been stopped by the GWIA:

- ♦ Individual email addresses or entire Internet domains can be placed on the user’s Block List. Messages from blocked addresses never arrive in the user’s mailbox.

- ♦ Individual email addresses or entire Internet Domains can be placed on the user's Junk List. Messages from these addresses are automatically delivered to the Junk Mail folder in the user's mailbox. The user can configure automatic deletion of items in the Junk Mail folder and can also create rules to act on items placed in the Junk Mail folder.
- ♦ Messages from users whose addresses are not in the user's personal address books can be automatically delivered to the Junk Mail folder.

The Junk Mail Handling feature in the GroupWise Windows client is enabled by default, although you can control its functionality in ConsoleOne (Domain, Post Office, or User object > *Tools* > *GroupWise Utilities* > *Client Options* > *Environment* > *Junk Mail*).

For detailed usage instructions for the Junk Mail Handling feature in the GroupWise client, see "[Handling Unwanted Email \(Spam\)](#)" in "[Email](#)" in the *GroupWise 2012 Windows Client User Guide*.

NOTE: The Junk Mail Handling feature is not available in WebAccess.

91 Virus Protection

Virus protection for your GroupWise system is provided by third-party products. For information about security products for use with your GroupWise system, see the [Novell Partner Product Guide](http://www.novell.com/partnerguid/) (<http://www.novell.com/partnerguid/>) and the [Novell Open Enterprise Server Partner Support site](http://www.novell.com/products/openenterpriseserver/partners) (<http://www.novell.com/products/openenterpriseserver/partners>).

See also [Part XVIII, "Security Policies,"](#) on page 1149.

XVI Security Policies

- ♦ Chapter 92, “Securing GroupWise Data,” on page 1151
- ♦ Chapter 93, “Securing GroupWise Agents,” on page 1153
- ♦ Chapter 94, “Securing GroupWise System Access,” on page 1155
- ♦ Chapter 95, “Secure Migrations,” on page 1157
- ♦ Chapter 96, “Undocumented Diagnostic Tools,” on page 1159

See also Part XVII, “Security Administration,” on page 1095.

For additional assistance in managing your GroupWise system, see [GroupWise Best Practices \(http://wiki.novell.com/index.php/GroupWise\)](http://wiki.novell.com/index.php/GroupWise).

92 Securing GroupWise Data

- ♦ [Section 92.1, “Limiting Physical Access to GroupWise Servers,” on page 1151](#)
- ♦ [Section 92.2, “Securing File System Access,” on page 1151](#)
- ♦ [Section 92.3, “Securing Domains and Post Offices,” on page 1151](#)

92.1 Limiting Physical Access to GroupWise Servers

Servers where GroupWise data resides should be kept physically secure, where unauthorized persons cannot gain access to the server consoles.

92.2 Securing File System Access

In ConsoleOne, Server objects for servers where GroupWise domains, post offices, and agents reside should be assigned appropriate trustees and rights to prevent access from unauthorized persons.

For additional data security, encrypted file systems should be used on servers where GroupWise domains, post offices, and agents reside. Only GroupWise administrators should have direct access to GroupWise data.

92.3 Securing Domains and Post Offices

In ConsoleOne, administrators in addition to the Admin user should be given rights judiciously, as described in [Chapter 87, “GroupWise Administrator Rights,” on page 1127](#).

The POA should be configured for client/server access, so that GroupWise users do not require any direct access to any databases in the post office. For more information, see [Section 36.2.1, “Using Client/Server Access to the Post Office,” on page 494](#).

93 Securing GroupWise Agents

- ♦ [Section 93.1, “Setting Up SSL Connections,” on page 1153](#)
- ♦ [Section 93.2, “Protecting Agent Web Consoles,” on page 1153](#)
- ♦ [Section 93.3, “Protecting Agent Startup and Configuration Files,” on page 1153](#)
- ♦ [Section 93.4, “Protecting Agent and Application Log Files,” on page 1154](#)
- ♦ [Section 93.5, “Protecting Agent Processes on Linux,” on page 1154](#)
- ♦ [Section 93.6, “Protecting Trusted Applications,” on page 1154](#)

93.1 Setting Up SSL Connections

All of the GroupWise agents should be configured to use SSL connections, as described in:

- ♦ [“Securing the Post Office with SSL Connections to the POA” on page 508](#)
- ♦ [“Securing the Domain with SSL Connections to the MTA” on page 643](#)
- ♦ [Section 48.2.3, “Securing Document Conversion with SSL Connections,” on page 721](#)
- ♦ [“Securing GWIA Connections with SSL” on page 812](#)
- ♦ [“Configuring Authentication and Intruder Lockout for the Monitor Web Console” on page 964](#)

93.2 Protecting Agent Web Consoles

If you do not provide passwords on the GroupWise agent Web consoles, unauthorized persons can access them by simply knowing the IP address or hostname of the machine where the agent runs, along with the HTTP port the agent is using. Set up GroupWise agent Web consoles with passwords as described in:

- ♦ [“Using the POA Web Console” on page 539](#)
- ♦ [“Using the MTA Web Console” on page 669](#)
- ♦ [Section 49.2, “Using the DVA Web Console,” on page 725](#)
- ♦ [“Using the GWIA Web Console” on page 827](#)
- ♦ [“Configuring Authentication and Intruder Lockout for the Monitor Web Console” on page 964](#)

93.3 Protecting Agent Startup and Configuration Files

The startup and configuration files for all GroupWise agents should be protected from tampering. See the following sections for the default locations of the agent startup and configuration files:

- ♦ [Chapter 40, “Using POA Startup Switches,” on page 581](#)
- ♦ [Chapter 45, “Using MTA Startup Switches,” on page 693](#)

- ♦ [Chapter 51, “Using Document Viewer Agent Startup Switches,”](#) on page 731
- ♦ [Chapter 59, “Using GWIA Startup Switches,”](#) on page 851
- ♦ [Chapter 73, “Using Monitor Agent Startup Switches,”](#) on page 1003

93.4 Protecting Agent and Application Log Files

The log files for all GroupWise agents and Web applications should be protected against access by unauthorized persons. Some contain very detailed information about your GroupWise system and GroupWise users. See the following sections for the default locations of the agent and application log files:

- ♦ [Section 37.3, “Using POA Log Files,”](#) on page 551
- ♦ [Section 43.3, “Using MTA Log Files,”](#) on page 677
- ♦ [Section 49.3, “Using DVA Log Files,”](#) on page 727
- ♦ [Section 56.6, “Using GWIA Log Files,”](#) on page 833
- ♦ [Section 63.2, “Using WebAccess Application Log Files,”](#) on page 918
- ♦ [Section 65.2, “Using Calendar Publishing Host Log Files,”](#) on page 932
- ♦ [Section 69.9, “Configuring Monitor Agent Log Settings,”](#) on page 965
- ♦ [Section 70.5, “Configuring Monitor Application Log Settings,”](#) on page 971

93.5 Protecting Agent Processes on Linux

On Linux, the GroupWise agents are installed to run as the `root` user by default. This is not a secure configuration. Immediately after installation, you should set up a non-root user for the agents to run as, as described in [“Running the Linux GroupWise Agents as a Non-root User”](#) in [“Installing GroupWise Agents”](#) in the *GroupWise 2012 Installation Guide*.

93.6 Protecting Trusted Applications

Trusted applications are third-party programs that can log in to POAs and GWIAs in order to access GroupWise mailboxes. For background information, see [Section 4.12, “Trusted Applications,”](#) on page 90.

Trusted applications log in to GroupWise agents by using trusted application keys that are created when the trusted application is created. It is essential that these keys are protected and not allowed to become public. Steps you can take to protect trusted application keys include:

- ♦ Associating the trusted application key with a single IP address whenever possible
- ♦ Reviewing third-party log files for sensitive data such as the key before sharing them with others
- ♦ Not sharing trusted application keys with others for any reason
- ♦ Removing old keys that are no longer needed

94 Securing GroupWise System Access

- ♦ [Section 94.1, “Using a Proxy Server with Client/Server Access,” on page 1155](#)
- ♦ [Section 94.2, “Using LDAP Authentication for GroupWise Users,” on page 1155](#)
- ♦ [Section 94.3, “Managing Mailbox Passwords,” on page 1155](#)
- ♦ [Section 94.4, “Enabling Intruder Detection,” on page 1156](#)

94.1 Using a Proxy Server with Client/Server Access

POAs in your GroupWise system should be located behind your firewall. If GroupWise client users want to access their GroupWise mailboxes from outside your firewall using the Windows client, you should set up a proxy server outside your firewall to provide access, as described in [Section 36.3.1, “Securing Client/Server Access through an External Proxy Server,” on page 506](#). GroupWise WebAccess users access their GroupWise mailboxes through their Web browsers, so your Web server handles the access issues for such users.

94.2 Using LDAP Authentication for GroupWise Users

LDAP authentication provides a more secure method of mailbox access than standard GroupWise authentication, which is the default when you set up your GroupWise system. Therefore, you should implement LDAP authentication, as described in [Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 510](#).

On the Post Office object, the LDAP user name that you provide on the Security property page should be granted only browser rights in the eDirectory tree. The password for the LDAP user should be long and randomly generated.

On the LDAP Server object, *Require TLS for All Operations* should be selected on the SSL/TLS Configuration property page. On the LDAP Group object, *Require TLS for Simple Binds with Password* should be selected.

On your LDAP servers, the trusted root certificate file should be write protected so that it cannot be tampered with.

94.3 Managing Mailbox Passwords

GroupWise offers varying levels of password security, as described in [Section 82.1, “Mailbox Passwords,” on page 1099](#). Make sure that you understand the options available to you and that you select the level of password security that is appropriate to your GroupWise system.

94.4 Enabling Intruder Detection

You can configure the POA to lock out a user that provides the wrong mailbox password too many times, as described in [Section 36.3.5, “Enabling Intruder Detection,”](#) on page 516.

95 Secure Migrations

- ♦ [Section 95.1, “GroupWise Server Migration Utility,” on page 1157](#)

95.1 GroupWise Server Migration Utility

During its operation, the GroupWise Server Migration Utility prompts for some restricted-access information. It also modifies critical GroupWise agent startup files. This section explains why.

- ♦ [Section 95.1.1, “Source Server Credentials,” on page 1157](#)
- ♦ [Section 95.1.2, “Destination Server root Password,” on page 1157](#)
- ♦ [Section 95.1.3, “Agent Startup Files,” on page 1158](#)

For more information about the GroupWise Server Migration Utility, see the [GroupWise Server Migration Guide](#).

95.1.1 Source Server Credentials

The Server Migration Utility prompts for a user ID and password that provides read/write access to the NetWare or Windows server so that the Linux server can mount the source server with read/write access.

In addition, the Server Migration Utility needs read/write access to the domain or post office directory that is being migrated. Read/write access enables the Server Migration Utility to copy the contents of the post office directory or domain directory, including the post office database and domain database, so that file locking is respected while the data is being copied. File locking prevents database damage.

95.1.2 Destination Server root Password

The Server Migration Utility prompts for the `root` password so that it can mount the NetWare volume or the Windows share to the Linux file system. It also needs the `root` password in order to communicate with the SSH (secure shell) daemon on the Linux server. The SSH daemon allows `root` access for the utility to install the GroupWise RPMs, to run the programs required for migration locally on the Linux server, and to create and save the Linux agent startup files.

In addition, `root` permissions might be required to write the post office or domain data to the Linux server, depending on where the user decided to locate the post office or domain. After the migration, the user can configure the GroupWise agents to run as a non-`root` user for improved security, as described in [“Running the Linux GroupWise Agents as a Non-root User”](#) in [“Installing GroupWise Agents”](#) in the [GroupWise 2012 Installation Guide](#).

95.1.3 Agent Startup Files

When the Server Migration Utility migrates an agent, the only change it makes to its startup file is to modify the --home switch to point to the new location of the post office or domain on the Linux server. Existing switch settings are retained, except for paths and IP addresses that would be invalid in the new Linux environment.

96 Undocumented Diagnostic Tools

In ConsoleOne, under *Tools > GroupWise Diagnostics*, a set of tools is available for use by Novell support engineers when attempting to diagnose or correct problems in a customer's GroupWise system. These tools are not intended for use by GroupWise customers without supervision. These tools are not documented.

XIX Appendixes

- ♦ [Appendix A, “GroupWise Port Numbers,”](#) on page 1163
- ♦ [Appendix B, “GroupWise URLs,”](#) on page 1177
- ♦ [Appendix C, “Linux Commands, Directories, and Files for GroupWise Administration,”](#) on page 1179
- ♦ [Appendix D, “Documentation Updates,”](#) on page 1185

A GroupWise Port Numbers

- ♦ [Section A.1, “Opening Ports for GroupWise Agents and Applications,” on page 1163](#)
- ♦ [Section A.2, “Protocol Flow Diagram with Port Numbers,” on page 1166](#)
- ♦ [Section A.3, “Post Office Agent Port Numbers,” on page 1167](#)
- ♦ [Section A.4, “Message Transfer Agent Port Numbers,” on page 1169](#)
- ♦ [Section A.5, “Document Viewer Agent Port Numbers,” on page 1170](#)
- ♦ [Section A.6, “Internet Agent Port Numbers,” on page 1170](#)
- ♦ [Section A.7, “WebAccess Application Port Numbers,” on page 1172](#)
- ♦ [Section A.8, “Calendar Publishing Host Port Numbers,” on page 1172](#)
- ♦ [Section A.9, “Monitor Agent Port Number,” on page 1173](#)
- ♦ [Section A.10, “Monitor Application Port Numbers,” on page 1173](#)
- ♦ [Section A.11, “GroupWise High Availability Service Port Number \(Linux Only\),” on page 1173](#)
- ♦ [Section A.12, “Port Numbers for Products Frequently Used with GroupWise,” on page 1174](#)

A.1 Opening Ports for GroupWise Agents and Applications

When you install GroupWise agents or applications on a server where a firewall is enabled, you must make sure that the firewall is configured to allow communication on the ports used by the GroupWise agents and applications on the server.

- ♦ [Section A.1.1, “Opening Ports on OES Linux,” on page 1163](#)
- ♦ [Section A.1.2, “Opening Ports on SLES,” on page 1164](#)
- ♦ [Section A.1.3, “Opening Ports on Windows,” on page 1165](#)

A.1.1 Opening Ports on OES Linux

The following procedure is an example of how to open ports through a firewall on Novell Open Enterprise Server (OES) Linux. The exact procedure for your specific version of OES might be slightly different.

- 1 In YaST, click *Security and Users > Firewall*.
- 2 In the left panel, click *Allowed Services*.

- 3 (Conditional) To open the port for Samba, so that ConsoleOne can access domain and post office directories on this server from a remote server:
 - 3a In the *Service to Allow* drop-down list, click *Samba Server*, then click *Add*.
- 4 (Conditional) To open ports for a Web browser for GroupWise WebAccess or for the agent Web consoles:
 - 4a In the *Service to Allow* drop-down list, select *HTTP Server* (for a non-secure HTTP connection), then click *Add*.
 - 4b In the *Service to Allow* drop-down list, select *HTTPS Server* (for a secure SSL connection), then click *Add*.
- 5 (Conditional) To open ports for the GWIA:
 - 5a In the *Service to Allow* drop-down list, select *IMAP Server* (for a non-secure IMAP connection), then click *Add*.
 - 5b In the *Service to Allow* drop-down list, select *IMAPS Server* (for a secure SSL IMAP connection), then click *Add*.
 - 5c In the *Service to Allow* drop-down list, click *LDAP Server* (for a non-secure LDAP connection), then click *Add*.
 - 5d In the *Service to Allow* drop-down list, click *LDAPS Server* (for a secure LDAP connection), then click *Add*.
 - 5e In the *Service to Allow* drop-down list, click *Mail Server*, then click *Add*.
 - 5f In the *Service to Allow* drop-down list, click *POP3 Server* (for a non-secure POP3 connection) then click *Add*.
 - 5g In the *Service to Allow* drop-down list, click *POP3S Server* (for a secure POP3 connection), then click *Add*.
- 6 (Conditional) To open ports for the other GroupWise agents:
 - 6a Click *Advanced*.
 - 6b In the *TCP Ports* field, list the port numbers, in a space-delimited list, for the GroupWise agents on this server, as provided in [Appendix A, "GroupWise Port Numbers," on page 1163](#).
 - 6c Click *OK*.
- 7 After you have opened all the ports that GroupWise components need to communicate through on this server, click *Next*.
- 8 Review the list of services and ports that you have configured for this server, then click *Accept*.

A.1.2 Opening Ports on SLES

The following procedure is an example of how to open ports through a firewall on SUSE Linux Enterprise Server (SLE). The exact procedure for your specific version of SLES might be slightly different.

- 1 In YaST, click *Security and Users > Firewall*.
- 2 In the left panel, click *Allowed Services*.
- 3 (Conditional) To open ports for Samba, so that ConsoleOne can access domain and post office directories on this server from a remote server:
 - 3a In the *Service to Allow* drop-down list, select *Samba Client*, then click *Add*.
 - 3b In the *Service to Allow* drop-down list, click *Samba Server*, then click *Add*.

- 4 (Conditional) To open ports for a Web browser for GroupWise WebAccess or for the agent Web consoles:
 - 4a In the *Service to Allow* drop-down list, select *HTTP Server* (for a non-secure HTTP connection), then click *Add*.
 - 4b In the *Service to Allow* drop-down list, select *HTTPS Server* (for a secure SSL connection), then click *Add*.
- 5 (Conditional) To open ports for the GroupWise agents and applications:
 - 5a Click *Advanced*.
 - 5b In the *TCP Ports* field, list the port numbers, in a space-delimited list, for the GroupWise agents and applications on this server, as provided in [Appendix A, "GroupWise Port Numbers,"](#) on page 1163.
 - 5c Click *OK*.
- 6 After you have opened all the ports that GroupWise components need to communicate through on this server, click *Next*, then click *Finish*.

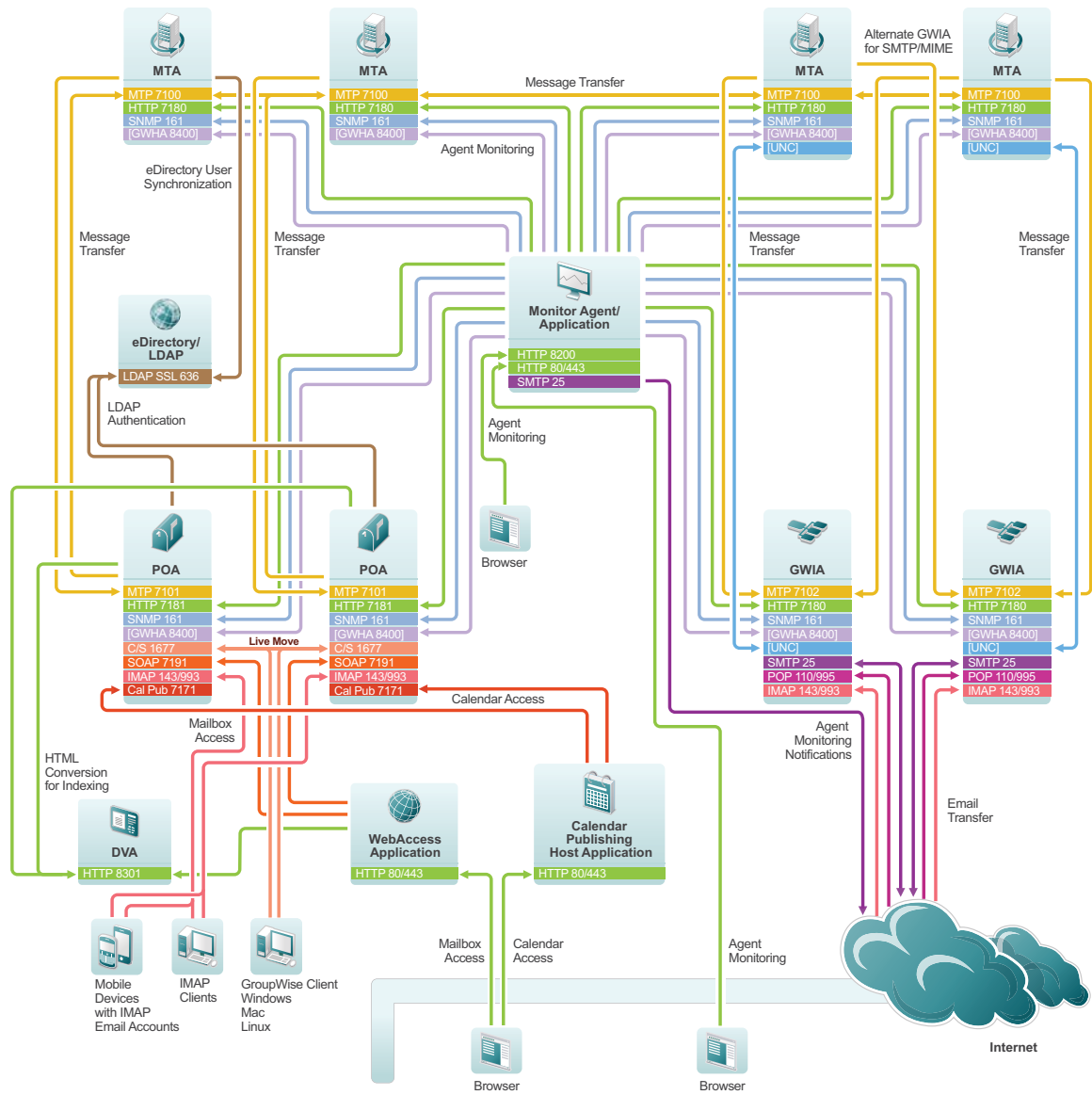
A.1.3 Opening Ports on Windows

The following procedure is an example of how to open ports through a firewall on Windows Server. The exact procedure for your specific version of Windows Server might be slightly different.

- 1 On the *Start* menu, click *Control Panel*, then under *System and Security*, click *Check firewall status*.
- 2 In the left panel, click *Advanced Settings* to open Windows Firewall with Advanced Security.
- 3 In the left panel, click *Inbound Rules*.
- 4 Click *Action > New Rule*.
- 5 Select *Port*, then click *Next*.
- 6 Make sure that *TCP* is selected.
- 7 In the *Specific local ports* field, list the port numbers, in a comma-delimited list, for the GroupWise agents and applications on this server, as provided in this appendix, then click *Next*.
- 8 Accept the default of *Allow the connection*, then click *Next*.
- 9 Accept the default for when the rule applies, or change it depending on your security preferences for the GroupWise agents and applications, then click *Next*.
- 10 In the *Name* field, specify a unique name for this set of port numbers, such as *GroupWise Ports*, then click *Finish*.

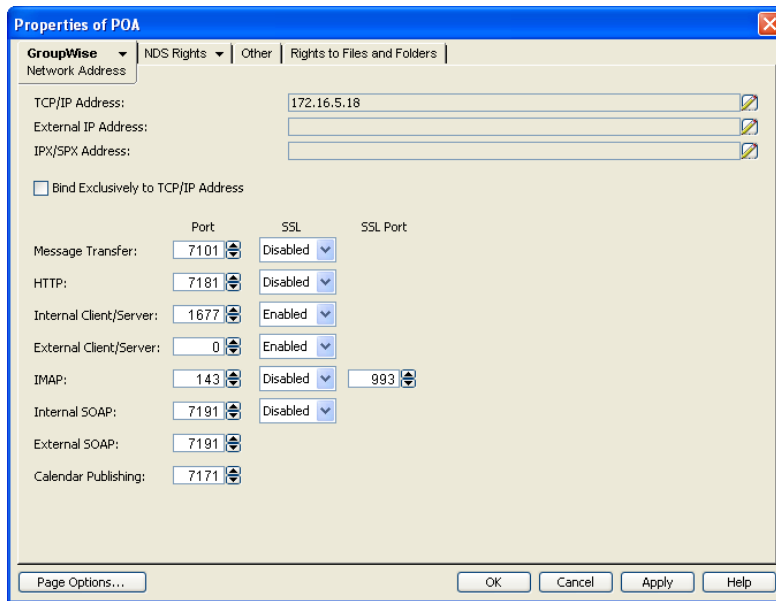
A.2 Protocol Flow Diagram with Port Numbers

[Click here to display a high-resolution, printable version.](#)



See also [Section A.12, "Port Numbers for Products Frequently Used with GroupWise,"](#) on page 1174.

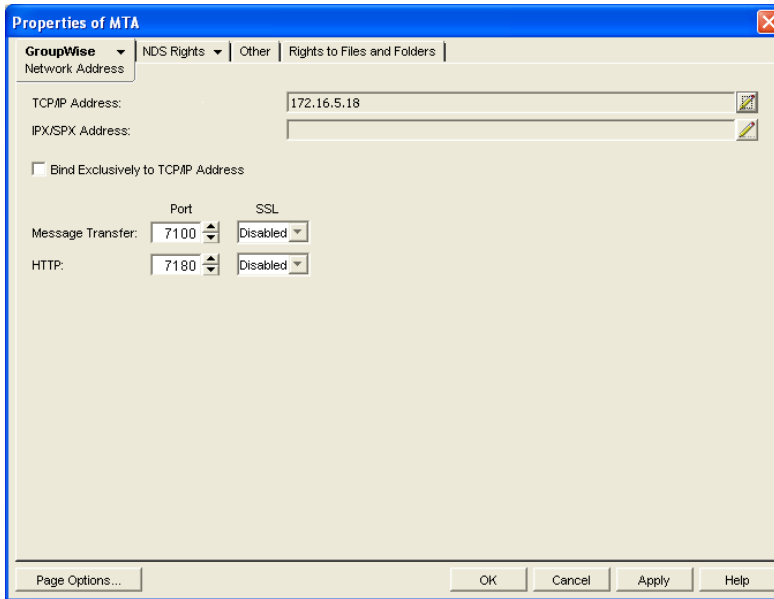
A.3 Post Office Agent Port Numbers



Protocol	Default Port Number	TCP / UDP	SSL Available?	Description
MTP	7101	TCP	Yes	Message Transfer Protocol Communication between the POA and the MTA "Using TCP/IP Links between the Post Office and the Domain" on page 487
HTTP	7181	TCP	Yes	Hypertext Transfer Protocol POA Web console Section 37.2, "Using the POA Web Console," on page 539
Internal Client/Server	1677	TCP / UDP	Yes	Local communication between the POA and GroupWise clients Section 36.2.1, "Using Client/Server Access to the Post Office," on page 494
External Client/Server	0	TCP / UDP	Yes	External communication between the POA and GroupWise clients (administrator-defined port number) Section 36.3.1, "Securing Client/Server Access through an External Proxy Server," on page 506

Protocol	Default Port Number	TCP / UDP	SSL Available?	Description
IMAP	143	TCP	No	Internet Message Access Protocol
IMAP SSL	993	UDP	Yes	<p>Communication between the POA and IMAP clients such as Netscape Mail, Eudora Pro, Microsoft Outlook, and Entourage</p> <p>Section 36.2.3, “Supporting IMAP Clients,” on page 498</p>
SOAP	7191	TCP	Yes	<p>Simple Object Access Protocol</p> <p>Communication between the POA and SOAP clients such as Evolution and the Novell Data Synchronizer Connector for GroupWise</p> <p>Section 36.2.4, “Supporting SOAP Clients,” on page 499</p>
Calendar Publishing	7171	TCP	No	<p>Calendar Publishing Protocol</p> <p>Communication between the POA and the Calendar Publishing Host</p> <p>“Connecting the Calendar Publishing Host to a POA” and Section 64.1.2, “Changing Post Office Settings,” on page 924</p>
SNMP	161	TCP / UDP	No	<p>Simple Network Management Protocol</p> <p>Communication between the POA and an SNMP management console</p> <p>Section 37.6, “Using an SNMP Management Console,” on page 553</p>

A.4 Message Transfer Agent Port Numbers



Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
MTP	7100	TC P	Yes	Message Transfer Protocol Communication between the MTA and the POA "Using TCP/IP Links between Domains" on page 632 and "Using TCP/IP Links between a Domain and its Post Offices" on page 637
HTTP	7180	TC P	Yes	Hypertext Transfer Protocol MTA Web console Section 43.2, "Using the MTA Web Console," on page 669
SNMP	161	TC P/UDP	No	Simple Network Management Protocol Communication between the MTA and an SNMP management console Section 43.6, "Using an SNMP Management Console," on page 679

A.5 Document Viewer Agent Port Numbers

Protocol	Default Port Number	TCP/UDP	SSL Available?	Description
HTTP	8301	TCP	Yes	Hypertext Transfer Protocol Communication between the DVA and the POA or the WebAccess Application Section 49.2, "Using the DVA Web Console," on page 725
HTTP	8302-8306	TCP	Yes	Hypertext Transfer Protocol Default DVA worker threads Section 50.1, "Controlling Thread Usage," on page 729

A.6 Internet Agent Port Numbers

The screenshot shows the 'Properties of GWIA' dialog box with the following settings:

- LDAP: POP3/IMAP4
- Server Directories: Access Control
- Reattach: Post Office Links
- GroupWise: Network Address
- NDS: (empty)
- TCP/IP Address: lbd-nw
- IPX/SPX Address: (empty)
- Bind Exclusively to TCP/IP Address
- Message Transfer: Port 0, SSL Disabled
- HTTP: Port 9850, SSL Disabled
- SMTP: Port 25, SSL Disabled
- POP: Port 110, SSL Disabled, SSL Port 995
- IMAP: Port 143, SSL Disabled, SSL Port 994
- LDAP: Port 389, SSL Disabled, SSL Port 636

Protocol	Default Port Number	TCP/UDP	SSL Available?	Description
MTP	0 or 7102	TCP	Yes	<p>Message Transfer Protocol</p> <p>Communication between the GWIA and the MTA</p> <p>The default port number of 0 (zero) configures a direct connection between the GWIA and the MTA, rather than using TCP/IP. Port number 7102 is an example of an administrator-defined MTP port number for a TCP/IP connection.</p> <p>Section 55.1, "Changing the Link Protocol between the GWIA and the MTA," on page 809</p>
HTTP	9850	TCP	Yes	<p>Hypertext Transfer Protocol</p> <p>GWIA Web console</p> <p>Section 56.2, "Using the GWIA Web Console," on page 827</p>
SMTP	25	TCP/UDP	Yes	<p>Simple Mail Transfer Protocol</p> <p>Communication between the GWIA and email systems across the Internet</p> <p>Section 53.1, "Configuring SMTP/MIME Services," on page 757</p>
POP	110	TCP	Yes	Post Office Protocol
POP SSL	995	UDP		<p>Communication between the GWIA POP email clients</p> <p>Section 53.2, "Configuring POP3/IMAP4 Services," on page 777</p>
IMAP	143	TCP	No	Internet Message Access Protocol
IMAP SSL	993	UDP	Yes	<p>Communication between the GWIA and IMAP clients such as Netscape Mail, Eudora Pro, Microsoft Outlook, and Entourage</p> <p>Section 53.2, "Configuring POP3/IMAP4 Services," on page 777</p>
LDAP	389	TCP	Yes	Lightweight Directory Access Protocol
LDAP SSL	636	P		<p>LDAP server supporting LDAP queries for GroupWise user information contained in the GroupWise Address Book</p> <p>Section 53.3, "Configuring LDAP Services," on page 782</p>

Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
SNMP	161	TC P/UDP	No	Simple Network Management Protocol Communication between the GWIA and an SNMP management console Section 37.6, "Using an SNMP Management Console," on page 553

A.7 WebAccess Application Port Numbers

Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
HTTP	80	TC P	No	Hypertext Transfer Protocol
HTTP SSL	443		Yes	GroupWise WebAccess user interface Section 63.1, "Using the WebAccess Application Web Console," on page 917

A.8 Calendar Publishing Host Port Numbers

Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
HTTP	80	TC P	No	Hypertext Transfer Protocol
HTTP SSL	443		Yes	Calendar Publishing Host user interface Calendar Publishing Quick Start (http://wwwtest.provo.novell.com/documentation/groupwise2012/pdfdoc/gw2012_qs_calpubuser/gw2012_qs_calpubuser.pdf) Calendar Publishing Host administrator interface Section 64.1.1, "Logging In to the Administration Web Console," on page 923

A.9 Monitor Agent Port Number

Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
HTTP	8200	TC P	Yes	Hypertext Transfer Protocol Monitor Agent Web console Chapter 68, "Understanding the Monitor Agent Consoles," on page 941

A.10 Monitor Application Port Numbers

Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
HTTP	80	TC P	No	Hypertext Transfer Protocol
HTTP SSL	443		Yes	Monitor Web console Chapter 68, "Understanding the Monitor Agent Consoles," on page 941

A.11 GroupWise High Availability Service Port Number (Linux Only)

Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
HTTP	8400	TC P	No	Hypertext Transfer Protocol Communication between the Monitor Agent and the GroupWise High Availability service (gwha) (Linux only) "Configuring the Monitor Agent to Communicate with the GroupWise High Availability Service" in "Installing GroupWise Agents" in the <i>GroupWise 2012 Installation Guide</i>

A.12 Port Numbers for Products Frequently Used with GroupWise

- ♦ [Section A.12.1, “Novell Messenger Port Number,”](#) on page 1174
- ♦ [Section A.12.2, “Novell Data Synchronizer Port Numbers,”](#) on page 1174
- ♦ [Section A.12.3, “BlackBerry Enterprise Server for Novell GroupWise Port Number,”](#) on page 1175

A.12.1 Novell Messenger Port Number

Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
HTTP	8300	TC P	No	<p>Hypertext Transfer Protocol</p> <p>Communication between the Messaging Agent and Messenger clients.</p> <p>“Using the Novell Messenger Download Page” in “Managing Messenger Client Users” in the <i>Novell Messenger 2.2 Administration Guide</i></p>

A.12.2 Novell Data Synchronizer Port Numbers

Protocol	Default Port Number	TC P/UDP	SSL Available?	Description
HTTP	8120	TC P	Yes	<p>Hypertext Transfer Protocol</p> <p>Synchronizer Web Admin</p> <p>“Synchronizer Web Admin” in <i>Mobility Pack Administration Guide</i></p>
TCP	4500	TC P	No	<p>Proprietary TCP protocol</p> <p>Communication between the GroupWise Connector and the POA.</p> <p>“GroupWise Post Office Agent” in “Planning a Data Synchronizer System” in the <i>Mobility Pack Installation Guide</i></p>
HTTP	80	TC P	No	Hypertext Transfer Protocol
HTTP SSL	443		Yes	<p>Communication between the Mobility Connector and mobile devices</p> <p>“Mobile Device Port” in “Planning a Data Synchronizer System” in the <i>Mobility Pack Installation Guide</i></p>

A.12.3 BlackBerry Enterprise Server for Novell GroupWise Port Number

Protocol	Default Port Number	TCP/UDP	SSL Available?	Description
TCP	3101	TCP	Yes	Proprietary TCP protocol Communication between BlackBerry Enterprise Server and BlackBerry devices BlackBerry Enterprise Server for Novell GroupWise Administration Guide (http://docs.blackberry.com/en/admin/deliverables/20840/BlackBerry_Enterprise_Server_for_Novell_GroupWise-NO_MAPTITLES_BLOBID-T813841-813841-0921092848-001-5.0.1-US.pdf)

B GroupWise URLs

Administrator URLs

In a URL, an agent server can be specified by its IP address or DNS hostname. The port numbers listed below are the default port numbers.

URL	Web Page
<code>http://poa_server:7181</code>	POA Web Console
<code>http://mta_server:7180</code>	MTA Web Console
<code>http://agent_server:8301</code>	DVA Web Console
<code>http://gwia_server:9850</code>	GWIA Web Console
<code>http://webaccess_server/gw/webacc?action=Admin.Open</code>	WebAccess Application Web Console
<code>http://monitor_server:8200</code>	Monitor Agent Web Console
<code>http://monitor_server/gwmon/gwmonitor</code>	Monitor Web Console
<code>http://calpubhost_server/gwcal/admin</code>	Calendar Publishing Host Admin Web Console

User URLs

URL	Web Page
<code>http://webaccess_server/gw/webacc</code>	WebAccess
<code>http://calpubhost_server/gwcal/calendar</code>	Calendar Publishing
<code>http://calpubhost_server/gwcal/freebusy/ user_id@internet_domain</code>	Free/Busy Publishing

C Linux Commands, Directories, and Files for GroupWise Administration

Some GroupWise administrators might be new to the Linux operating system. This appendix provides basic Linux commands, directories, and files to assist you if are running GroupWise on Linux for the first time.

- ♦ [Section C.1, “Linux Operating System Commands,” on page 1179](#)
- ♦ [Section C.2, “GroupWise Directories and Files on Linux,” on page 1183](#)
- ♦ [Section C.3, “Linux GroupWise Commands,” on page 1184](#)

C.1 Linux Operating System Commands

This section lists Linux commands that can help you manage your GroupWise system on Linux. It also helps you create a Linux core file if you need Support assistance with the Linux GroupWise agents.

- ♦ [Section C.1.1, “Basic Commands,” on page 1179](#)
- ♦ [Section C.1.2, “File and Directory Commands,” on page 1180](#)
- ♦ [Section C.1.3, “Process Commands,” on page 1180](#)
- ♦ [Section C.1.4, “Disk Usage Commands,” on page 1181](#)
- ♦ [Section C.1.5, “Package Commands,” on page 1181](#)
- ♦ [Section C.1.6, “File System Commands,” on page 1181](#)
- ♦ [Section C.1.7, “Network Commands,” on page 1182](#)
- ♦ [Section C.1.8, “Linux Core File,” on page 1182](#)

C.1.1 Basic Commands

The following basic commands are available on Linux:

Command	Description
<code>man <i>command</i></code>	Displays information about any Linux command, including the commands used to start GroupWise programs.
<code>whoami</code>	Displays who you are logged in as.
<code>uname -a</code>	Displays the kernel version, along with other useful information

C.1.2 File and Directory Commands

The following file and directory commands are available on Linux:

Command	Description
<code>pwd</code>	Displays your current directory ("print working directory").
<code>ls -l</code>	Lists the files in the current directory, along with useful information about them.
<code>ls -al</code>	Includes hidden system files (those whose names start with a dot) in the list.
<code>more file_name</code>	Pages through the contents of a file (forward only).
<code>less file_name</code>	Pages through the contents of a file and lets you page back up through the file.
<code>tail file_name</code>	Displays the last 10 lines of a file. This is helpful for log files. (The <code>head</code> command displays the first 10 lines.)
<code>cp source destination</code>	Copies a file or directory.
<code>mv source destination</code>	Moves or renames a file or directory.
<code>find starting_directory -name file_name</code>	Find the specified file, starting in the specified directory. Specifying <code>/</code> starts the find operation in the root directory.
<code>grep string file</code>	Searches the specified file for the specific string of characters. This is useful for locating specific information in GroupWise agent startup files.
<code>mkdir directory_name</code>	Creates a new directory.
<code>rmdir directory_name</code>	Deletes an empty directory.
<code>rm file_name</code>	Deletes a file.
<code>rm -r directory_name</code>	Deletes a directory and recursively deletes its contents.
<code>cat file_name</code>	Displays a file.
<code>cat file_name / printer_device</code>	Prints a file.

C.1.3 Process Commands

The following process commands are available on Linux:

Command	Description
<code>top</code>	Lists all processes, sorted by CPU percentage with the highest at the top of the list.
<code>ps -eaf grep program</code>	Lists all processes and their IDs associated with the specified program. Wildcard characters can be used to list a group of related programs (for example, <code>gw*</code>).
<code>ps -aux grep user_name</code>	Lists all processes and their IDs associated with the specified user.
<code>kill process_ID</code>	Stops the specified process like a normal exit.

Command	Description
<code>kill -9 process_ID</code>	Stops the specified process after it has failed to exit normally. Temporary files are not cleaned up.
<code>killall program</code>	Kills all processes associated with the specified program.
<code>xkill</code>	Closes the window that you click on with the resulting box-shaped cursor.

C.1.4 Disk Usage Commands

The following disk usage commands are available on Linux:

Command	Description
<code>df</code>	Lists file system disk space usage in terms that make sense to your computer.
<code>df -h</code>	Lists file system disk space usage in terms that make sense to humans.
<code>du</code>	Lists disk space usage of each subdirectory below your current working directory
<code>du -s</code>	Lists the cumulative disk space usage of your current working directory.
<code>du -s file_or_directory</code>	Lists the disk space usage for a file or the cumulative disk space usage for a directory and its contents.

C.1.5 Package Commands

The following package commands are available on Linux:

Command	Description
<code>rpm -qa grep novell</code>	Lists all Novell packages installed on your server
<code>rpm -qi package_name</code>	Lists useful information about an installed package, such as name, version, release date, install date, size description, build date, and so on.
<code>rpm -ql package_name</code>	Lists where each file in the package has been installed
<code>rpm -e package_name</code>	Uninstalls a package

C.1.6 File System Commands

The following file system commands are available on Linux:

Command	Description
<code>mount</code>	Lists the file systems that are currently mounted on your server.

Command	Description
<pre>ncpmount -S <i>fully_qualified_hostname</i> -V <i>volume_name</i> -A <i>ip_address</i> -U <i>fully_qualified_admin_user</i> /<i>linux_mount_directory</i></pre>	<p>Mounts a Linux filesystem to a Linux server.</p> <p>For more information, see “Mounting an OES Linux File System Using NetWare Core Protocol (NCP)” on page 42.</p>
<pre>mount -t smbfs //<i>fully_qualified_hostname/windows_share_name</i> /<i>linux_mount_directory</i> -o <i>username=windows_administrator</i></pre>	<p>Mounts a Windows server or Samba share as a file system on your Linux server.</p> <p>For more information, see “Mounting a SLES File System Using Samba” on page 43 or “Making a Windows Server Visible in Linux ConsoleOne” on page 49.</p>
<pre>mount -t cifs //<i>fully_qualified_hostname/windows_share_name</i> /<i>linux_mount_directory</i> -o <i>username=windows_administrator,noserverino</i></pre> <p>The <code>noserverino</code> option uses client-generated inode numbers instead of server-generated inode numbers, which produces a more reliable CIFS mount.</p>	<p>Mounts a Windows server or Samba share as a file system on your Linux server.</p> <p>For more information, see “Mounting a SLES File System Using Samba” on page 43 or “Making a Windows Server Visible in Linux ConsoleOne” on page 49.</p>

C.1.7 Network Commands

The following network commands are available on Linux:

Command	Description
<code>ifconfig -a</code>	Lists the IP address and other detailed information about the NIC in your Linux server.
<code>hostname</code>	Displays the hostname of your server.
<code>dig</code>	Displays host information about your server
<pre>netstat -lnp grep <i>program</i> netstat -lnp egrep '<i>program program ...</i>'</pre>	Lists the port numbers in use by one or more programs. It is also a handy command for checking to see whether the specified programs are currently running.
<code>ping <i>ip_address_or_hostname</i></code>	Checks to see if the specified server is responding on the network.

C.1.8 Linux Core File

A core file is an image of a process such as a GroupWise agent that is created by the Linux operating system when the agent terminates unexpectedly. A proper core file can help Novell Support determine why a GroupWise agent is having problems in your GroupWise system. See TID 3447847, [“How to Obtain a GroupWise Agent Core File on Linux,”](#) in the [Novell Support Knowledgebase](#) (<http://www.novell.com/support>).

C.2 GroupWise Directories and Files on Linux

- [Section C.2.1, “Component Installation Directories on Linux,”](#) on page 1183
- [Section C.2.2, “Linux Agent Software Subdirectories,”](#) on page 1183
- [Section C.2.3, “Linux Agent Startup and Configuration Files,”](#) on page 1183

C.2.1 Component Installation Directories on Linux

GroupWise 2012 Troubleshooting 3: Message Flow and Directory Structure illustrates the following directory structures where software and data are located in a GroupWise system on Linux:

- [“Linux MTA, POA, and DVA Installation Directory”](#) for the GroupWise agents
- [“Linux Internet Agent Installation Directory”](#) for the GWIA
- [“Linux Monitor Agent Installation Directory”](#) for Monitor
- [“Web Application Installation Directories on Your Web Server”](#) for the GroupWise Web applications (WebAccess, Calendar Publishing Host, and Monitor)
- [“Linux Software Distribution Directory”](#)

C.2.2 Linux Agent Software Subdirectories

The following directories contain files common to all Linux GroupWise agents:

Directory	Description
/opt/novell/groupwise/agents/bin	Executables
/opt/novell/groupwise/agents/lib	Libraries
/opt/novell/groupwise/agents/share	Startup files and language files
/etc/init.d	Startup scripts
/etc/opt/novell/groupwise	Configuration files
/var/log/novell/groupwise	Log files

C.2.3 Linux Agent Startup and Configuration Files

The following files are commonly used during GroupWise administration on Linux:

File	Description
/opt/novell/groupwise/agents/share/ post_office.poa	POA startup file
/opt/novell/groupwise/agents/share/ domain.mta	MTA startup file
/opt/novell/groupwise/agents/share/ gwdva.dva	DVA configuration file
/opt/novell/groupwise/agents/share/ gwia.cfg	GWIA configuration file

File	Description
<code>/var/opt/novell/groupwise/webaccess/webacc.cfg</code>	WebAccess Application configuration file
<code>/opt/novell/groupwise/agents/share/monitor.xml</code>	Monitor Agent configuration file
<code>/var/opt/novell/groupwise/monitor/gwmonitor.cfg</code>	Monitor Application configuration file
<code>/etc/xinetd.d/gwha</code>	High Availability service definition file
<code>/etc/opt/novell/groupwise/gwha.conf</code>	High Availability service configuration file for controlling the agents
<code>/etc/opt/novell/groupwise/agents/uid.conf</code>	Non-root user configuration file

C.3 Linux GroupWise Commands

Command	Description
<code>./grpwise start</code> <code>./grpwise stop</code> <code>./grpwise status</code> <code>./grpwise print</code>	Starts/stops/monitors all GroupWise agents as daemons in the <code>/etc/init.d</code> directory.
<code>rcgrpwise start</code> <code>rcgrpwise stop</code> <code>rcgrpwise status</code> <code>rcgrpwise print</code>	Starts/stops/monitors all GroupWise agents as daemons in any directory.
<code>rcgrpwise start</code> <code>post_office.domain</code> <code>rcgrpwise start domain</code> <code>rcgrpwise start gwdva</code> <code>rcgrpwise domain.gwia start</code>	Starts/stops/monitors a specific GroupWise agent as a daemon. Replace <code>start</code> with <code>stop</code> or <code>status</code> in any of the sample commands.
<code>./gwpoa --show</code> <code>@post_office.poa &</code> <code>./gwm^ta --show @domain.mta &</code> <code>./gwia --show @gwia.cfg &</code>	Starts a specific GroupWise agent with a user interface in the <code>/opt/novell/groupwise/agents/bin</code> directory.
<code>./grpwise-ma start</code> <code>./grpwise-ma stop</code> <code>./grpwise-ma status</code>	Starts/stops/monitors the Monitor Agent.
<code>rcgrpwise-ma start</code> <code>rcgrpwise-ma stop</code> <code>rcgrpwise-ma status</code>	The Monitor Agent does not have the same kind of user interface as the other agents. It does have a Web console like the other agents.

D Documentation Updates

This section lists updates to the *GroupWise 2012 Administration Guide* that have been made since the initial release of GroupWise 2012. The information helps you to keep current on documentation updates and, in some cases, software updates (such as a Support Pack release).

The information is grouped according to the date when the *GroupWise 2012 Administration Guide* was republished. Within each dated section, the updates are listed by the names of the main table of contents sections.

The *GroupWise 2012 Administration Guide* has been updated on the following dates:

- ♦ [Section D.1, “April 16, 2013 \(GroupWise 2012 SP2\),” on page 1185](#)
- ♦ [Section D.2, “September 20, 2012 \(GroupWise 2012 SP1\),” on page 1187](#)
- ♦ [Section D.3, “August 18, 2014 \(GroupWise 2012 SP3\),” on page 1189](#)

D.1 April 16, 2013 (GroupWise 2012 SP2)

Location	Change
System	
Section 2.1, “ConsoleOne on Linux,” on page 39	Added steps for manually installing IBM JRE 1.5 and declining installation of the bundled JRE 1.4.2,
“Mounting a Samba Share” on page 45	Added the <code>noserverino</code> option to the CIFS mount command.
“Making a Windows Server Visible in Linux ConsoleOne” on page 49	
Post Offices	
Section 12.4, “Auditing Mailbox License Usage in the Post Office,” on page 207	Clarified that mobile device access by Novell Data Synchronizer requires only a limited client license; clarified that an external entity mailbox requires a full client license.
Users	
Section 14.7.4, “Creating a Nickname for a User,” on page 252	Added that user nicknames are visible in the GroupWise Address Book if you filter for them.
Section 14.10, “Unlocking GroupWise Accounts,” on page 254	Added instructions for unlocking a user account after intruder detection has locked the user out.
Resources	

Location	Change
Section 15.1.2, "Resource Types," on page 265	Added the new role resource.
Section 15.1.4, "Resource Owners," on page 266	Explained how to add a password to a resource mailbox.
Section 16.7.3, "Creating a Nickname for a Resource," on page 276	Added that resource nicknames are visible in the GroupWise Address Book if you filter for them.
Distribution Lists, Groups, and Organizational Roles	
Section 18.9.3, "Creating a Nickname for a Distribution List," on page 297	Added that distribution list nicknames are visible in the GroupWise Address Book if you filter for them.
Post Office Agent	
Section 36.4.1, "Scheduling Database Maintenance," on page 517	Specified the maximum length for scheduled event names and action names.
Message Transfer Agent	
Section 42.2.3, "Enabling Exchange Address Book Synchronization," on page 645	Added a link to the GroupWise/Exchange Coexistence Guide .
Section 42.4.1, "Using eDirectory User Synchronization," on page 652	Specified the maximum length for schedule event names.
WebAccess	
Section 62.2.5, "Controlling WebAccess Usage," on page 909	Improved the instructions for allowing and preventing user access to WebAccess.
Section 62.3.1, "Customizing the WebAccess User Interface with Your Company Logo," on page 911	Clarified that the logo images files should be located under your Web server's document root directory.
Calendar Publishing Host	
Section 64.2.2, "Setting the Published Calendar Auto-Refresh Interval," on page 928	Improved the example of the usefulness of the Auto-Refresh Interval settings.
Client	
"Send Options: Disk Space Management" on page 1059	Clarified that the Limits Apply to Cache option also applies to Remote mailboxes.
Security Administration	
"Linux: Using OpenSSL" on page 1109	Added the <code>-key</code> parameter to the <code>openssl</code> command.

Location	Change
Section 83.2.2, "Generating a Self-Signed Certificate," on page 1111	Updated the reference for the Novell Certificate Server to refer to the Open Enterprise Server documentation.
Appendixes	
Section C.1.6, "File System Commands," on page 1181	Added the <code>noserverino</code> option to the CIFS mount command.

D.2 September 20, 2012 (GroupWise 2012 SP1)

Location	Change
System	
Section 3.3.1, "Changing the Column Display and Order," on page 64	Provided examples of useful information to add to object listings in ConsoleOne.
Section 7.1, "GroupWise User Languages," on page 123	Added Bulgarian and Turkish as fully supported in WebAccess.
Domains	
Section 8.3.1, "Creating the New Domain," on page 139	Added a step for handling the situation where the location for the new domain is on a different machine from where you are running ConsoleOne.
Post Offices	
Section 11.3.1, "Creating the New Post Office," on page 181	Added a step for handling the situation where the location for the new post office is on a different machine from where you are running ConsoleOne.
Section 12.6, "Tracking and Restricting Client Access to the Post Office," on page 209	Provided an example of how to specify the GroupWise 2012 minimum client release version.
Users	
"Creating GroupWise Accounts for eDirectory Users" on page 220	Removed the sections titled "Using a Template to Create GroupWise Accounts" and "Creating GroupWise Accounts by Importing Users." You should no longer use ConsoleOne to create User objects in eDirectory. You should use iManager instead.
"Adding a Global Signature to Users' Messages" on page 231	Clarified the note so that it pertains only to external messages.
Resources	
"Creating Rules for a Resource" on page 269	Added instructions for creating auto-accept/decline rules.
Databases	
"Setting Up a Restore Area" on page 435	Clarified that the name of the restore area directory must follow the same conventions as a post office directory.
Post Office Agent	

Location	Change
"Using an SNMP Management Console" on page 553	Improved the instructions for setting up the POA to work with the SNMP Service on Windows.
"Configuring a Dedicated Client/Server POA (Windows Only)" on page 562, Section 38.2.2, "Configuring a Dedicated Message File Processing POA (Windows Only)," on page 565, Section 38.4.2, "Configuring a Dedicated Database Maintenance POA (Windows Only)," on page 568, and Section 39.5, "Configuring a Dedicated Indexing POA (Windows Only)," on page 577	Clarified that configuring more than one POA is useful only on Windows.
"Enabling the Document Viewer Agent (DVA) for Indexing" on page 576	Clarified the advantages of using the DVA instead of the DCA for indexing.
Message Transfer Agent	
"Using an SNMP Management Console" on page 679	Improved the instructions for setting up the MTA to work with the SNMP Service on Windows.
Document Viewer Agent	
"Windows: Installing Additional DVAs" on page 716	Corrected the instructions for installing the DVA independently on a Windows server.
Internet Agent	
"Using an SNMP Management Console" on page 553	Improved the instructions for setting up the GWIA to work with the SNMP Service on Windows.
"--msstu" on page 867	Clarified that this switch pertains to the sender's address, not the recipients' addresses.
WebAccess	
Section 62.3.1, "Customizing the WebAccess User Interface with Your Company Logo," on page 911	Added instructions for customizing the WebAccess interface for your company logo.
Section 62.3.6, "Enabling an LDAP Address Book," on page 916	Added instructions for enabling an LDAP address book for WebAccess users.
Calendar Publishing Host	
Section 64.2.4, "Configuring an External POA IP Address," on page 929	Corrected the default calendar publishing port number.
Client	
Section 76.2, "Setting Client Options," on page 1030	Clarified how locks work.

Location	Change
Section 77.1, "Using GroupWise AutoUpdate and SetupIP to Distribute the GroupWise Windows Client," on page 1069	Improved the SetupIP instructions.
Security Administration	
"Generating a Certificate Signing Request" on page 1107	Provided alternatives to GWCSRGEN for creating a CSR.
Appendixes	
"User URLs" on page 1177	Added the Calendar Publishing Host free/busy URL.

D.3 August 18, 2014 (GroupWise 2012 SP3)

Location	Change
WebAccess	
Section 63.2.2, "Configuring WebAccess Application Log Settings," on page 918	Added information about proper use of the <code>Log.path</code> entry of <code>webacc.cfg</code> .

