



Administrator's Guide

Release 3.8.3
December 2006
Part Number 010-00452

This manual and Mirapoint software are copyright © 1998-2006 Mirapoint, Inc. All rights reserved. You may not print, copy, reproduce, modify, distribute or display this work in hard copy, electronic, or any other form, in whole or in part, by any electronic, mechanical, or other means, without the prior written consent of Mirapoint, Inc., except that you are permitted to make one copy for archival purposes only in connection with the lawful use and operation of this software. Mirapoint and the Mirapoint logo are registered trademarks of Mirapoint, Inc. RazorGate, Mirapoint Directory Server, Mirapoint Message Director, Mirapoint Message Server, WebCal Direct, and WebMail Direct are trademarks of Mirapoint, Inc.

Portions of this product are Copyright © 1982, 1986, 1989, 1991, 1993 the Regents of the University of California. All Rights Reserved.

Portions of this product are Copyright © 1997, 1998 FreeBSD, Inc. All Rights Reserved.

Portions of this product are Copyright © 1996-1998 Carnegie Mellon University. All Rights Reserved.

Portions of this product are Copyright © 1997-1998 the Apache Group. All Rights Reserved.

Portions of this product are Copyright © 1987-1997 Larry Wall. All Rights Reserved. See <http://www.perl.org>.

Portions of this product Copyright © 1990, 1993-1997 Sleepycat Software. All Rights Reserved.

This software is derived in part from the SSLava™ Toolkit, which is Copyright © 1996-1998 by Phaos Technology Corporation. All Rights Reserved.

Portions of this product are Copyright © 1998-2000 Bruce Verderaime. All Rights Reserved.

Macintosh is a trademark of Apple Computer, Inc.

Legato and NetWorker are trademarks of Legato Systems, Inc.

Windows is a trademark of Microsoft Corporation.

Java and Solaris are trademarks of Sun Microsystems, Inc.

All other trademarks are the property of their respective owners.

OTHER THAN ANY EXPRESS LIMITED WARRANTIES THAT MIRAPOINT PROVIDES TO YOU IN WRITING, MIRAPOINT AND MIRAPOINT'S LICENSORS PROVIDE THE SOFTWARE TO YOU "AS IS" AND EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MIRAPOINT'S LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR OTHER TORT), ARISING IN ANY WAY OUT OF YOUR USE OF THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF DAMAGES. Mirapoint's liability shall be as limited in the License Agreement.

MIRAPOINT, INC. SOFTWARE LICENSE AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT (LICENSE) CAREFULLY BEFORE DOWNLOADING OR OTHERWISE USING THE SOFTWARE. BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, YOU ARE NOT AUTHORIZED TO DOWNLOAD OR USE THIS SOFTWARE.

1. Scope. This License governs your use of any and all computer software, any documentation printed or electronic, or other code, whether on disk, in read only memory, or on any other media (collectively, the “Mirapoint Software”) provided to you as part of or with a Mirapoint Product.

2. License, not Sale, of Mirapoint Software. The Mirapoint Software is licensed, not sold, to you by MIRAPOINT, INC. or its affiliate, if any (“Mirapoint”). YOU MAY OWN THE MEDIA ON WHICH THE MIRAPOINT SOFTWARE IS PROVIDED, BUT MIRAPOINT AND/OR MIRAPOINT’S LICENSOR(S) RETAIN TITLE TO THE MIRAPOINT SOFTWARE. The Mirapoint Software installed on the Mirapoint Product and any copies which this License authorizes you to make are subject to this License.

3. Permitted Uses. This License allows you to use the pre-installed Mirapoint Software exclusively on the Mirapoint Product on which the Mirapoint Software has been installed. With respect to Mirapoint Software [identified by Mirapoint as the “administrative application” that has not been pre-installed on the Mirapoint Product, this License allows you to copy, use and install such Mirapoint Software on one or more administrative workstations on which the Mirapoint Software is supported. You may make one copy of the Mirapoint Software in machine-readable form for backup purposes only, provided that such backup copy must include all copyright and other proprietary information and notices contained on the original.

4. Proprietary Rights; Restrictions on Use. You acknowledge and agree that the Mirapoint Software is copyrighted and contains materials that is protected by copyright, trademark, trade secret and other laws and international treaty provisions relating to proprietary rights. You may not remove, deface or obscure any of Mirapoint’s or its suppliers’ proprietary rights notices on or in the Mirapoint Software or on output generated by the Mirapoint Software. Except as permitted by applicable law and this License, you may not copy, decompile, reverse engineer, disassemble, modify, rent, lease, loan, distribute, assign, transfer, or create derivative works from the Mirapoint Software. Your rights under this License will terminate automatically without notice from Mirapoint if you fail to comply with any term(s) of this License. You acknowledge and agree that any unauthorized use, transfer, sublicensing or disclosure of the Mirapoint Software may cause irreparable injury to Mirapoint, and under such circumstances, Mirapoint shall be entitled to equitable relief, without posting bond or other security, including but not limited to, preliminary and permanent injunctive relief.

5. Disclaimer of Warranty on Mirapoint Software. You expressly acknowledge and agree that use of the Mirapoint Software is at your sole risk. Unless Mirapoint otherwise provides an express warranty with respect to the Mirapoint Software, the Mirapoint Software is provided “AS IS” and without warranty of any kind and Mirapoint and Mirapoint’s licensor(s) (for the purposes of provisions 5 and 6, Mirapoint and Mirapoint’s licensor(s) shall be collectively referred to as “Mirapoint”) EXPRESSLY DISCLAIM ALL WARRANTIES AND/OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

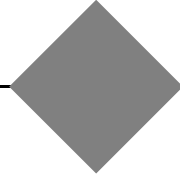
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN ADDITION, MIRAPOINT DOES NOT WARRANT THAT THE MIRAPOINT SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE MIRAPOINT SOFTWARE WILL RUN UNINTERRUPTED OR BE ERROR-FREE, OR THAT DEFECTS IN THE MIRAPOINT SOFTWARE WILL BE CORRECTED. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR OTHER DISCLAIMERS, SO THE ABOVE EXCLUSION OR DISCLAIMERS MAY NOT APPLY TO YOU.

6. Limitation of Liability. UNDER NO CIRCUMSTANCES, INCLUDING NEGLIGENCE, SHALL MIRAPOINT BE LIABLE FOR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THIS LICENSE. FURTHER, IN NO EVENT SHALL MIRAPOINT'S LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE, DATA OR PROFITS OR INTERRUPTION), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING NEGLIGENCE OR OTHER TORT), ARISING IN ANY WAY OUT OF YOUR USE OF THE SOFTWARE OR THIS AGREEMENT, EVEN IF ADVISED OF THE POSSIBILITY OF DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Mirapoint's total liability to you for all damages exceed the amount paid for this License to the Mirapoint Software.

7. Government End Users. If the Mirapoint Software is supplied to the United States Government, the Mirapoint Software and any documentation are provided with RESTRICTED RIGHTS. The Mirapoint Software is classified as "commercial computer software" and the documentation is classified as "commercial computer software documentation" or "commercial items," pursuant to DFAR Section 227.7202 or FAR Section 12.212, as applicable. Any use, modification, reproduction, display or disclosure of the Mirapoint Software or any documentation by the United States Government shall be governed by the terms of this License.

8. Miscellaneous. This License will be governed by and construed in accordance with the laws of the State of California, U.S.A., without reference to its conflict of law principles. If a court of competent jurisdiction finds any provision of this License invalid or unenforceable, that provision will be amended to achieve as nearly as possible the same economic effect as the original provision and the remainder of this License will remain in full force. Failure of a party to enforce any provision of this License shall not waive such provision or of the right to enforce such provision. This License sets forth the entire agreement between the parties with respect to your use of the Mirapoint Software and supersedes all prior or contemporaneous representations or understandings regarding such subject matter. No modification or amendment of this License will be binding unless in writing and signed by an authorized representative of Mirapoint. You will not export, reexport, divert, transfer or disclose, directly or indirectly, the Mirapoint Software, Mirapoint Products or any technical information and materials supplied under this Agreement without complying strictly with the export control laws and all legal requirements in the relevant jurisdiction, including without limitation, obtaining the prior approval of the U.S. Department of Commerce.

Contents



List of Tables	19
List of Figures.....	21
Preface	25
Typographic Conventions	25
About Mirapoint Documentation	26
About this Book.....	27

Part 1 Configuration Tasks

1	
All Deployments Start Here.....	31
Pre-Configuration Checklist.....	31
Prerequisites.....	33
Accessing the Administration Suite	34
Accessing the Command Line Interface (CLI)	37



Initial Setup Common to All Deployments.....	38
Accessing the Setup Wizard	38
Completing the Setup Wizard	39
Checking for Software Updates	46
Restricting Administrator Access	48
Adjusting Administration Security	50
Checking Basic Configurations	50
Completing Your Configuration.....	51
Mirapoint Messaging and LDAP	51
Managing the Cache.....	51
LDAP Binding	51
User LDAP Lookups.....	52
User Login Authentication.....	52
Domain-Based Routing.....	53
Mail Groups Support.....	54
Group Membership ACLs	55
Autoprovisioning User Accounts	55
Setting Up the LDAP Client Queries	56

2

All-In-One Message Server Deployment	63
Before You Begin.....	64
Information Required for this Configuration.....	64
Configuring An All-In-One Message Server	66
Accessing the Administration Suite	67
Checking for Licenses	68
Setting the Administration Timeout.....	68
Configuring Anti-Virus Scanning.....	69
Configuring MailHurdle.....	74
Configuring Anti-Spam Scanning.....	76
Setting Up a User Directory Service	80

Additional Command Line Configuration Tasks	85
Configuring WebMail.....	91
Configuring IMAP	93
Configuring SMTP.....	94
Enabling and Starting Services	96
Resetting the Administration Timeout	97
Verifying the All-In-One Setup.....	98
Refresh the Administration Suite	98
Create a Class Of Service	98
Create User Accounts.....	99
Send a Test Message	100
Receive a Test Message.....	101
Verify the Address Book Directory Service.....	102
Create a Calendar Event	103
Optional Configuration Tasks	103
Adding Networks or Domains to the Reject List.....	103
Setting the HTTP Default Access	104
Configuring Safe Lists and Blocked Lists	105
Troubleshooting.....	105
LDAP Errors.....	105
Test Message Send Fails.....	106
Next Steps.....	107

3

RazorGate Security Deployment for Exchange	109
Before You Begin	110
Information Required for this Configuration	110
Configuring Two RazorGates to Secure Exchange	112
Accessing the Administration Suite	112
Checking for Licenses	113



Setting the Administration Timeout.....	113
Configuring Anti-Virus Scanning.....	114
Configuring MailHurdle.....	119
Configuring Anti-Spam Scanning.....	122
Configuring Inbound Routing—RGs Security Deployment.....	125
Setting SMTP Security Checks and Mail Domains.....	130
Configuring Outbound Routing—RGs Securing Exchange.....	132
Enabling and Starting Services.....	133
Resetting the Administration Timeout.....	134
Verifying the RazorGate Security Setup.....	135
Optional Configuration Options.....	136
Setting Connection Proxies.....	136
Next Steps, RG Security Deployment.....	137

4

RazorGate with Junk Mail Manager Security Deployment for Exchange 139

Before You Begin.....	140
Information Required for this Configuration.....	140
Configuring Two RazorGates with JMM to Secure Exchange.....	145
Accessing the Administration Suite.....	146
Checking for Licenses.....	147
Setting the Administration Timeout.....	147
Configuring Anti-Virus Scanning.....	148
Configuring MailHurdle.....	153
Configuring Anti-Spam Scanning.....	155
Setting SMTP Security Checks.....	159
Configuring Inbound Routing—RGs + JMM Security Deployment .	161
Configuring Outbound Routing.....	169
Enabling and Starting Services.....	170

Resetting the Administration Timeout	171
Verifying the RazorGate with JMM Security Setup	171
Next Steps, RG with JMM Security Deployment	172

5

Multi-Tier, Multi-Appliance Deployment	175
Before You Begin	176
Multi-Tier Terminology	177
Configuring a Multi-Tier Deployment	177
Getting Started.....	178
Security Screening (RazorGate Appliances).....	180
Directory Services for User Data (Mirapoint Appliances).....	188
Routing (RazorGate Appliances)	192
Message Store and Calendar (Mirapoint Appliances).....	195
Reset the Administration Timeout	197

Part 2

Administration Tasks

6

Monitoring Tasks	201
Internal Distribution Lists for Monitoring	201
Viewing Performance At-a-Glance	203
Pie-Chart Categories	204
Using the Performance Gauges.....	205
Mail Graphs	207
POP/IMAP Graphs	209



WebMail Graphs	210
Junk Mail Graphs.....	212
Directory Graphs.....	214
Misc Graphs	217
External Graphs	218
Disk Graphs	221
Network Graphs.....	224
CPU Graphs	226
Using the Message Queue	227
About the Queue	228
What to Look for in the Queue	230
Viewing the Queue Summary	230
Sorting Messages in the Queue	232
Searching the Queue	239
Temporarily Stopping Mail Service.....	241
Deleting the Queue for a Domain	242
Viewing Hardware Status	242
Monitoring Storage	242
Monitoring Hardware Health.....	249
Viewing Alerts	250
Viewing User and/or Administrator Activity	251
Using the User Audit Trail	251
Using the Admin Audit Trail	252
Monitoring External Systems via SNMP.....	253
Configuring SNMP Monitoring.....	253
Adding SNMP Hosts	254
Adding SNMP Traps	255

7

Provisioning Tasks 257

Managing Delegated Domains	258
Adding Delegated Domains	260
Creating an Administrator for a Delegated Domain.....	263
Adding Delegated Domain Administrators to the Postmaster DL ...	264
Finding a Delegated Domain.....	265
Selecting a Domain	265
Editing Delegated Domains.....	267
Configuring Calendar Options for Domains	274
Adding Directory Services to Delegated Domains	286
Deleting Delegated Domains.....	288
Managing User Accounts	288
About Users and Administrators.....	289
User Account Requirements.....	290
Adding Users	292
Finding a User.....	296
Editing Users.....	296
Deleting Users.....	297
Viewing Presence/Last Login Times	297
Establishing User Account Policies.....	298
Bulk Provisioning Users	298
Managing Folders	300
Folder Naming Conventions.....	300
Folder Access Control Lists.....	301
Finding/Viewing Folders	302
Adding Folders	303
Changing Folder Access Control.....	305
Changing a Folder Quota	306
Renaming a Folder.....	307
Adding a Sub-folder.....	307



Creating a Shared Folder	307
Deleting a Folder	308
Sending Messages to User Sub-Folders.....	309
Managing Messages.....	309
Sending Messages to Folders.....	309
Managing Distribution Lists	310
Distribution List Naming Conventions	311
Adding and Populating Distribution Lists.....	312
Finding Distribution Lists	315
Editing Distribution Lists.....	316
Deleting Distribution Lists.....	316

8

Policy Tasks	317
Managing Classes of Service	317
Class of Service Features and Configuration Options	318
Enabling COS.....	321
Adding and Populating a Class of Service	321
Assigning Classes of Service.....	322
Finding Classes of Service	323
Editing Classes of Service.....	324
Deleting Classes of Service.....	324
Managing Storage Policies	324
Creating Storage Policies	326
Editing Storage Policies.....	329
Deleting Storage Policies.....	330
Managing Content Policies (Domain Filters).....	332
Content Filtering Options.....	332
Understanding Quarantine Management	337
Creating a Message Filter	339

Reordering a List of Filters	346
Attaching a Signature to All Messages From a Domain	348
Using Wire Taps	349
Using Word List Filters	351
Filter Examples	374

9

Security Tasks	379
Using Security Features	379
Network Security	380
Inbound Message Handling	382
Message Content Handling	384
Outbound Message Handling	386
Working with MailHurdle	388
Modifying MailHurdle	389
Adding and Deleting MailHurdle Allowed Hosts.....	392
Setting Advanced MailHurdle Configuration Options	392
Using Antivirus Scanning	396
About the Anti-Virus Engines	397
About Cleanable vs. Non-cleanable Viruses.....	398
How Antivirus Quarantine Works.....	398
Modifying Signature-based Anti-Virus.....	399
Setting Notifications for Sophos and F-Secure Anti-Virus	401
Scheduling Updates for Sophos and F-Secure Anti-Virus.....	406
Modifying Predictive-based (RAPID) Anti-Virus.....	409
Setting Notifications for RAPID Anti-Virus	412
Scheduling Updates for RAPID Anti-Virus.....	413
Using Antispam Scanning.....	416
Anti-Spam Scanning Options	417
Modifying Anti-Spam Scanning	419
Scheduling Updates for Anti-Spam Scanning.....	422



Setting the Allowed Senders List	425
Setting the Blocked Senders List.....	428
Setting the Allowed Mailing Lists List	431
Updating Relay Domains (Relay List).....	434
Updating Blocked Domains (Reject List)	435
Updating Your Realtime Blackhole List (RBL)	437
Configuring NIC Failover	439
Using Security Quarantine	441
Assigning the Quarantine Administrator Role	441

10

Using Junk Mail Manager (JMM)	443
About Junk Mail Manager.....	443
How Junk Mail Manager Quarantine Works	445
Junk Mail Manager LDAP Records	446
Modifying Junk Mail Manager	447
Administering Junk Mail Domains	450
Adding Junk Mail Domains.....	451
Selecting a Junk Mail Domain	452
Deleting Junk Mail Domains	452
Managing Junk Mail Domain Accounts.....	452
About Junk Mail Accounts for Distribution Lists	453
Adding Junk Mail Domain Accounts.....	454
Editing Junk Mail Domain Accounts	455
Deleting Junk Mail Domain Accounts	456
Setting Up Junk Mail Manager Content Filtering.....	456
Setting the JMM Allowed Senders List	456
Setting the JMM Blocked Senders List	456
Setting the JMM Allowed Mailing Lists List.....	457
Creating JMM Message Filters	457

Setting JMM Notification Messages.....	457
Setting the JMM Welcome Message.....	458
Setting the JMM Over-Quota Message	459
Bulk Account Provisioning for JMM.....	461
Bulk Creating JMM Accounts.....	462

11

Using the Operations Console	465
Managing Operations Console Groups	466
Adding, Editing, and Deleting Groups	468
Administering Groups.....	469
Synchronizing Groups.....	471
Importing and Exporting Groups.....	471
Using the Operations Console Dashboard.....	472
Using Operations Console Alerts	474

12

Using Logs and Reports	475
Receiving Daily and Weekly Reports	475
Time Strings.....	476
Daily Reports.....	476
Weekly Reports	478
Logs/Reports Overview.....	493
Abbreviations Used in Logs	494
Mail Reports.....	495
Top (Mail Users).....	496
Summary (Logins).....	497
Local (Mail Users)	498
Remote (Mail Users)	499

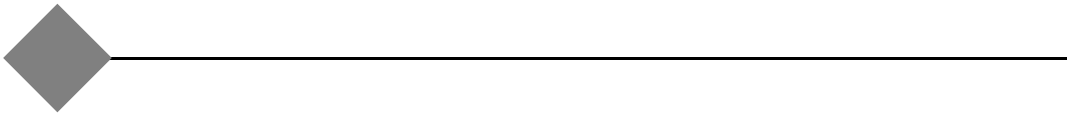


Traffic Summary.....	500
Detailed (Mail Logs).....	501
Search.....	504
Logins Reports.....	505
Top (Logins).....	505
Traffic Rates (Logins)	506
Detailed (Logins)	507
Failed by User (Logins)	508
Failed by IP (Logins).....	508
Security Reports.....	509
Anti-Virus Reports	509
Anti-Spam Reports	511
Content Filtering Reports	512
MailHurdle Reports	513
System Reports	515
Command Report	515
Folders Report	516
Folder Size & Quota Information.....	517
Largest 50 Folders	517
Top 50 Folders Nearest Quota	517

13

Backup and Restore Tasks	519
Mirapoint Backup Solutions	520
About NDMP Backup	520
About Administration Protocol Backup.....	523
Backup and Restore Concepts.....	524
Backup Schemes	524
About Tape Drives and Tape Libraries	527
Backup Protocols.....	527

Using NDMP for Backup	528
Setting Up the NDMP Service	529
Configuring Your DMA	529
Restoring Data with NDMP	529
Using the Administration Protocol for Backup.....	530
Using the Administration Protocol with a Local Storage Device	531
Using the Administration Protocol with RMT	534
Index.....	539



List of Tables

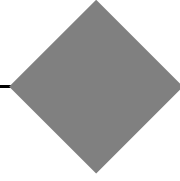


Table 1	Typographic Conventions.....	25
Table 2	Books and Online Help for Mirapoint Appliances.....	26
Table 3	Administration Suite Interface Options.....	34
Table 4	Mirapoint Supported Browsers.....	35
Table 5	Query Specifications for LDAP Client Queries	57
Table 6	Query Specifications and LDAP Attribute Mapping	58
Table 7	Filter Variable Values	60
Table 8	Filter Logical Operators.....	61
Table 9	Differences in Setup of MailHurdle Server and JMM Server	144
Table 10	Settings for Domain, JMM Host, and Mailhost.....	166
Table 11	Default Mirapoint Distribution Lists	202
Table 12	Mail Traffic Graphs (see Figure 10).....	208
Table 13	POP/IMAP Activity Graphs (see Figure 11)	209
Table 14	WebMail Activity Graphs (see Figure 12).....	211
Table 15	Junkmail Statistics Graphs (see Figure 13).....	213
Table 16	LDAP Directory Statistics Graphs (see Figure 14).....	215
Table 17	Miscellaneous Services Graphs	217
Table 18	External Server Monitoring Graphs (see Figure 15).....	220
Table 19	Disk Usage Information Graphs (see Figure 16).....	222
Table 20	Network Traffic Graphs (see Figure 18)	225
Table 21	CPU Activity Graphs	227
Table 22	Boolean Operators.....	241
Table 23	Disk View Properties Data Box Items (see Figure 24)	245
Table 24	Array View Properties Data Box Items (see Figure 24)	246
Table 25	Store View Properties Data Box Items (see Figure 24)	248
Table 26	Admin Audit Trail Report	253

Table 27	Access Control Permissions	302
Table 28	Dashboard Status Colors.....	473
Table 29	Report Fields	479
Table 30	Time-Based Report Fields.....	489
Table 31	Abbreviations Used in Logs	494
Table 32	Top Mail Users Report.....	496
Table 33	Local Mail Traffic Report	498
Table 34	Remote Mail Traffic Reports.....	499
Table 35	Number-and-Rate Summary.....	500
Table 36	Message-Size Summary.....	501
Table 37	Number-of-Recipients Summary	501
Table 38	Detailed Mail Logs	502
Table 39	Filtering Event Codes	503
Table 40	Top Logins By User	505
Table 41	Login Traffic Rates.....	506
Table 42	Detailed Login Report	507
Table 43	Failed Logins By User	508
Table 44	Virus Scanning Summary Report.....	510
Table 45	Detailed Virus Scanning Information Report.....	511
Table 46	Anti-Spam Information Report.....	512
Table 47	Content Filtering Statistics Report	512
Table 48	MailHurdle Host Summary	513
Table 49	MailHurdle To Address Summary	514
Table 50	MailHurdle From Address Summary	514
Table 51	System Information Report	515
Table 52	Command Report.....	516
Table 53	Folder Size & Quota Information.....	517
Table 54	What Gets Backed Up—Image-Based vs. Message-Based.....	525

List of Figures

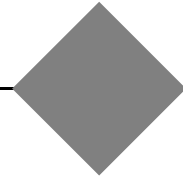


Figure 1	DIT Hierarchical Setup.....	59
Figure 2	All-in-One Deployment Example.....	63
Figure 3	RazorGates Security Deployment Scenario	109
Figure 4	RazorGate with JMM Security Deployment for Exchange.....	139
Figure 5	Example Pseudo-host DNS Records	142
Figure 6	Trusted Host Relationships In A Multi-Tier Environment	167
Figure 7	Multi-tier Deployment Example	175
Figure 8	Trusted Host Relationships In A Multi-Tier Environment	187
Figure 9	Performance Graphs: Gauges.....	206
Figure 10	Mail Performance Graphs.....	207
Figure 11	POP/IMAP Performance Graphs.....	209
Figure 12	WebMail Performance Graphs	211
Figure 13	Junkmail Performance Graphs, Detail	212
Figure 14	Directory Performance Graphs	215
Figure 15	External Performance Graphs (Detail)	219
Figure 16	Disk Performance Graphs.....	221
Figure 17	Disk Pie Charts.....	223
Figure 18	Network Performance Graphs Detail.....	224
Figure 19	Network Traffic Pie Charts	225
Figure 20	CPU Performance Graphs Detail	226
Figure 21	Queue Summary Page.....	231
Figure 22	Queue Sort Page	233
Figure 23	Queue Search Page	239
Figure 24	Monitoring > Storage Page Disk View	243
Figure 25	Monitoring IDE Storage	243
Figure 26	Monitoring > Storage Page Disk View Properties Box Detail.....	244

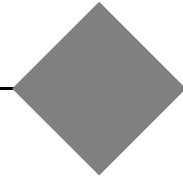
Figure 27	Monitoring > Storage Page Array View Properties Box Detail...	246
Figure 28	Monitoring > Storage Page Store View Properties Box Detail....	248
Figure 29	Monitoring > Health Monitor Page.....	249
Figure 30	Monitoring > Alerts Page	251
Figure 31	Primary Domain and Delegated Domains.....	259
Figure 32	Domains > Administer Domains Page, Add a Domain	261
Figure 33	Domains > Administer Domains Page, Select a Domain	266
Figure 34	Delegated Domains Folders Page.....	269
Figure 35	Delegated Domains Distribution List Page	270
Figure 36	Domains > Signature Page	271
Figure 37	Domains > Over-Quota Message Page	272
Figure 38	Domains > Calendar > Main Configuration Page	277
Figure 39	Domains > Calendar > Search Configuration Page	279
Figure 40	Domains > Calendar > Resources Page.....	281
Figure 41	Domains > Calendar > Subscribed Page.....	284
Figure 42	Mirapoint Add User Page.....	293
Figure 43	Mirapoint Add User Page, Deleted non-LDAP User	297
Figure 44	Mirapoint Folders Page—Find Folder Search Result.....	303
Figure 45	Mirapoint Folders Page—Collapsed View	304
Figure 46	Mirapoint Folders Page—Expanded View	305
Figure 47	Example of Distribution List Named Sales	311
Figure 48	Add Distribution List Page	313
Figure 49	Edit Distribution List Page	314
Figure 50	Class of Service Edit Page.....	320
Figure 51	Domains > Administer Domains Page, Domain Quotas	325
Figure 52	Mirapoint Add User Page, Quota and COS Included	326
Figure 53	Destination Domain Filter Options	332
Figure 54	Example Message Source, MIME Type Indicated.....	335
Figure 55	Advanced Content Filters Page, Add Filter	339
Figure 56	Add/Edit Advanced Content Filter Page	340
Figure 57	Advanced Content Filters Page, Reordering Filters	347
Figure 58	Content Filtering > Wire Tap Page	349
Figure 59	Word List Editor for Word List Content Filters.....	353
Figure 60	Content Filtering > Blocked Addresses Page	356
Figure 61	Content Filtering > Blocked Messages Page	359
Figure 62	Content Filtering > Blocked Attachments Page	362
Figure 63	Content Filtering > Redirected Attachments Page.....	365

Figure 64	Content Filtering > Corporate Word List Page	368
Figure 65	Content Filtering > Objectionable Word List Page.....	371
Figure 66	Network Security Layer	380
Figure 67	Inbound Traffic Handling Layer	382
Figure 68	Message Content Control	384
Figure 69	Outbound Message Control Layer.....	386
Figure 70	MailHurdle Processing for Inbound Messages	389
Figure 71	MailHurdle Configuration Page	390
Figure 72	MailHurdle Allowed Hosts Page	392
Figure 73	MailHurdle Advanced Page, Detail.....	393
Figure 74	MailHurdle Check for Message Advanced Page Detail	395
Figure 75	MailHurdle Flush Triplets Advanced Page Detail	396
Figure 76	Anti-Virus Signature Engine Configuration Page	400
Figure 77	Anti-Virus Signature Engine Notifications Page	402
Figure 78	Anti-Virus SENDER Message, Notification Page Detail	403
Figure 79	Anti-Virus SUMMARY Message, Notification Page Detail	403
Figure 80	Anti-Virus DELETED Message, Notification Page Detail	404
Figure 81	Anti-Virus Signature Engine Updates Page.....	407
Figure 82	Anti-Virus Predictive Engine (RAPID) Configuration Page	410
Figure 83	Anti-Virus Predictive Engine (RAPID) Notifications Page.....	412
Figure 84	Anti-Virus Predictive Engine (RAPID) Updates Page	414
Figure 85	Anti-Spam Configuration Page Detail.....	418
Figure 86	Anti-Spam Configuration Page Detail, Options	420
Figure 87	Anti-Spam Updates Page.....	423
Figure 88	Anti-Spam Allowed Senders Page	426
Figure 89	Anti-Spam Blocked Senders Page	429
Figure 90	Anti-Spam Allowed Mailing Lists Page.....	432
Figure 91	Anti-Spam Relay List Page.....	435
Figure 92	Anti-Spam Reject List Page.....	436
Figure 93	Anti-Spam RBL Host Page.....	438
Figure 94	RazorGate Junk Mail Manager > Configuration Page	448
Figure 95	RazorGate Junk Mail Manager Domains Page	451
Figure 96	RazorGate Junk Mail Manager Accounts Page.....	453
Figure 97	RazorGate Junk Mail Manager Welcome Message Page.....	458
Figure 98	RazorGate Junk Mail Manager Over-Quota Message Page	460
Figure 99	RazorGate Junk Mail Manager Bulk Create Accounts Page	461
Figure 100	Mirapoint Operations Console Login Page.....	466



Figure 101 Operations Console Groups Page 467
Figure 102 Operations Console Edit Groups Page..... 468
Figure 103 Operations Console Administer-Home View of Group Master .470
Figure 104 Operations Console Dashboard Page 472
Figure 105 Top Mail Users..... 497
Figure 106 Local Mail Traffic 498
Figure 107 Remote Mail Traffic..... 499

Preface



Welcome to the *Mirapoint Administrator's Guide*. This book is designed to allow system administrators to configure and administer Mirapoint messaging solutions.

Mirapoint appliances can be deployed in many different scenarios, ranging from a single “all-in-one” appliance supporting a single organization to a large number of appliances arranged into a sophisticated multi-tier network supporting a large enterprise or service provider company. Configuration of an individual Mirapoint appliance depends upon understanding its role in a particular deployment scenario.

This book assumes that you are familiar with industry-standard networking concepts and terminology and have a general understanding of how Internet email messaging works. For an overview, see the Wikipedia [E-mail](#) article. Important terms are also defined in the

Typographic Conventions

Table 1 explains what different fonts indicate in this book.

Table 1 Typographic Conventions

Font	Indicates	Example
Roman	Ordinary text	The e-mail server organizes mailboxes hierarchically.

Table 1 Typographic Conventions

Font	Indicates	Example
Bold	Definitions; also screen elements such as menus, commands, and option labels	A folder is a container that stores e-mail messages. Use the Ldap Set command to enable autoprovisioning.
<i>Italic</i>	Emphasis; book titles	Specify <i>at least two</i> DNS servers. See the <i>Mirapoint Administration Protocol Reference</i> for details.
Typewriter	Screen display text; command names	Enter your password:
Typewriter Bold	Text that you type exactly as shown	Sntp Set Sntpauth
<i>Typewriter Italic</i>	Placeholders for variables you provide	<i>sys_IP_address</i>

About Mirapoint Documentation

Table 2 Books and Online Help for Mirapoint Appliances

Document Title	What the Document Describes
<i>Planning Guide</i>	Describes different Mirapoint solutions.
<i>Series 500 Hardware Installation and Maintenance</i>	Describes how to install and maintain the Mirapoint Series 500 hardware.
<i>M5000 Hardware Installation and Maintenance</i>	Describes how to install and maintain the Mirapoint Series 5000 hardware.
<i>M5000S Storage Area Network (SAN) Edition Hardware Installation and Maintenance</i>	Describes how to install and maintain the Mirapoint M5000S hardware. SAN provides fast through-put, large capacity, and integral backup.

Table 2 Books and Online Help for Mirapoint Appliances

Document Title	What the Document Describes
<i>M5000N Network-Attached Storage (NAS) Edition Hardware Installation and Maintenance</i>	Describes how to install and maintain the Mirapoint M5000N hardware. NAS/NFS provides large capacity, reduced cost, and simplified backup.
<i>Administration Suite Online Help</i>	Provides instructions for using the Mirapoint Administration Suite. Access by clicking the Help link in the Administration Suite.
<i>Administration Command-Line Interface Help</i>	Describes the administration command-line interface and syntax for all commands. Access by entering the Help keyword on the Mirapoint command line.
<i>Mirapoint Administration Protocol Reference</i>	Describes the Mirapoint administration protocol. Available from http://support.mirapoint.com .

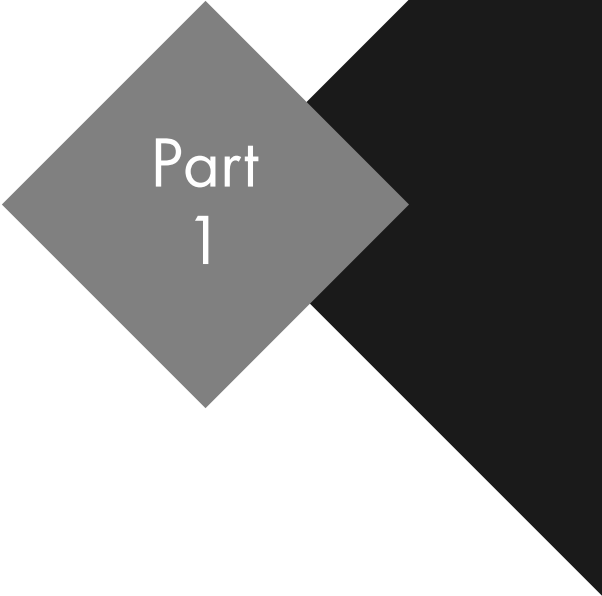
About this Book

This book provides basic configuration tasks in Chapter 1, “All Deployments Start Here,” and a configuration guide for the deployment scenarios described in greater detail in the *Mirapoint Administrator’s Planning Guide*:

- ◆ Chapter 2, “All-In-One Message Server Deployment”: A single Message Server configured to perform routing, directory, security, and storage functions.
- ◆ Chapter 3, “RazorGate Security Deployment for Exchange”: one or more RazorGate appliances providing routing and security functions on behalf of an Exchange server.
- ◆ Chapter 4, “RazorGate with Junk Mail Manager Security Deployment for Exchange”: one or more RazorGate appliances providing routing and security functions on behalf of an Exchange server, and Junk Mail Manager providing the capability of managing unsolicited commercial email.
- ◆ Chapter 5, “Multi-Tier, Multi-Appliance Deployment”: Multiple appliances networked to provide routing, security, storage, directory, and proxy services.



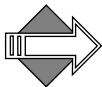
Configuration Tasks



All Deployments Start Here

Mirapoint appliances can be deployed in many different scenarios, ranging from a single, all-in-one appliance that supports an entire organization to a large number of appliances arranged in a sophisticated multi-tier network to support a large enterprise or service provider clients. How you configure an individual Mirapoint appliance depends on understanding its role in the selected deployment scenario.

This chapter describes the configuration steps that need to be performed for all Mirapoint appliances, regardless of the selected deployment scenario. Complete these steps before proceeding to the chapter that describes how to configure appliances for your selected deployment scenario. This chapter also includes a section on “Mirapoint Messaging and LDAP,” that describes how the various Mirapoint routing and proxying subsystems interact with LDAP; this information is provided to help you make your advanced configuration choices in the chapters that follow.



In this document, the term **router** refers to an email router, rather than a network packet router. Third-parties sometimes refer to email routers as relays.

Pre-Configuration Checklist

A number of tasks need to be completed before a Mirapoint appliance can be configured. Some of these tasks might require significant advance planning and preparation, as well as detailed familiarity with your network infrastructure and intended deployment. The checklist below will alert you to some of these larger issues before you begin

configuration. Refer to the *Mirapoint Administrator's Planning Guide* for a complete discussion of these factors.

- ◆ **Domain Name System (DNS)**—Mirapoint appliances do not act as DNS servers, but DNS services must be available on the network for Mirapoint appliances to work correctly. The appropriate DNS records (A, PTR, MX, and CNAME) for your appliance must be entered into the server database used by your appliance.
- ◆ **Lightweight Directory Access Protocol (LDAP)**—Many Mirapoint features require access to an LDAP server for data management. Simple deployments for Mirapoint appliances can use the standard Mirapoint LDAP server. However, more complex systems supporting non-Mirapoint equipment might require the design of a custom LDAP infrastructure. Designing and implementing a custom LDAP infrastructure is a non-trivial undertaking and requires advanced planning.
- ◆ **Licenses**—Many Mirapoint features require a license. Licenses purchased with the appliance are pre-installed and are activated during configuration. Activating licenses is straightforward; make sure that you have all the licenses required for your specific deployment.



If an LDAP-related license expires, the LDAP settings will revert to the default once an updated license is applied. Please monitor your system license expiration dates and backup your system configuration to avoid unplanned downtime.

- ◆ **Backups**—Mirapoint appliances are usually backed up with a third-party client (Veritas NetBackup, Legato NetWorker, Tivoli Storage Manager, or BakBone NetVault) that supports the Network Data Management Protocol (NDMP). Understand your deployment's backup needs before beginning configuration.
- ◆ **Secure Socket Layer (SSL)**—Obtaining SSL digital certificates from a certificate authority such as VeriSign can take hours or days. If you intend to configure your Mirapoint appliance to use SSL, familiarize yourself with the procedure for obtaining one or more certificates. While some steps of the procedure cannot be performed until the appliance is powered up, you can gather the organizational information required by the certificate authority in advance.

- ◆ **Branding**—The look-and-feel of the Mirapoint appliance user interface can be customized to meet your corporate or organizational requirements. Such customization is called *branding*. Configuring a Mirapoint appliance to use an existing brand is straightforward, but the creation and implementation of a brand is a non-trivial effort that can require significant advance preparation.

Prerequisites

Procedures in this chapter apply to both Message Store appliances and RazorGate (security/routing). The remaining sections assume that you have completed the following tasks for your appliance:

- ◆ **Hardware installation**—All hardware must be rack-mounted, cabled, and powered on. See your hardware manual for details.
- ◆ **DNS server database**—The DNS server must be populated with the following DNS records for the appliance:

- ❖ **A record**—Maps the hostname to an IP address (lookup).
Example:

```
Dns Lookup mail.example.com ""  
A 64.124.80.66
```

- ❖ **PTR record**—Maps an IP address to hostname (reverse lookup).
Example:

```
Dns Lookup 64.124.80.66 type=PTR  
PTR mail.example.com
```

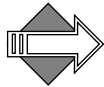
- ❖ **MX record**—Specifies the hostname (not an IP address) of a Message Server; this must be specified for every domain for which the system receives mail. MX records contain a domain name, a preference level (which can be used for load balancing), and a mail machine hostname. Example:

```
Dns Lookup example.com type=MX  
MX 50 mercury.example.com  
MX 20 venus.example.com  
MX 10 mars.example.com
```

- ❖ **CNAME record**—(optional) Maps one name to another name for an address. Sometimes called a *host alias*. Example:

```
Dns Lookup mail.example.com type=CNAME  
CNAME corp.supernews.com
```

- ◆ **Basic system setup**—This is described on the Quick Start card shipped with your appliance. The following information should have been entered into the appliance, either through the LCD and keypad module on the front panel of the appliance, or through a VGA monitor and keyboard attached to the appliance:
 - ❖ Appliance IP address
 - ❖ Appliance netmask
 - ❖ Default router (gateway) IP address
 - ❖ DNS server IP address (primary)
 - ❖ Temporary Administration password



If you ran the Mirapoint Setup Wizard after installing your appliance, you might already have performed some of the tasks described in the following sections. You can omit configuration tasks described below that you have already performed.

Accessing the Administration Suite

The procedures given in this book use the Administration Suite web interface. To access the Administration Suite, you need a web browser that supports tables and forms. Most newer browsers are suitable.

Table 3 lists the various administration interfaces available.

Table 3 Administration Suite Interface Options

URL Suffix	Description
miradmin	Default administration UI for your appliance
madmin	Message Server administration
rgadmin	RazorGate administration
ocadmin	Operations Console interface for multiple appliances

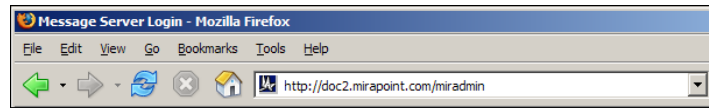
Table 4 Mirapoint Supported Browsers

For Windows systems	<ul style="list-style-type: none"> ❖ Firefox 1.0 and above (Mozilla 1.7 and above) ❖ Netscape Browser 7.1 and above ❖ Microsoft Internet Explorer 6.0 and above
For Macintosh systems	Safari 1.2 and above

To access the Administration Suite, follow these steps.

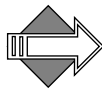
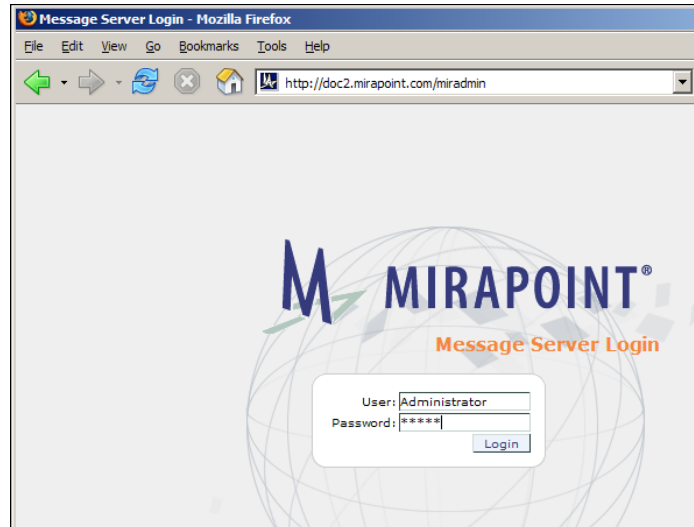
1. Go to this URL, where *miServer* is the IP address or name (if configured in your DNS) of your Mirapoint server.

http://miServer/miradmin



The Administration Suite **Login** page for that server appears. If you try to access an unlicensed interface, an error page results.

2. In the **User** option, enter the login name **Administrator**. In the **Password** option, enter the temporary administration password you specified for the appliance during the hardware setup. Click **Login**.

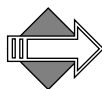


The Administration Suite displays text in UTF-8, an international character set. As a consequence, font changes might result.

The Administration Suite has an idle-timeout that automatically ends sessions that are idle for an extended period of time; by default this timeout is 10 minutes. If your session expires, you need to log back in to the Administration Suite to continue the setup process.

Using the Administration Suite Setup Wizard

The Administration Suite Setup Wizard steps through the basic configuration of a Mirapoint appliance. On a newly installed system, the Administration Suite automatically displays the Setup Wizard. You can access the Setup Wizard at any time at **Home > System > Setup Wizard**.



This chapter describes the Mirapoint Administration Suite Setup Wizard, not the E-Z Setup Wizard that may display with some RazorGate systems. The two Wizards are nearly identical and the procedures here apply to both.

Everything that you can do in the Setup Wizard can also be done with the regular Administration Suite pages. However, Mirapoint

recommends that you configure routing and enable Junk Mail Manager (JMM) using the Setup Wizard before configuring options through the Administration Suite pages.

This chapter describes how to perform the basic configuration of your Mirapoint appliance through the Setup Wizard. You'll also use the Setup Wizard to complete the JMM configuration procedures described in Chapter 4, "RazorGate with Junk Mail Manager Security Deployment for Exchange." Most other procedures in this book describe how to set options through the regular Administration Suite pages.

Accessing the Command Line Interface (CLI)

Some tasks must be done using the command line interface (CLI). To log in to the appliance using the CLI:

1. **Telnet** to port 23 on the Mirapoint appliance. Specify the Mirapoint appliance using the IP address you assigned to it during the hardware setup.
2. Enter the login name **Administrator**.
3. Enter the temporary administration password you specified for the appliance during the hardware setup:

```
OK mail.example.com admin@ 3.8 server ready
User: Administrator
Password:
OK User logged in
mail.example.com>
```

You can now enter additional configuration information for the appliance using the CLI.



The CLI has an extensive online Help system that can be accessed by typing **Help** or **Help About *Commandname***.

Initial Setup Common to All Deployments

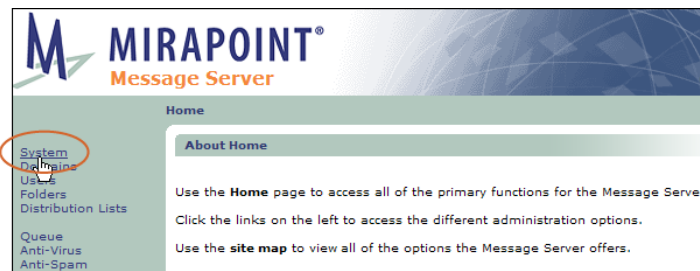
The initial setup of your appliance, regardless of deployment scenario, involves these tasks:

- ◆ Accessing the Setup Wizard
- ◆ Completing the Setup Wizard
- ◆ Checking for Software Updates
- ◆ Restricting Administrator Access
- ◆ Adjusting Administration Security

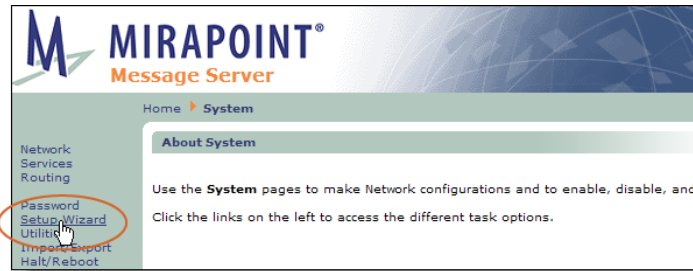
Accessing the Setup Wizard

The Setup Wizard start page is displayed automatically the first time you log into the Administration Suite. On subsequent log-ins, the Setup Wizard can be accessed from **Home > System > Setup Wizard**. If the Setup Wizard does not display, access it by following these steps.

1. Click **System** in the page menu on the left to access the **System** configuration pages.



2. Click **Setup Wizard** to access the Setup Wizard pages.



Completing the Setup Wizard

Step through the setup procedure using the navigation links in the upper-right corner of the Setup Wizard pages. You can navigate between pages in the Setup Wizard with the **Previous** and **Next** links without altering your configuration.

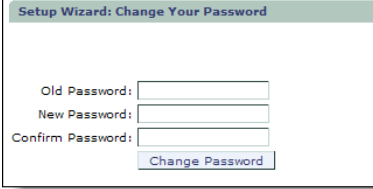


To make changes, you must use the controls on each page to explicitly save your changes or your changes are lost when you go to the next page. For example, to change your password, you must enter your new password information and click the **Change Password** button for the new password to take effect.

1. **Setup Wizard** page. Begin the setup process by clicking **Next** in the upper-right corner.



2. **Change Your Password** page (optional). The new password must be fewer than 80 characters long.



Setup Wizard: Change Your Password

Old Password:

New Password:

Confirm Password:

To change your password:

- a. Specify your current administration password in the **Old Password** option.
- b. Enter and confirm your new password in the **New Password** and **Confirm Password** options. Passwords are case-sensitive and can contain up to 80 characters (letters and numbers).
- c. When you're done, click **Next** to continue.



Good security practice requires an administrator password that cannot be easily guessed, cannot be found in a dictionary, and so forth. Mirapoint recommends a minimum password length of at least ten (10) characters with a mix of uppercase and lowercase characters as well as numbers and punctuation characters.

3. **Set QuarantineAdmin User Account** page. Click **Next** to continue. You can set up quarantine administrators once your system is up and running. For information about quarantining messages and adding quarantine administrators, see “Using Security Quarantine.”
4. **Set Network Identifiers** page. The network settings and DNS server configured during installation are shown on the **Set Network Identifiers** page. Verify that the network settings are correct and configure at least one additional DNS server as a backup. If you are unsure what the appropriate network settings for your appliance are, consult your network administrator.

Setup Wizard: Set Network Identifiers

IP Address: 63.107.133.212
 Netmask: 255.255.255.224
 Host Name: ue1
 Domain Name: explore.mirapoint.ca
 Default Router: 63.107.133.222

Set

Set Domain Name Servers

Specify DNS servers for network identifier lookup.

DNS Server:

Add

1 to 1 of 1 <Prev | Next>

DNS Server
<input type="checkbox"/> 63.107.133.194

Remove



If you change the IP address of the appliance, you lose your connection to the server and must reconnect through the new IP address.

To add a DNS server:

- a. Enter the DNS server's IP address in the DNS Server option.
- b. Click the **Add** button.
- c. When you're done, test your DNS servers or click **Next** to continue.

You can test your DNS server connections from the **Set Network Identifiers** page. Follow these steps.

Test Domain Name Server

The **Lookup** utility allows you to test your Domain Name Servers.

Domain Name/IP: mirapoint.com

ANY

Lookup Clear

Results for: mirapoint.com

```
A: 205.217.153.166
MX: 100 sift.mirapoint.com
MX: 100 sift2.mirapoint.com
NS: ns5.mirapoint.com
NS: ns6.mirapoint.com
NS: ns.meer.net
NS: ns2.meer.net
```

- a. Enter the domain name or IP address of an Internet server such as *mirapoint.com* in the **Domain Name/IP** option.
 - b. Click the **Lookup** button. If the appliance can connect to the DNS server(s), the page refreshes with the results of the lookup.
 - c. When you're done, click **Next** to continue.
5. **Licenses** page. All installed Mirapoint licenses are listed on this page. Verify that all of the licenses listed on your license sheet from Mirapoint are shown on this page. If any of your purchased licenses are **not** listed on this page, install them.

Setup Wizard: License

Your Host ID is **000e0c4b11b8**.
Click **Install Licenses** to retrieve and apply available licenses.

[Install Licenses](#)

License Key:

[Show License Keys](#)

License Name	Expiration Date
System OPERATING	
User-limit 20	
Upgrades Allowed	Dec 22 2008
Mirapoint Antispam SE 100 users	Dec 21 2008
Web-mail 100 users	
POP 100 users	
IMAP 100 users	
Directory Server Access 100 users	
Calendar 100 users	
Group calendar 100 users	
SMTP FastPath	
Sophos virus filtering 100 users	Dec 21 2008
Message Server	

To install licenses click the **Install Licenses** button to retrieve and apply your licenses from the Mirapoint license server.

If your licenses cannot be retrieved, apply them one at a time:

- a. Copy an individual key from your licenses PDF.
- b. Paste the key into the **License key** option.
- c. Click the **Apply** button.
- d. When you're done, click **Next** to continue.

If you are unable to install licenses it is likely because your system is not connected to the Internet or the licenses you want are not available on this server. Licenses are retrieved from a system in the

Mirapoint.com domain. If you have difficulties, contact Mirapoint Technical Support at support-admin@mirapoint.com.

6. **Operations Console vs. Administration Suite** page. This page allows you to designate this appliance as a **Replica** member of a defined Operations Console group. If this is not applicable, click **Next**.
7. **Set System Time** page.

To set the system time and date:

- a. Select your time zone and click the **Set Timezone** button.
- b. Set the current date and time and click the **Set Clock** button.
- c. When you're done, click **Next** to continue.

You can also add NTP servers on this page though this is optional. NTP is a protocol for synchronizing the system clocks of networked computers. If you use NTP, the appliance system clock is automatically kept in sync with the network time servers. To ensure that a time server can be reached for synchronization, specify multiple servers. If you do not have an NTP server of your own, we recommend specifying 0.us.pool.ntp.org, 1.us.pool.ntp.org, 2.us.pool.ntp.org. For more information about NTP, see <http://ntp.org>.



Mirapoint strongly recommends that you use an NTP server to keep your time synchronized. Some facilities, such as Kerberos authentication, require synchronized clocks.

8. **Set Relay List** page. Click **Next** to continue. You do not need to configure any relays at this time.
9. **Set Mail Domains** page. Click **Next** to continue. You do not need to set mail domains at this time.

10. **Routing Via Local Router** page. Click **Next** to continue. You do not need to configure routing options at this time. Routing options are set as part of the deployment-specific configuration procedures. Please note: If you have installed the LDAP Routing license, this page does not display; instead, the **Choose Routing Method** page displays. If the **Choose Routing Method** page displays, click **Next** to continue; you do not need to choose a routing method at this time.
11. **Security** page. Click **Next** to continue. You do not need to modify the default security (antispam and antivirus) options. Please note: If no antispam or antivirus licenses have been installed, this page displays empty.
12. **Service Reporting** page. Configure service reporting to send alerts and weekly reports to selected administrators and Mirapoint Customer Service.

Setup Wizard: Service Reporting

[Previous](#) | [Next](#) | [Close](#)

Service Reporting automatically sends e-mail alerts and weekly reports about your system's health and performance to Mirapoint Customer Service. Alerts and Reports do not reveal the contents of any mail messages.

Make sure the contact information below is up-to-date.

Service Reporting is currently **enabled** on your system. This allows Mirapoint Customer Service to predict and prevent failures. Click **Disable it** to remove customercare@mirapoint.com from the system-alerts and weekly-reports distribution lists.

Service Reporting is currently **enabled**.

Set Contact Information:
This information will be appended to all Alerts and Reports. Use 7-bit ASCII letters for the best results.

Contact Information:

To set your service reporting options:

- a. Make sure service reporting is enabled. If it isn't, click the **Enable It** button to turn on service reporting.
- b. Enter the administrator contact information you want to include in your service reports and click the **Update** button.
- c. Enter the email address of each person who should receive Mirapoint system alerts in the **Alerts Recipients Email Address** option and click the **Add** button. The Administrator user is included in the alert list by default but later, when you create additional administrators, you'll want to add them.

Set Alerts Recipients:
Set the e-mail addresses to receive **alerts** from the system.

E-mail Address:

1 to 1 of 1 <Prev | Next>

Alerts recipients		
<input checked="" type="checkbox"/>	Administrator	<input type="button" value="Remove"/>

- d. Enter the email address of each person who should receive Mirapoint system reports in the **Reports Recipients Email Address** option and click the **Add** button. (The Administrator is included in the report list by default.)

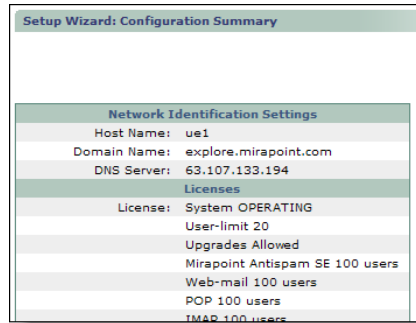
Set Reports Recipients:
Set the e-mail addresses to receive **reports** from the system.

E-mail Address:

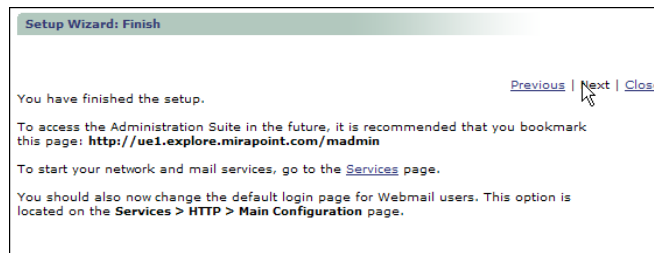
1 to 1 of 1 <Prev | Next>

Reports recipients		
<input checked="" type="checkbox"/>	Administrator	<input type="button" value="Remove"/>

- e. When you're done setting your service reporting options, click **Next** to continue.
13. **Configuration Summary** page. Review the information displayed in the configuration summary. If you need to make any changes, click **Previous** to return to any page, make the changes, and then click **Next** to step back through the Wizard to return to the **Configuration Summary** page. When you're done, click **Next** to complete the setup process.



14. **Finish** page. You are now done entering information in the Setup Wizard. Bookmark the Administration Suite URL that's displayed on this page and then click **Close** to exit the Setup Wizard.



Next, you need to complete the initial setup by doing the following:

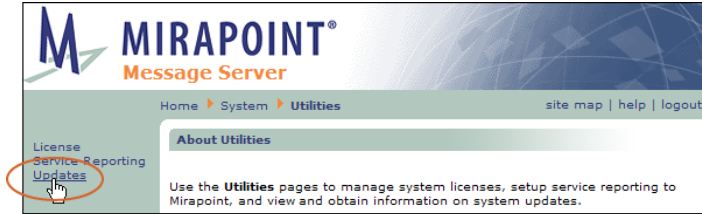
- ◆ Checking for Software Updates
- ◆ Restricting Administrator Access
- ◆ Adjusting Administration Security

Checking for Software Updates

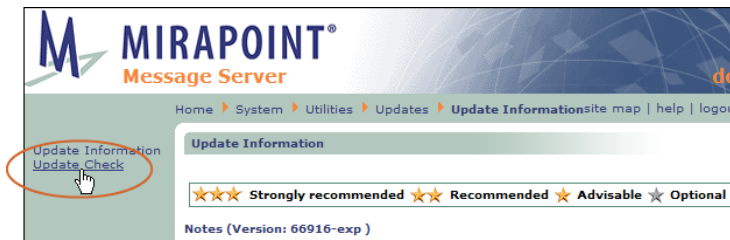
Before you start using your appliance, you need to make sure that you have the latest version of the Messaging Operating System (MOS) installed. Update information is available by logging in to <http://support.mirapoint.com> and going to **Software Center > Current MOS Releases > 3.8 Releases**; you will need a login ID to do this. If you don't have a Mirapoint Support login ID, send an email to

support-admin@mirapoint.com requesting one. To check for updates using the Administration Suite:

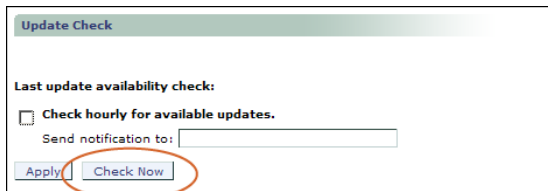
1. Go to **Home > System > Utilities**.
2. Click **Updates** to open the **Update Information** page.



3. Click **Update Check** to go to the **Update Check** page.

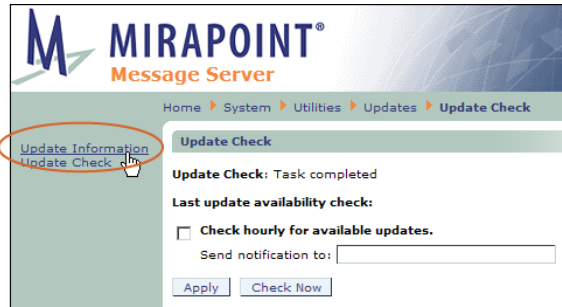


4. Click the **Check Now** button on the **Update Check** page to check for available updates. When the check is complete, the page displays the last machine update date. (**Update Check: Task Completed** is displayed if there are no updates.)



Note: To receive notifications of updates automatically, enable the **Check hourly for available updates** checkbox, enter the email address where notifications should be sent, and click the **Apply** button.

- To view newly-available updates, click **Update Information** on the left to go back to the **Update Information** page.



This page lists all available Mirapoint Software updates. **Before installing any update, view its description to verify that it applies.** For more information about updates, log in to <http://support.mirapoint.com> or contact Mirapoint Technical Support at support-admin@mirapoint.com.

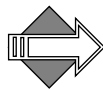
- To install an update, click the **Install** button and follow the update instructions to complete the installation.



When you install an update, the system must reboot and all services are interrupted. Once the system has restarted, you will need to reconnect to the Administration Suite to proceed with the setup process. Please note: Most patches do not require a reboot to install.

Restricting Administrator Access

By default, the appliance administration service accepts administrator logins from any IP address. To restrict administrator logins to a designated set of IP addresses or network subgroup, use the **System > Services > Administration > Trusted Admin** page to specify the addresses from which the administration service should accept administrator logins.



The Trusted Admin specifications you make here display on the **Security > Trusted Admin** page and changes you make on that page will display here, as well.

Set Trusted Admin

Specify certain IP addresses for administration purposes.
Only administrators logging onto the specified addresses are granted administration privileges.
You may specify an entire network as trusted using a network specifier.

Trusted Admin:

No items in list

On the **Trusted Admin** page, enter the IP address of the client host to which you want to restrict administration activity (you can also use a network specifier; see below for details). Click **Add**. The Trusted Admin list is updated with the new client host or network. Administration activity can only take place on that client or network. If you have not already added this client, you are prompted to do so before any other can be specified; this prevents accidental lock-out.

About Trusted Network Specifiers

In addition to designating individual IP addresses as trusted, you can specify an entire network as trusted using a network specifier, a string of the form:

dotted-quad/mask-bits

where *dotted-quad* is an IP address in dotted decimal notation, such as 10.0.0.0, and *mask-bits* is the number of bits in the network mask to be used in comparing addresses. If *mask-bits* is 8, the first octet must match; if *mask-bits* is 16, the first two octets must match; if *mask-bits* is 24, the first three octets must match.

For example, if **192.168.0.0/24** is the only trusted network specifier, a client connecting from 192.168.0.76 is granted access (the first three octets match), but a client connecting from 192.168.5.76 is denied access (the third octet does not match).

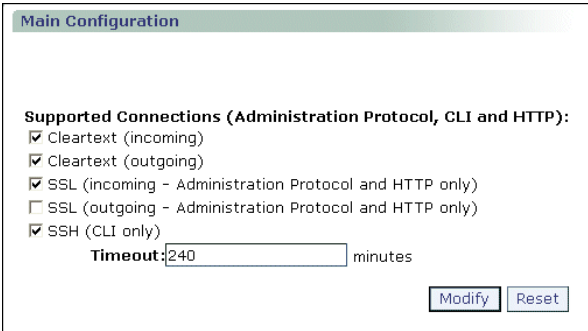
Only users whose IP addresses match one of the trusted IP addresses or network specifiers are allowed administration privileges. Users whose addresses do not match are denied access.

Adjusting Administration Security

Before you start using your appliance, you will want to enable SSL (secure sockets layer) and SSH (secure shell), if licensed.

1. Go to **Home > System > Services > Administration > Main Configuration**.
2. Select **SSL (incoming - Administration Protocol and HTTP only)** and **SSH (CLI only)**. Select **SSL (outgoing - Administration Protocol and HTTP only)** if you want outbound communications encrypted as well; this could be needed in the case of a RazorGate acting as a proxy server to a Message Store that had SSL configured.

When you are done, click **Modify** to save your changes.



The screenshot shows a web interface titled "Main Configuration". Under the heading "Supported Connections (Administration Protocol, CLI and HTTP):", there are five checkboxes: "Cleartext (incoming)", "Cleartext (outgoing)", "SSL (incoming - Administration Protocol and HTTP only)", "SSL (outgoing - Administration Protocol and HTTP only)", and "SSH (CLI only)". The first, second, third, and fifth checkboxes are checked. Below these is a "Timeout" field with the value "240" and the unit "minutes". At the bottom right of the form are two buttons: "Modify" and "Reset".

Checking Basic Configurations

Before continuing, make sure you have completed the initial setup of the software by:

- ◆ [“Completing the Setup Wizard” on page 39](#)
- ◆ [“Checking for Software Updates” on page 46](#)
- ◆ [“Restricting Administrator Access” on page 48](#)
- ◆ [“Adjusting Administration Security” on page 50](#)

Once these tasks are done, you can proceed to “Completing Your Configuration,” next.

Completing Your Configuration

To finish the appliance software setup, you need to follow the procedures outlined in the appropriate chapter for your deployment:

- ◆ [Chapter 2, “All-In-One Message Server Deployment”](#)
- ◆ [Chapter 3, “RazorGate Security Deployment for Exchange”](#)
- ◆ [Chapter 4, “RazorGate with Junk Mail Manager Security Deployment for Exchange”](#)
- ◆ [Chapter 5, “Multi-Tier, Multi-Appliance Deployment”](#)

Mirapoint Messaging and LDAP

This section describes how the various Mirapoint routing and proxying subsystems interact with LDAP. Read this to help make better choices as you complete your configuration.

Managing the Cache

LDAP queries take advantage of a system cache of previous lookups. This is a time-to-revive cache, meaning that entries are only fetched again on demand when expired; cache is used if LDAP servers fail to respond.

The cache can be managed with the CLI commands **Ldap Set Cachetimeout** and **Ldap Flushcache**.

LDAP lookup results can be tested using the **Ldap Testquery** command.

LDAP Binding

Mirapoint appliances do not use persistently bound connections to LDAP servers, because some LDAP servers cannot deal with the load.

By default, Mirapoint appliances bind anonymously to LDAP, except when performing user login authentication, in which case the querying system binds as the user to be authenticated.

Non-anonymous binding is done with the **Ldap Addaccess** command.

To add an access profile allowing a Mirapoint appliance to access and modify an area of the LDAP database, use the following command:

```
tag Ldap Addaccess baseDN bindDN password passwd-type
```

where:

- ◆ *baseDN* is the base distinguished name (baseDN) of a location. in the LDAP database that the Mirapoint appliance will access.
- ◆ *bindDN* is a distinguished name (bind DN) for authentication.
- ◆ *password* is the password for the specified bind DN.
- ◆ *passwd-type* is one of
 - ❖ **Encodedpass**—the password is encoded.
 - ❖ **Pass**—the password is plaintext (see **Help User Set**).

User LDAP Lookups

When a Mirapoint routes a message, it must look up information about the destination user. The same lookup is needed to proxy an IMAP or POP connection for a user. In both cases the DN and attributes for all **User:** queries are retrieved in one operation using the base DN and filter **User:Publishedname** query. The cache is checked before doing these lookups and is populated with positive results.

This type of lookup is used for SMTP routing, POP proxying, IMAP proxying, HTTP redirection (for WebMail, WebCal, GroupCal, and Administration Suite), outbound sender masquerading, and user login authentication.

User Login Authentication

Mirapoint appliances can use LDAP to authenticate user logins. This eases appliance maintenance by centralizing user and configuration data.

When a Mirapoint appliance uses LDAP to authenticate a user, it must first determine the user's DN. This is done with **User: lookup**. The cache is checked first; if the DN is not present, the query is cached.

Domain-Based Routing

Mirapoint appliances can use a wildcard record for all users in a given domain. This is done by having a record that looks like *@domain* selected by the **User:Publishedname** query. Mirapoint appliances can also equate one domain to another. This is useful to support legacy domains, often used when companies change names or domain. Equated domains are initiated by specifying a **User:Routingaddr** attribute of *@newdom*.

Both these features are supported by LDAP lookups. Domain-based lookups increase LDAP traffic, but caching can minimize overhead.

If a username is fully qualified and the LDAP **User:** lookup fails, a user of the form *@domain* is looked up if it is not already in the cache. Both positive and negative responses are cached.

If a **User:Routingaddr** attribute exists and is of the *@newdomain* form, the user's name is rewritten to *user@newdomain*. A lookup of *user@newdomain* is done from the cache, then from LDAP, to see if there is specific routing information for this user. No domain-based lookup is done after this lookup.

All domain-equates must point directly at the end record; no recursive lookups are done. Positive results of this last lookup are cached.

Equated Domains

You can use a single LDAP entry to specify that all messages or logins for a particular domain are to be routed to a different domain. Both envelope and header of redirected messages get rewritten. An example:

```
mail: @example.com  
mailRoutingaddress: @ejemplo.co.es
```

You can set a system-wide default in LDAP by specifying the following value for the mail attribute:

```
mail: @
```

Overriding an Equated Domain Route

You can override equated domain routing for specific users by adding explicit LDAP entries for them. Explicit LDAP entries take precedence over generalized entries to equate domains. An example:

```
mail: juser@example.com  
mailAlternateAddr: juser@smallco.com
```

Mail Groups Support

To facilitate expansion of LDAP groups into distribution lists, mail groups can be created in an LDAP database and referenced by queries. Mirapoint appliances can obtain a list of group members from LDAP and use them as a distribution list.

During address expansion, a lookup based on the **Mailgroup:Members** query looks up all attributes specified in **Mailgroup:Members** and **Mailgroup:Owner**. These are then sorted into a number of groups.

If the attribute **Mailgroup:Owner** has an associated type of **Indirect**, another LDAP lookup is done with the **User:Publishedname** query to retrieve and cache the RFC 822 address of the list owner.

Another set of mail group members comes from attributes listed in **Mailgroup:Members** with an associated type of **Direct**. These are stored in the list of RFC 822–style addresses.

Yet another set of mail group members comes from attributes listed in **Mailgroup:Members** with an associated type of **Indirect**. These are sorted by the base DN of their value. For each base DN returned in the query above, a separate base scope LDAP search is performed with the **User:Publishedname** attribute. The results of these nested lookups are added to the list of RFC 822–style addresses.

LDAP Mail Groups

Mail groups can be created to replace single-server distribution lists (DLs) by defining LDAP records like this one for **d1XY**:

```
dn: mail=d1XY@example.com,ou=lists,dc=example,dc=com  
cn: d1XY  
mail: d1XY@example.com
```

```

mailLocalAddress: d1XY
owner: mailadm@example.com
mgrpRFC822MailMember: juser@example.com
mgrpRFC822MailMember: jane@example.com
mgrpRFC822MailMamber: +archive.d1XY@example.com
objectClass: mailGroup
objectClass: groupOfNames

```

In this example, errors go to owner **mailadm**. The **d1XY** mailgroup has two members, and all messages are saved in a shared **archive** folder. The following related **Ldap Setquery** commands must be specified:

```

Ldap Setquery mailgroup:Members "baseDN" "(mail=$(group))"
    "uniquemember mgrprfc822address" "indirect direct"
Ldap Setquery mailgroup:Owner "baseDN" "(mail=$(group))" "owner" ""

```

If you put users in the **ou=people,o=top** hierarchy and mail groups in **ou=lists,o=top** and specify different baseDNs for both the sets of users and groups, you get the effect of a “backslash” in **sendmail** alias files (local delivery). A back-slashed user becomes a **uniquemember** (with DN of the user); everyone else becomes an **mgrpRFC822address**. For more on LDAP queries, see “Setting Up Queries” on page 110.

Group Membership ACLs

Folder access permissions can be stored using LDAP groups. When you need to determine whether the user is a member of a group:

1. Determine the DN of the user. Do this with a **User:Publishedname** query, using the cache as described above.
2. Find the DN of the group. Do this with the base DN and filter specified in the **User:Groupmembership** query.
3. Assuming you have both DN's, perform an LDAP compare to see if there is an attribute in **User:Groupmembership** that has the value of the user's DN. Group membership is valid for an IMAP session.

Autoprovisioning User Accounts

Mirapoint appliances can automatically create a user account from LDAP when the user logs in for the first time or when the first message arrives. Messages addressed to a local user cause an LDAP **User:** lookup. If the name associated with **User:Mailhost** attribute is the same

as local host, then the user account and inbox are created. This can cause repeated LDAP lookups in the case of incorrectly addressed e-mail.

An LDAP entry is required to autoprovision each user. Domain-based routing (*@example.com* for everyone) does not trigger autoprovisioning. If the LDAP database has sufficiently detailed records, Mirapoint users are automatically created as needed. LDAP autoprovisioning does not create subfolders underneath the Inbox, nor can it set custom ACLs.

For instructions on setting up LDAP queries for autoprovisioning, see “Setting Up Autoprovisioning of Users” on page 90.

Setting Up the LDAP Client Queries

Mirapoint LDAP clients can be any entity (application, server, etc.) that accesses or queries the Directory Server for information contained within the server’s directory information tree (DIT). Individual users do not directly access or communicate with a directory (LDAP) server—client applications do. The LDAP attributes specified in any query filter must be indexed in the directory’s database.

LDAP Query Basics

You create LDAP queries on the client server (Message Director or Message Server) to support the needs of client applications, such as LDAP routing. Queries enable lookup and retrieval of data from the LDAP server. They tell the Directory Server what information to return and where in the database to start searching for that information.

To properly construct your LDAP queries, it is important to understand the query process. The following is an example of LDAP routing:

An e-mail is received by an IMR, where the system looks at the “To:” address. The IMR matches components of the e-mail address with the variable values specified in the query filter strings, and expands or replaces variables with the corresponding portions of the address. The IMR transmits the query to the Directory Server, which responds with the information requested.

A query is comprised of four arguments:

- ◆ The query specification —A Mirapoint-defined alias that refers to an LDAP attribute to be returned by the Directory Server.
- ◆ A baseDN—The location in the directory information tree (DIT) where the information search begins.
- ◆ A filter—What to look for in the DIT: an attribute-value pair to find the object (mailbox, domain, login) you are searching for.
- ◆ An attribute—The information you want: the LDAP attribute value or data field to be returned, as determined by the filter.

These arguments are used in the LDAP **Setquery** command syntax to manage LDAP lookup operations.

Query Specifications

The query specification is a named collection of configuration data used to retrieve a particular piece of information from an LDAP database. The query specification name is a Mirapoint-defined name for an LDAP attribute. For example, the query specification **User:PublishedName** maps to the attribute **mail**.

Table 5 below identifies the query specification required by each LDAP client discussed in this chapter.

Table 5 Query Specifications for LDAP Client Queries

Query Specification	LDAP Routing	Mailgroup DL	IMAP Proxy	HTTP Redirect	Authentication	Autoprovision
user:PublishedName	Set	Set	Set	Set	Set	Set
user:Mailhost	Set	N/A	Set	Set	Set	Set
user:RoutingAddr	Set	N/A	Set	Set	Set	Set
user:LoginId	N/A	N/A	N/A	N/A	Set	Set

Table 5 Query Specifications for LDAP Client Queries (Continued)

Query Specification	LDAP Routing	Mailgroup DL	IMAP Proxy	HTTP Redirect	Authentication	Autoprovision
user:Quota	N/A	N/A	N/A	N/A	N/A	Set
user:Fullname	N/A	N/A	N/A	N/A	Set	Set
mailgroup:Member	N/A	Set	N/A	N/A	N/A	N/A
mailgroup:Owner	N/A	Set	N/A	N/A	N/A	N/A

Query specifications map to LDAP attributes stored in the Directory Server's database. See Table 6 below for this mapping.

Table 6 Query Specifications and LDAP Attribute Mapping

Query Specification	LDAP Attribute
user:PublishedName	mail
user:Mailhost	mailHost
user:RoutingAddr	mailRoutingAddress
user:LoginId	uid
user:Uuid	miUuid
user:Quota	quota
user:Fullname	cn
mailgroup:Member	mgrpMailMember
mailgroup:Owner	owner

The BaseDN

The baseDN specifies where in the LDAP database (DIT) to begin the information search. An LDAP database is a named container that stores one or more directory information trees (DITs). The DIT is a hierarchy

of object entries. The baseDN can be the topmost entry in the DIT, also known as the rootDN, or it can be a leaf-node. For example, if the rootDN is specified as the baseDN, it could be `o=top`; if a leaf-node is specified as the baseDN, it could be `ou=users,o=top` (see Figure 1 below).

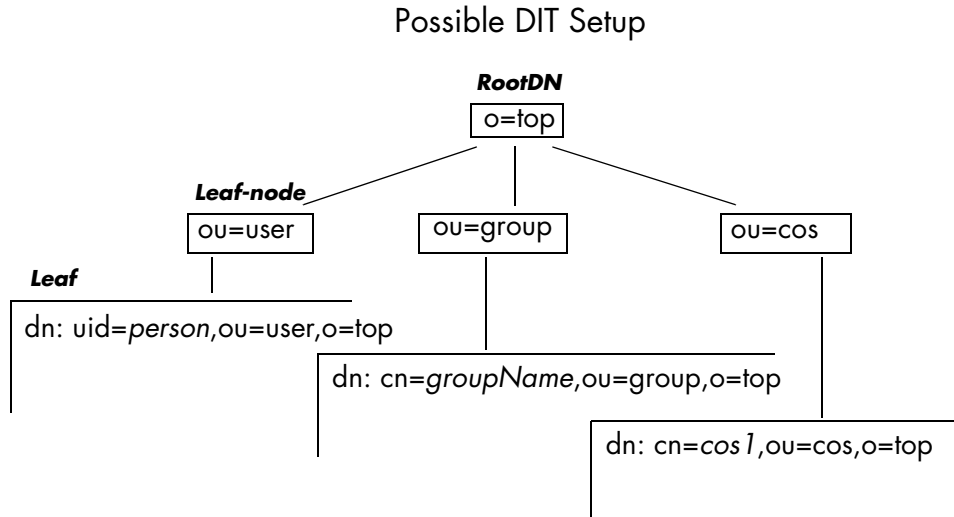


Figure 1 DIT Hierarchical Setup

Filters

A filter specifies what information you want to search for in an LDAP database. A basic filter is comprised of an LDAP attribute, a comparison operator, and a value enclosed in parentheses; this is known as an **attribute value assertion (AVA)**. For example:

```
(mail=$(login))
```

Where **mail** is the attribute, **=** is the comparison operator, and **\$(login)** is the value. The entire string is the AVA.

See Table 6 on page 58 for a list of the attributes used in setting up Mirapoint LDAP client queries.

Use the following comparison operators to construct AVA filters:

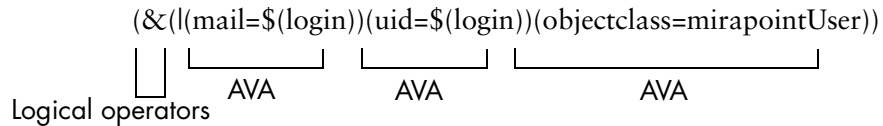
- = Equality
- >= Greater than
- <= Less than

Filter values are expanded with information found in an e-mail address before the query is sent on to the Directory Server, and can be classified as either “User” or “Group.” See Table 7 below for a list of the values that can be specified in the filter string, their corresponding e-mail component, and their classification.

Table 7 Filter Variable Values

Values	Classification	E-mail Address Component
\$(login)	User	user@example.com
\$(mbox)	User	user
\$(domain)	User/Group	example.com
\$(dcmapi)	User/Group	example
\$(group)	Group	group1@example.com
\$(groupname)	Group	group1

A Mirapoint LDAP query filter can be set up with one or more AVAs, each enclosed in parentheses, prefaced by one or more logical operators that are enclosed in parentheses. For example:



See Table 8 below for the logical operators used in Mirapoint queries.

Table 8 Filter Logical Operators

Logical Operator	Description
&	And —Used when including multiple groups of filter AVAs. For example: (&(l(mail=\${login}))(uid=\${login}))(objectclass=mirapointuser))
	Or —Used when grouping multiple AVA filters. For example: ((mail=\${login}))(uid=\${login}))
!	Not —Used when including multiple groups of filter AVAs. For example: (!(l(mail=\${login}))(uid=\${login}))(mailHost=\${login}))

Setting Up Queries

For various “user” queries, the baseDN and filters in the query string must be the same. The same is true for “group” queries. However the baseDN and filters used in “user” queries do not have to be the same as those used in “group” queries. LDAP query syntax is as follows:

Queryspec Basedn Filter Attr Type

where:

- ◆ **Queryspec** is the Mirapoint query specification.
- ◆ **Basedn** is the location in the directory information tree (DIT) where the information begins.
- ◆ **Filter** is an attribute-value pair to find the object (mailbox, domain, login) you want to search for.
- ◆ **Attr** is the LDAP attribute value or data field to be returned, as determined by the filter.
- ◆ **Type** is reserved and used only in MailGroup: queries. Type is represented by an empty string ("") in all other queries.

Use the **Ldap Setquery** command to set up one query for each LDAP client on the Message Director.

See Table 5 on page 57 for information on what queries need to be set to support each client. Mirapoint recommends that the following query filter template be used for all “user” queries:

```
"(&(|(mail=$(login))(uid=$(login))(maillocaladdress=$(login))
(objectclass=mirapointMailUser))"
```

The following template is recommended for all “group” queries:

```
"(&(|(mail=$(group))(maillocaladdress=$(group))
(objectclass=mirapointMailUser))"
```

For example, a query for *user:publishedName* as the **Mail** attribute could look like the following:

```
Ldap Setquery user:publishedName "BaseDN"
"(&(|(mail=$(login))(uid=$(login))(maillocaladdress=$(login))
(objectclass=mirapointMailUser))" Mail ""
```

where:

- ◆ **User:publishedName** represents the queryspec.
- ◆ *BaseDN* represents the place in the database to start looking for requested information, “dc=example,dc=com” for example.
- ◆ “(|(mail=\$(login))(uid=\$(login))(maillocaladdress=\$(login)))” specifies the filter, and “(&...(objectclass=mirapointMailUser))” qualifies the filter so it applies only to mail-user information in the LDAP database.
- ◆ **Mail** represents the attribute of this filter.
- ◆ "" represents an empty string for Type, which is reserved for MailGroup queries.

As of Release 3.4, the first query establishes a template that is followed by successive **Ldap Setquery** commands.

All-In-One Message Server Deployment

In this deployment, a Message Server appliance performs message screening including MailHurdle, antivirus, antispam, and filtering; directory services; and message storage and delivery. How to set up these functions is described in this chapter. For more information on this deployment, see the *Mirapoint Administrator's Planning Guide*.

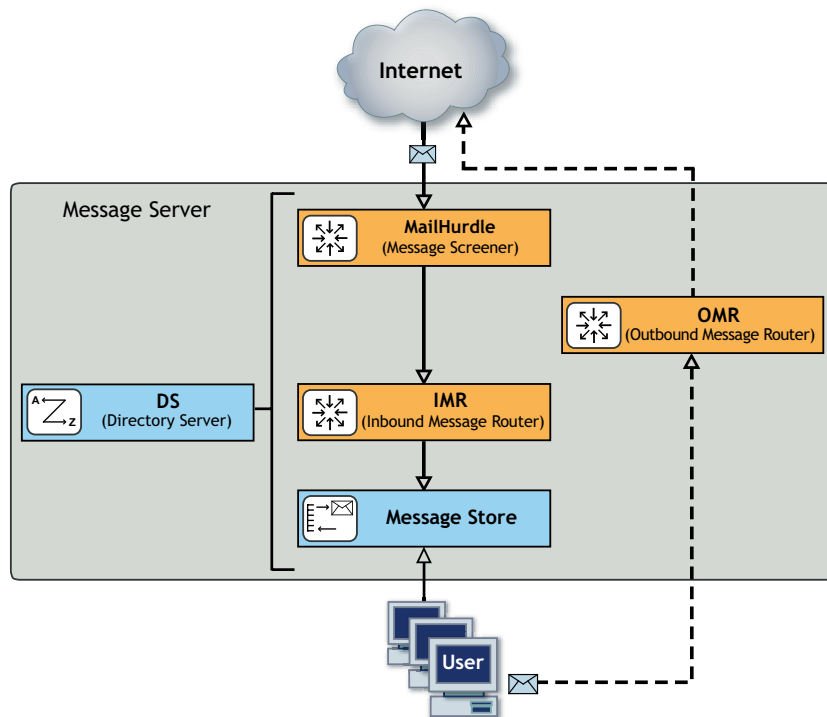


Figure 2 All-in-One Deployment Example

Before You Begin

Before you begin configuring your Message Server's security and messaging functions, make sure that you have read [Chapter 1, "All Deployments Start Here,"](#) and performed the tasks described, including:

- ◆ [Pre-Configuration Checklist](#) (as applicable):
 - ❖ Domain Name System (DNS) servers configured
 - ❖ Lightweight Directory Access Protocol (LDAP) set up
 - ❖ Licenses obtained (licenses are implementation specific)
 - ❖ Backup requirements defined
 - ❖ Secure Sockets Layer (SSL) certificates obtained
- ◆ [Prerequisites](#):
 - ❖ Hardware installation (connected to the Internet)
 - ❖ DNS server database records
 - ❖ Basic system setup (described on the Quick Start Setup card shipped with your appliance)
- ◆ [Initial Setup Common to All Deployments](#):
 - ❖ Secure administrator account set
 - ❖ Appliance clock set
 - ❖ Network settings verified, DNS server(s) added
 - ❖ Licenses installed
 - ❖ Service Reporting options set
 - ❖ Software updates obtained
 - ❖ Administrator access restricted
 - ❖ SSL security for administrator logins set

Information Required for this Configuration

You need the following information to configure you All-in-One Message Server, as documented here:

- ◆ A list of senders and recipients (IP addresses, domain names, and email addresses) that you want to **safelist** by adding to your Allowed Senders/Allowed Mailing Lists. Safelisting senders/recipients ensures that mail from or to, respectively, those addresses

is never subject to antispam delays. You will also set priority on those lists to override antispam scanning.

- ◆ A list of RBL (Realtime Blackhole List) servers. You can learn more about this through Wikipedia: <http://en.wikipedia.org/wiki/DNSBL>.
- ◆ The hostname, port number, and authentication credentials (if appropriate) for your Proxy Server if your site blocks outgoing HTTP and FTP connections. This is required to get system, antivirus, and antispam updates.
- ◆ The hostname and port number of any address book directories that you want to add, as well as the display name for each.
- ◆ The hostname, port number, and baseDN of any calendars that you want to add, as well as the display name for each.
- ◆ Names of all Group Calendar resources and a name for the Group Calendar resource mailgroup (something like “resources” is fine).
- ◆ IP addresses for all DNS servers you want to add.



Even if you currently only expect to use a single domain, Mirapoint recommends that you create your domain as a delegated domain rather than using the primary (default) domain. This provides you with the flexibility of adding additional namespaces later. When you have delegated domains, only use the primary domain for global administration. All mail handling is best done through the delegated domains.

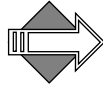
- ◆ **Licenses**—The licenses for this deployment are listed below. Verifying installed licenses and installing licenses is described in step 5 of [“Completing the Setup Wizard” on page 39](#). Note: Licenses are implementation-specific.
 - ❖ Required licenses:
 - User Limit: appropriate for your needs
 - LDAP Routing
 - WebMail: appropriate for your needs
 - Corporate Edition: appropriate for your needs
 - POP: appropriate for your needs
 - IMAP: appropriate for your needs
 - Message Server
 - Group Calendar

- SSL
- Directory Server
- Domain Administration
- ❖ Optional licenses (you'll want at least one antivirus and one antispam):
 - Sophos (signature-based) virus filtering
 - F-Secure (signature-based) virus filtering
 - RAPID (predictive-based) virus filtering
 - Antispam (Principal Edition) or Antispam SE (Signature Edition)



Checking your licenses is described below on page 68.

Mirapoint recommends at least one signature-based antivirus and RAPID. Please Note: RAPID antivirus must be used in conjunction with a signature-based antivirus engine (Sophos or F-Secure).



The two Antispam licenses are mutually exclusive.

Configuring An All-In-One Message Server

When you configure a Message Server for an all-in-one deployment, it performs security functions, plus message retrieval, storage and delivery, and outbound message handling. This involves the following tasks:

- ◆ Accessing the Administration Suite
- ◆ Checking for Licenses
- ◆ Setting the Administration Timeout
- ◆ Configuring MailHurdle
- ◆ Configuring Anti-Virus Scanning
- ◆ Configuring Anti-Spam Scanning
- ◆ Setting Up a User Directory Service
- ◆ Additional Command Line Configuration Tasks
- ◆ Configuring WebMail

- ◆ Configuring IMAP
- ◆ Configuring SMTP
- ◆ Enabling and Starting Services
- ◆ Resetting the Administration Timeout

At this point, we recommend you test your all-in-one setup:

- ◆ Refresh the Administration Suite
- ◆ Create a Class Of Service
- ◆ Create User Accounts
- ◆ Send a Test Message
- ◆ Receive a Test Message
- ◆ Verify the Address Book Directory Service
- ◆ Create a Calendar Event

Three optional configuration tasks are also described:

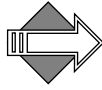
- ◆ Adding Networks or Domains to the Reject List: This restricts what domains can send mail to your system.
- ◆ Setting the HTTP Default Access: This determines what application opens when the URL is opened.
- ◆ Configuring Safe Lists and Blocked Lists: These allow mail from certain senders or recipients to always (or never, in the case of the Blocked list) have their mail delivered.

Accessing the Administration Suite

You use the Administration Suite to perform most Message Server configuration tasks; some can only be done through the command line interface (CLI). To access the Administration Suite, go to **`http://hostname/miradmin`**, where *hostname* is your appliance's fully-qualified domain name. Log in as administrator.

The Administration Suite displays function links at the left and a navigation bar at the top that tracks your current location within the

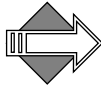
page hierarchy. The **Site Map** link (in the upper right corner) displays links to most pages.



If you are accessing the Administration Suite for the first time, the Setup Wizard displays. You need to use the Setup Wizard to perform the basic configuration tasks described in [“Completing the Setup Wizard” on page 39](#) before continuing.

Checking for Licenses

To verify that you have the licenses you need for this configuration, go to **Home > System > Utilities > License** page to see all the license keys available to you.



The MailHurdle license does not display; it is part of the Anti-Spam license.

Setting the Administration Timeout

You'll want to change the default Administration Suite timeout from 10 minutes to at least 60 minutes while you configure the Message Server.

Go to **Home > System > Services > Administration > Main Configuration** page and change the **Timeout** to at least 60 minutes. Click **Modify** to save your changes.

Note: You'll want to change it back to 10 minutes once you are done.

A screenshot of a web-based configuration window titled "Main Configuration". The window has a light green header bar. Below the header, the text "Supported Connections (Administration Protocol, CLI and HTTP):" is followed by a list of options with checkboxes: "Cleartext (incoming)" (checked), "Cleartext (outgoing)" (checked), "SSL (incoming - Administration Protocol and HTTP only)" (unchecked), "SSL (outgoing - Administration Protocol and HTTP only)" (unchecked), and "SSH (CLI only)" (unchecked). Below these options is a text input field labeled "Timeout:" containing the number "60", followed by the word "minutes". At the bottom right of the window are two buttons: "Modify" and "Reset".

Configuring Anti-Virus Scanning

Anti-Virus scanning is a licensed feature. If you have not purchased a virus scanning license, skip this section and proceed to [“Configuring Anti-Spam Scanning” on page 76](#).

There are three antivirus scanners you can license and configure: F-Secure, Sophos, and RAPID. **F-Secure** and **Sophos** are **signature-based**, meaning they use databases of known viruses to identify messages that contain viruses. **RAPID** is **predictive-based**, meaning it uses a database of heuristics to identify messages that *potentially* contain viruses. Because RAPID finds potential viruses, rather than known viruses, its only available action is quarantine. RAPID-quarantined messages are automatically released after a configurable amount of time, allowing one of the signature-based antivirus engines to re-scan the messages and ensure that viruses are caught.



Mirapoint recommends configuring one signature-based antivirus scanner and RAPID antivirus scanner on all-in-one deployments. Note: RAPID antivirus must be used in conjunction with a signature-based antivirus; used alone it is ineffective. You can run all three antivirus engines on one system if you have all three licenses.

Configuring F-Secure or Sophos Anti-Virus

To configure Sophos or F-Secure Anti-Virus, follow these steps. You'll need to repeat the procedure if you have both scanners.

1. Go to **Home > Anti-Virus**, click the link at left for the scanner to be configured, F-Secure or Sophos (only licensed options display). The main page for that virus scanner opens. Click **Configuration**.



2. On the **Anti-Virus > virus scanner > Configuration** page, if the scanner is disabled, click the **Enable It** button. Accept the default **Auto-Clean (Delete)** option. If you want to archive caught viruses, enter an e-mail address in the **Anti-Virus Quarantine** field.



Messages sent to the **Anti-Virus Quarantine** contain live viruses and should not be opened on a desktop computer.

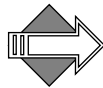
Anti-Virus is currently **enabled**.

Select one of these Anti-Virus Actions

Action	Description
<input checked="" type="radio"/> Auto Clean (Delete)	Auto Clean if possible. Otherwise, delete the infected attachment.
<input type="radio"/> Auto Clean (Ignore)	Auto Clean if possible. Otherwise, ignore the virus and process the message normally.
<input type="radio"/> Delete	Delete the infected attachment.
<input type="radio"/> Ignore	Ignore the virus and process the message normally.

Anti-Virus Quarantine
A copy of the original infected message can be quarantined for administrative purposes.
Note that these mail messages will contain live viruses.

E-mail address:



If you select the **Auto Clean (Ignore)** or **Ignore** options, infected messages will be delivered to your users. If you make changes, click **Apply** to save your changes.

You do not need to modify the **Anti-Virus > Notifications** page.

3. On the **Anti-Virus > virus scanner > Updates** page, change the default hourly time if this is not good for your site. If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**. When you are done, click **Apply** to save your changes.

The screenshot shows a dialog box titled "Automatic Update and Proxy Server". It contains the following elements:

- Automatically update:**
 - *Hourly: :39 (on the minute)
 - Daily: 00:00 (on the hour)
 - Weekly: Sunday (day of week)
 - Monthly: 1 (on the day)
- *Strongly Recommended
- Use Proxy Server:**
 - Host:
 - Port:
 - User ID:
 - Password:
- Buttons:

Configuring RAPID Anti-Virus

RAPID Anti-Virus is a licensed feature, it uses a **predictive-based** methodology that immediately categorizes suspect mail as spam based on heuristics maintained in a rulegroup. To be effective, RAPID must be used in conjunction with one of the signature-based antivirus scanners, F-Secure or Sophos. Alone, RAPID is not an effective antivirus solution.

There are some file extensions that always trigger the RAPID antivirus quarantine action; for details, see [“Modifying Predictive-based \(RAPID\) Anti-Virus” on page 409](#) in the Administration Tasks part of this book.

To configure RAPID Anti-Virus, follow these steps.

1. Go to **Home > Anti-Virus > RAPID > Configuration**, if the scanner is disabled, click the **Enable It** button.

Anti-Virus is currently **enabled**.

Anti-Virus Quarantine
All e-mail messages potentially containing a virus are quarantined automatically.
All other e-mail messages will be delivered to the recipient(s).

Note that these mail messages may contain live viruses.

Quarantine folder: user.UserName[.Folder.Folder...
Note: UserName must have quarantine administrator role.

2. Accept the default **Quarantine folder** address, a subfolder of the Administrator account. Later, you might use any valid `user.username.subfolder` e-mail address for an account with the Quarantine Administrator role. For details, see [“How Antivirus Quarantine Works” on page 398](#), and [“Using Security Quarantine” on page 441](#) in the Administration Tasks part of this book. If you make changes, click **Apply** to save your changes.

Afterwards, all messages potentially containing a virus are automatically quarantined for 8 hours to the specified email address; other messages are delivered normally. The auto-release time can be modified using the CLI; see **Help About Antivirus**.

3. Go to **Anti-Virus > RAPID > Notifications** and modify the format of virus notifications as appropriate. Whereas notifications for F-Secure or Sophos-caught viruses are not really needed, because those are known viruses, notifications for RAPID quarantined potential viruses are very important. Users should be made aware that a message is quarantined for a potential virus.



In the **To** option, add the appropriate administrator’s email address (or just **Administrator** to use the default). Notifications are sent to the specified RAPID AV quarantine administrator(s) when messages are quarantined. Use commas (,) as separators to enter multiple email addresses.

When you are done, click **Apply** to save your changes.

Send this notification to the message recipient(s) when a potential virus is found.

This notification is currently **disabled**.

To:

From:

Subject:

Message:

Unicode (UTF-8)

\$(recipientlist)=Recipient(s) \$(sender)=Sender
 \$(subject)=Subject \$(action)=Action
 \$(attachments)=List of attachments
 \$(domain)=Current Domain
 \$(filtername)=Filter name that triggered the notification

4. Go to **Home > Anti-Virus > RAPID > Updates** and change the default hourly time if this is not good for your site.

If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**.

When you are done, click **Apply** to save your changes.

Automatic Update and Proxy Server

Automatically update:

*Hourly: (on the minute)

Daily: (on the hour)

Weekly: (day of week)

Monthly: (on the day)

**Ruleset Name:

**Required for RAPID AV Updates
 *Strongly Recommended

Use Proxy Server:

Host:

Port:

User ID:

Password:

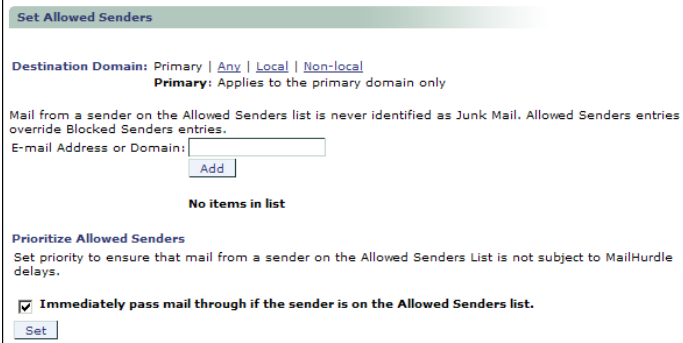
Configuring MailHurdle

Mirapoint MailHurdle blocks spam by screening messages from unrecognized sources. When a message is received from an unrecognized source, MailHurdle temporarily fails the message and sends a **retry later** code. A properly-configured mail server automatically re-sends the message, which is then accepted by MailHurdle; however, most spam mailers do not retry.

To configure MailHurdle to ensure the timely delivery of valid messages, follow these steps.

1. Go to **Home > Anti-Spam > Allowed Senders**. Leave the Destination Domain option at the default, **Primary**. Add domains and SMTP email addresses from which your users often receive email; after each entry click **Add**. Select the **Immediately pass mail through if the sender is on the Allowed Senders list** option.

When you are done, click **Set** to save your changes.



The screenshot shows the 'Set Allowed Senders' configuration window. At the top, it says 'Set Allowed Senders'. Below that, there are options for 'Destination Domain' with 'Primary' selected, and links for 'Any', 'Local', and 'Non-local'. A note states: 'Primary: Applies to the primary domain only'. Below this, a message explains: 'Mail from a sender on the Allowed Senders list is never identified as Junk Mail. Allowed Senders entries override Blocked Senders entries.' There is an input field for 'E-mail Address or Domain:' with an 'Add' button next to it. Below the input field, it says 'No items in list'. Further down, there is a section titled 'Prioritize Allowed Senders' with the text: 'Set priority to ensure that mail from a sender on the Allowed Senders List is not subject to MailHurdle delays.' At the bottom, there is a checked checkbox for 'Immediately pass mail through if the sender is on the Allowed Senders list.' and a 'Set' button.

2. Go to **Anti-Spam > Allowed Mailing Lists**. Leave the **Destination Domain** option at the default, **Primary**. Add recipients whose email should *not* be subject to MailHurdle screening; in general this is used to protect distribution lists (also known as mailing lists). For example, you might want to add your support address to the Allowed Mailing Lists so mail sent to support is always delivered immediately. After each entry, click **Add**. Select the **Immediately pass mail through if the recipient is on the Allowed Mailing Lists** option.

When you are done, click **Set** to save your changes.

3. Go to **Anti-Spam > MailHurdle > Configuration**, if MailHurdle is disabled, click the **Enable It** button; several options display once MailHurdle is enabled. Leave the **MailHurdle Server** option empty, you do not need it for an all-in-one configuration. Likewise, you can accept the default **Triplet Timeouts** for now; you might want to adjust them later after you've established a baseline.

You do not need to click **Set** unless you make changes.

4. Do not modify the **MailHurdle > Allowed Host** page. In an all-in-one deployment, you do not need to add allowed hosts.
5. Do not modify the **MailHurdle > Advanced** page. The defaults are appropriate for all-in-one deployments.

This completes the MailHurdle set up.

For more information on MailHurdle and all of the available options, see [“Working with MailHurdle” on page 388](#) in the Administration Tasks part of this book.

Continue configuring Anti-Spam scanning with the following procedures.

Configuring Anti-Spam Scanning

Anti-Spam scanning is a licensed feature. There are two antispam licenses, **Mirapoint Antispam** (Principal Edition) and **Mirapoint Antispam SE** (Signature Edition), which are mutually-exclusive; however, the configuration options for both are identical and the update options differ only slightly. For details , see [“Principal Edition vs. Signature Edition” on page 417](#). To configure Anti-Spam scanning:

1. Go to **Home > Anti-Spam > Configuration**, click **Enable It**, if needed.

Anti-Spam Configuration

The Anti-Spam scanning utility scans all incoming e-mail messages for junk mail.

Anti-Spam scanning is currently **enabled**. [Disable It](#)
(Mirapoint Anti-Spam scanning is based on SpamAssassin)

[Set Threshold](#) [Show Junk Mail Statistics](#)
 Set a threshold for qualifying messages as junk mail (spam). The lower the threshold, the more likely messages will qualify as junk mail. The higher the threshold, the less likely messages will qualify as junk mail.

Threshold Number: (0 - 300, increment by 1)

Set Anti-Spam Warning Flag
 The Anti-Spam warning flag is added to the Subject line of all messages that qualify as junk mail (spam).

Add Warning Flag
 Flag Text:

Set Junk Mail Explanation
 Junk Mail Explanation inserts an "X-Junkmail-Info:" header to the message with an explanation of why it did (or did not) qualify as junk mail. The explanation includes the spam score, per rule; the name of each spam rule that was matched; and a simple description of the rule. If the total of all the spam scores received exceeds the **Threshold** (see [Set Threshold](#) section on this page), the message qualifies as junk mail.

Insert Junk Mail Explanation

Set Junk Mail Reporting
 Junk Mail Reporting provides a user option, **Report to system support**, for spam that the filter missed and false spam that accidentally triggered the filter. System folders for each are created when the options are used and Mirapoint is periodically sent samples from each folder; this can help Mirapoint make junk mail scanning improvements.

Enable Junk Mail Reporting

Disable Local Recipient Check
 The Anti-Spam local recipient check, ON by default, causes only mail to addresses in the local routing table to be scanned. This may be inappropriate for routers. Select the option below to disable this check, causing every message being routed to get scanned regardless of recipient address.

Scan messages for any recipient

[Apply](#)

Recommendations are:

- ❖ **Threshold Number:** Accept the default threshold of 50. Lower values incur more false positives; higher values miss spam.
- ❖ **Add Warning Flag:** Select. This adds a text string to the message subject indicating that the message is spam. The default string is Spam?.
- ❖ **Insert Junk Mail Explanation:** Accept the default (de-selected); in general, users do not need this feature. Note: This option only displays for **Mirapoint Antispam (Principal Edition)**.
- ❖ **Enable Junk Mail Reporting:** Accept the default (selected); this helps Mirapoint tune the antispam scanning rules.

- ❖ **Scan messages for any recipient:** Accept the default (deselected); this option is not needed on an all-in-one deployment. When you are done, click **Apply** to save your changes.
2. Go to **Anti-Spam > Updates**, select the rulegroup, Principal Edition: **default**, Signature Edition (RAPID): **RPDENGINE** or (in Asia) **RPDASIA**, and click **Update Now**. If you don't see the appropriate rulegroup, enter the **Rule Group Name** and click **Install**. If you clicked **Update Now**, the installed rulegroup is updated; if you clicked **Install**, the named rulegroup is installed. Note: Updating or installing rulegroups can take a few minutes.

Anti-Spam Updates

Install/Update Rule Groups

Rule Group Name:

Rule Group Name	Expiration Date	Delete
<input checked="" type="checkbox"/> default	2007-09-24	<input type="button" value="X"/>

(Warning: Installing or updating rule group(s) will interrupt the services.)

Set Automatic Update & Proxy Server

Update all rule groups every week

Use Proxy Server:

Host:

Port:

User ID:

Password:

3. Select **Update all rule groups every week**. If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**. When you are done, click **Apply** to save your changes.
4. Do not modify the **Anti-Spam > Relay List** page unless you have an existing front-end, like Postini or Barracuda. You do not normally need to configure relays for an all-in-one deployment. If you are integrating with an existing system, enter the IP addresses of each front-end server.
5. Go to **Anti-Spam > RBL Host List**. If the service is disabled, click **Enable it**. If you have subscribed to an RBL service, add the service's host name to the **RBL Host List** page. Mirapoint recommends subscribing to an RBL service, or setting up a local

RBL server to block connections from known spam propagators by checking the connection source against a list maintained by a trusted third-party. See the Wikipedia DNSBL article at <http://en.wikipedia.org/wiki/DNSBL> for more information.

If you make changes, click **Apply** to save your changes.

6. Go to **Anti-Spam > Reject List**. Enter the domain name of any known spam sites if your site lacks access to an RBL service or there are sites that you know you want to block. Click **Add** for each address you enter.

Setting Up a User Directory Service

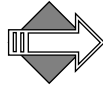
The Message Server includes a built-in LDAP directory server you can use for user authentication.

To use the Message Server's internal LDAP directory, you need to use the command-line interface (CLI) to set up the directory and configure the Message Server to use the directory.

In addition to setting up the internal directory service, Mirapoint recommends that you use the CLI to set TCP, address book, and calendar options before returning to the Administration Suite to complete the configuration process. These procedures are provided in [“Additional Command Line Configuration Tasks,”](#) following this section.

To access the CLI, telnet to your Message Server on the default telnet port (port 23) and log into the CLI as the Administrator:

```
User: telnet hostname.domain.com  
OK hostname.domain.com admin 3.8 server ready  
User: Administrator  
Password: password  
OK User logged in
```



CLI commands are *not* case-sensitive. To make the examples easier to read, they are shown in mixed case.

Set Up the Internal LDAP Directory

In a browser, go to <http://www.mirapoint.com/support/allinone.html> to see the commands as they must be entered (without line breaks). You can copy and paste the data from this file. If you have any problems accessing the HTML file, the data that needs to be entered is given in the steps below. Do not add spaces after commas or enter carriage

returns in the middle of a command—line breaks in the command examples below usually indicate spaces.

Follow these steps to set up the internal LDAP directory with a directory database named **miratop**.

1. Enter the **dir adddb** command to create a new LDAP database named miratop:

```
hostname.com> dir adddb miratop
OK Completed
```

2. Enter the **dir addbsuffix** command to add a new DIT (directory information tree) with the distinguished name (DN) `o=miratop` to the directory named miratop:

```
hostname.com> dir addbsuffix miratop o=miratop
OK Completed
```

3. Enter the **dir setdoption** command to set the directory administrator's RootDN (distinguished name):

```
hostname.com>dir setdoption miratop RootDN uid=administrator,o=miratop
OK Completed
```

4. Enter the **dir setdoption** command to set the directory administrator's RootPW. Substitute the system administrator password for *adminpassword*. This is the secure administrator account password that you created during basic system setup.

```
hostname.com> dir setdoption miratop RootPW adminpassword
OK Completed
```

5. Enter the **dir addindex** command to create the index for the directory's user attribute:

```
hostname.com> dir addindex "" miuserid eq
INFO "reindexing: miratop"
INFO "reindexing: default"
OK Completed
```

6. Import LDIF data to define the elements in the directory's DIT; first you enter the **importldif** command, then copy and paste from the file provided in step [b](#):
 - a. Begin the LDIF data import by entering this command:


```
hostname.com> dir importldif "" "c"
Enter LDIF directory data, finish with a "." on a line by
itself:
```
 - b. In a browser, go to <http://www.mirapoint.com/support/allinone.ldif> and copy and paste the LDIF data as input to the above command.
 - c. End the LDIF data import by entering a period (.) on a line by itself:


```
.

INFO "adding data"
INFO "5 of 5 successful"
OK Completed
```

Note: If you have any problems accessing the ldif file, the data that needs to be entered is given below. There must be a blank line before each DN entry, no spaces after commas, and no trailing blanks at the ends of the lines.

```
dn: o=miratop
objectClass: organization
o: miratop

dn: ou=domains,o=miratop
objectClass: organizationalUnit
ou: domains

dn: miDomainName=primary,ou=domains,o=miratop
objectClass: midomain
miDomainName: primary

dn: ou=cos,o=miratop
objectClass: organizationalUnit
ou: cos

dn: miDomainName=primary,ou=cos,o=miratop
objectClass: midomain
miDomainName: primary
```

Configure the Message Server to Use the Internal LDAP Directory

Once you have set up the internal LDAP directory, you need to configure the Message Server to use the directory. These commands are also available for copy and paste (or a visual check without line breaks) online at <http://www.mirapoint.com/support/allinone.html>.

1. Enter the **service** command to enable the LDAP directory service:

```
hostname.com>service enable dir
OK Completed
```

2. Enter the **service** command to start the LDAP directory service:

```
hostname.com>service start dir
OK Completed
```

3. Enter the **ldap add** command to add the internal LDAP directory (127.0.0.1 = localhost):

```
hostname.com>ldap add ldap://127.0.0.1:389
OK Completed
```

4. Set the basic LDAP query specifications for retrieving the **published name**, **mailhost**, **routing address**, and **login id** attributes from the LDAP directory. The query specifications consist of the directory's **base DN** (o=miratop), a **filter** string that contains a series of LDAP attribute-value pairs, and the **ldap** attribute name. The filter string is the same for each query, but you must set it first—do not skip step a. The **mailhost**, **routing address**, and **login id** queries can use the base DN and filter from the **published name** query.

Do not enter carriage returns in the middle of a command—line breaks in the command examples below usually indicate spaces.

- a. Enter the **ldap setquery** command to set the **publishedname** query:

```
hostname.com>ldap setquery user:publishedname o=miratop
"(|(mail=${login})(mlloginid=${login}))" mail ""
OK Completed
```

- b. Enter the `ldap setquery` command to set the `mailhost` query:

```
hostname.com>ldap setquery user:mailhost "" "" mailhost ""
OK Will use basedn and filter from user:publishedname query
```

- c. Enter the `ldap setquery` command to set the `routingaddr` query:

```
hostname.com>ldap setquery user:routingaddr "" "" mail ""
OK Will use basedn and filter from user:publishedname query
```

- d. Enter the `ldap setquery` command to set the `quota` query:

```
hostname.com>ldap setquery user:quota "" "" mimailquota ""
OK Will use basedn and filter from user:publishedname query
```

- e. Enter the `ldap setquery` command to set the `loginid` query:

```
hostname.com>ldap setquery user:loginid "" "" miloginid ""
OK Will use basedn and filter from user:publishedname query
```

- f. Enter the `ldap setquery` command to set the `uuid` query:

```
hostname.com>ldap setquery user:uuid "" "" miuuid ""
OK Will use basedn and filter from user:publishedname query
```

5. Enter the `ldap setquery` command to set the `mailgroup` members query (notice that the filter is different):

```
hostname.com>ldap setquery mailgroup:members o=miratop
"(&(objectclass=mailgroup)(cn=$(group)))" "mgrpRFC822MailMember
uniqueMember" "direct indirect"
OK Completed
```

6. Enter the `ldap addaccess` command to enable the Message Server to modify the LDAP database. Use the password you set in step 4 in [“Set Up the Internal LDAP Directory” on page 80](#) in place of *adminpassword*:

```
hostname.com>ldap addaccess o=miratop uid=administrator,o=miratop pass
Password: adminpassword
OK Completed
```

7. Enter the `conf enable` command to enable all LDAP configuration options, including the LDAP auto-provisioning pages:

```
hostname.com>conf enable ldapall
OK Completed
```

8. Enter the `cos enable` command to enable COS (if a feature is unlicensed, the command will fail); you can copy and paste this list if you want all these features available for COS:

```
cos enable antispan
cos enable antivirus
cos enable autoreply
cos enable calendar
cos enable enterpriseui
cos enable filter
cos enable forward
cos enable getmail
cos enable groupcalendar
cos enable imap
cos enable msgexpiration
cos enable msgundelete
cos enable pop
cos enable quota
cos enable sender_as
cos enable sender_av
cos enable ssl
cos enable webmail
```

9. Enter the `auth set` command to set the authentication mechanism:

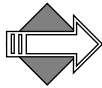
```
hostname.com> Auth Set Default Plaintext:Ldap
OK Completed
```

This completes the setup of the internal directory service. Keep your CLI window open and continue with [“Additional Command Line Configuration Tasks” on page 85](#).

Additional Command Line Configuration Tasks

While you are logged into the CLI, we recommend that you also perform the following configuration tasks:

- ◆ Limiting TCP Connections
- ◆ Setting up Group Calendar
- ◆ Adding the Address Book URL



CLI commands are *not* case-sensitive. To make the examples easier to read, they are shown in mixed case.

Setting up Group Calendar

Calendar groups require the presence of an LDAP database, internal or external. This procedure sets up Group Calendar with the internal LDAP. Group Calendar is a licensed feature, ensure that you have the license before beginning; you can check for it on the **System > Utilities > License** page. These commands are also available for copy and paste (or a visual check without line breaks) online at <http://www.mirapoint.com/support/allinone.html>.

When choosing LDAP schema and creating user entries in the database, note that the following attributes are employed by group calendar:

- ◆ **Mailroutingaddress** specifies where users receive e-mail (required).
- ◆ **Mailhost** specifies a server to keep schedules (required as fallback).
- ◆ **miUUID** specifies unique user ID (required in release 3.4 and later). This maps to **user:Uuid** for **Ldap Setquery**. For more information see [“Setting Up Queries” on page 61](#).
- ◆ **LoginID** specifies the user ID (recommended but not required).

This is the **url add** command syntax for group calendar (do not use a period (.) or other special characters in the *instance* name):

```
url add groupcalendar:instance "description" "ldapur1" "options"
```

To set up group calendar, follow these steps at the command line:

1. Enter **Url Add** so group calendar users can find each other, possibly on different servers. If you choose, replace *User Lookup* with a custom name for this lookup. Note, this URL uses “127.0.0.1” (“localhost”):

```
hostname.com> url add groupcalendar:userlookup "User
Lookup""ldap://127.0.0.1:389/
miDomainName=primary,ou=domains,o=miratop?cn,miloginid?sub?(&(|
(objectclass=person)(objectclass=inetorgperson)(objectclass=mir
apointUser))(|(uid=$(cn)*)(miloginid=$(cn)*)(sn=$(cn)*)(givenna
me=$(cn)*)))" "(uidalias=miloginid)"
OK Completed
```

Note: The system LDIF uses **miloginid** to identify the user, not **uid**. In fact, the LDIF does not contain a uid at all. For this reason, the search query must be defined to return miloginid instead of uid (this is the **?cn,miloginid?** portion of the URL). Since Calendar assumes

that **uid** is the attribute used to uniquely identify users, this URL must tell it to use **miloginid** instead (this is the **(uidalias=miloginid)** portion of the URL).

2. Enter **Url Add** again so calendar users can locate resourcegroups, possibly on different servers. If you choose, replace *Group Lookup* with a custom name for this lookup. Note, this URL uses "127.0.0.1" ("localhost"):

```
hostname.com> url add groupcalendar:grouplookup "Group Lookup"
"ldap://127.0.0.1:389/
miDomainName=primary,ou=domains,o=miratop?mail?sub?(mail=*(cn)
*)" "(cnalias=mail)"
```

If you need to re-enter the **Url Add** command, first delete the previous one with this command where *name* is the name of the url you are deleting and *instance* is the particular instance you are deleting:

```
hostname.com> url delete "name:instance"
OK Completed
```

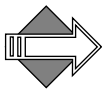
For example, this command...

```
hostname.com> url delete groupcalendar:userlookup
OK Completed
```

...deletes the URL you added in step [1](#), above.

3. Set the Group Calendar mode to LDAP (or ALL; ALL looks in LDAP first and then locally for users), enter this command:

```
hostname.com> calendar set groupcalmode ALL
OK Completed
```



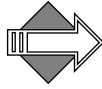
The **userlookup** query (step [1](#)) describes a user URL mapping for group calendar, while the **grouplookup** query (step [2](#)) describes a group URL mapping. In the examples above, **User Lookup** and **Group Lookup** are just arbitrary labels for the class instance. The **ldap://** URLs are very complicated, being built up by substituted components into a DN.

Continue Group Calendar setup using the Administration Suite pages (<http://hostname.com/miradmin>); follow these steps.

4. Go to **Home > Domains > Calendar > Resources**. In the **Resourcegroup name** option, enter a name for the distribution list that will hold all of your calendar resources; for example,

“resourceList”. Select **LDAP** as the database to write to. Click **Set Group Name**.

Additional options display that enable you to set actual resources. This entry becomes an **LDAP** mailgroup (if **Local** is selected, it becomes a distribution list).



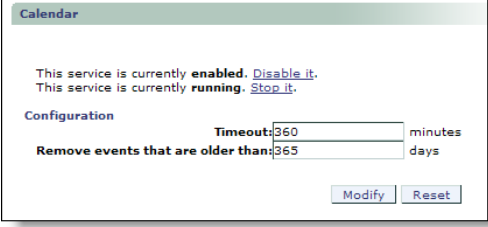
Group Calendar setup is domain specific, later, when you have created delegated domains, you will select the delegated domain on the **Domains > Administration** page before doing this step.

5. Specify the following for each resource (meeting rooms, equipment such as projectors, and so forth) that you want to make available for calendar users. This information is added to your LDAP database.
 - ❖ **Fullname:** The name of the resource as you want it to appear in the **Choose a Resource** drop-down list of the **Schedules** tab for calendar new events.
 - ❖ **Userid:** Since this resource is treated as a user by the system, enter an identifier.
 - ❖ **Password:** Enter a password for the resource.
 - ❖ **Allow any user to view what events are booked with this resource** (default is enabled): This sets permissions so that all calendar users can see when the resource is available.
6. Click **Add Resource**.

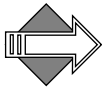
Result: The resource entries are made available in the calendar **Schedules** tab **Choose a Resource** drop-down list; lookups are sent to your LDAP database.

Complete Group Calendar setup by enabling the Calendar service to allow users to schedule events and share calendar information via WebCal. Idle WebCal connections will be disconnected when the idle timeout is reached.

7. Go to **Home > System > Services > Calendar**. If needed, click **Enable it** and **Start it**. If desired, change the idle **Timeout**; the default is 360 minutes.



8. If desired, change the **Remove events that are older than** option; the default is 365 days. Click **Modify** to save your changes.



There are many Calendar defaults that you can set on a per-domain basis using the **Domains** menu **Calendar** pages for a selected domain. for full details on these defaults, see [“Configuring Calendar Options for Domains” on page 274](#) in the Administration Tasks part of this book.

Adding the Address Book URL

Use the **url add** command to add an address book URL that points to the addressbook directory service you are adding.

This is the **url add** command syntax for **addrbook** (do not use a period (.) or other special characters in the *instance* name):

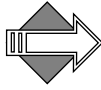
```
url add "addrbook:instance" "description" "ldapurl" "options"
```

This is an example for use with Internal LDAP and the Mirapoint schema plus a filter needed for Group Calendar; the two variables, *primary* and *Primary Directory* could be changed. You can use this example URL, modified as needed.

```
hostname.com> url add "addrbook:primary" "Primary Directory"
"ldap://127.0.0.1:389/
miDomainName=primary,ou=domains,o=miratop??sub?(&(objectclass=m
irapointmailuser)(|(sn=$(cn))(givenname=$(cn))(cn=$(cn))(mail=$
(mail)*)(maillocaladdress=$(mail)))" ""
OK Completed
```

The address book directory service is domain sensitive; the command as given adds a directory service to the primary domain, but not any delegated domains. To add the address book URL for a delegated domain, and for more examples of the **url add addrbook** command, see

[“Adding Directory Services to Delegated Domains” on page 286](#) in the Administration Tasks part of this book.



Because this deployment is an all-in-one, the address book directory service you just added points to the localhost and contains no contacts. To add contacts, use the **Add User** page; details are provided in [“Managing User Accounts” on page 288](#) in the Administration Tasks part of this book.

Limiting TCP Connections

In a denial-of-service attack, systems are overwhelmed by requests from a small set of sources, slowing down response time and reducing bandwidth for bonafide users. You can deter denial of service attacks by limiting the number of TCP connections and the connection rate.

To do this, you enable the **LimitTcpConnectionCount** and **LimitTcpConnectionRate** options via the CLI; enter these commands at the command line:

```
hostname.com> Netif Set LimitTcpConnectCount "" On
OK Completed
hostname.com> Netif Set LimitTcpConnectRate "" On
OK Completed
```

By default, the TCP connection count limit is 50 and the connection rate limit is 400 every ten seconds. You can also specify your own limits and use the **Netif AddTrustedIP** command to exempt selected hosts from the TCP limits; for more information see the CLI online **Help About Netif**.

This completes command line configurations. Return now to your Administration Suite (<http://hostname.com/miradmin>) browser and complete your all-in-one configuration by following the remaining procedures.

Setting Up Autoprovisioning of Users

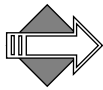
Autoprovisioning of users can be performed by the Message Server when it can connect to an external LDAP server, or if it has the service running internally.

Autoprovisioning automatically creates a new user account and inbox (mailbox folder), possibly with disk quota, from the LDAP server database if it finds sufficiently detailed records. Autoprovisioning does not create subfolders, nor can it set custom access control lists.

Six queries are defined for autoprovisioning: **publishedName**, **mailhost**, **routingAddr**, **loginID**, **quota**, and **fullname**. See [Table 5 on page 57](#) for query specifications. See [Table 6 on page 58](#) for the mapping of query specifications to LDAP attributes.

To autoprovision users, follow these steps:

1. Enable LDAP autoprovisioning with the **Ldap Set** command:
Ldap Set Autoprovisioning On
2. Verify that your LDAP database contains entries that specify values for the attributes detailed in [Table 5 on page 57](#).
3. Construct the required queries as described in [“Setting Up Queries” on page 61](#).



More information on autoprovisioning, including how to transfer existing records, is provided in [Bulk Provisioning Users](#) in the Administration Tasks part of this book.

Configuring WebMail

Enable the WebMail service to allow users to retrieve and manage their messages from a Web browser. When the **External Mail** feature is enabled, users can download POP3 mail from other clients. Idle WebMail connections will be disconnected when the idle timeout is reached.



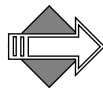
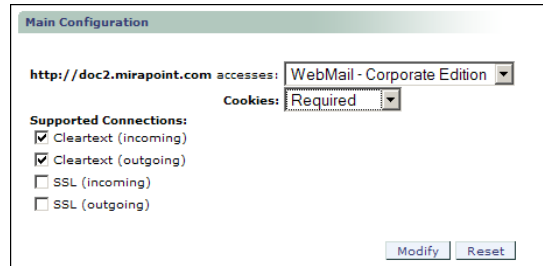
Mirapoint recommends using IMAP and WebMail in an all-in-one deployment.

To configure the WebMail service, follow these steps.

1. Go to **Home > System > Services > HTTP > Main Configuration** and set WebMail to be the default HTTP access for your users by choosing **WebMail (Standard Edition)** or **WebMail (Corporate**

Edition) from the drop-down list for the **http://<hostname.domain.com>** accesses option.

Important Note!: An error may display if you select **WebMail—Corporate Edition**, “Invalid root value ‘enterpriseui’”. If you get this error, go to **Home > System > Services > WebMail** and disable/stop and then enable/start the Corporate Edition service. You can then return to **Home > System > Services > HTTP > Main Configuration** and select **WebMail—Corporate Edition** as your default HTTP access.



Once the default access is set to WebMail, to access the Administration Suite go to **http://hostname/miradmin**, where *hostname* is your appliance’s fully-qualified domain name.

2. Also on the **HTTP > Main Configuration** page, protect WebMail session IDs by selecting **Required** for the **Cookies** option. This prevents users from unintentionally giving access to their mail by copying and pasting their session ID into an e-mail.

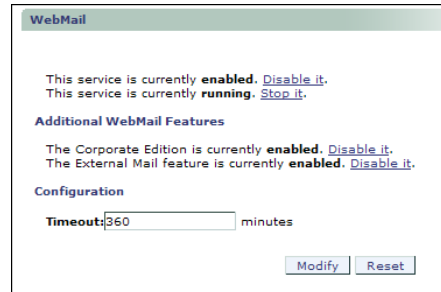


For optimum network security, require cookies for all HTTP sessions. This is not the default because some users believe cookies compromise privacy and they disable them in their web browsers.

3. If you have SSL licensed, select the **Supported Connections** options including **SSL (incoming)**; you can leave the **SSL (outgoing)** option deselected.

When you are done, click **Modify** to save your changes.

4. Go to **Home > System > Services > WebMail**. If desired, change the idle **Timeout**; the default is 360 minutes. Click **Modify** to save your changes.



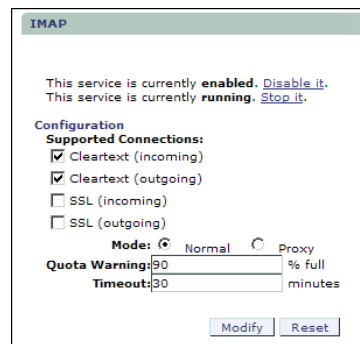
5. If the WebMail service is disabled, click **Enable it**. If the service is stopped, click **Start it**.

Configuring IMAP

Enable the IMAP service to allow users to retrieve and manage their messages using the Internet Message Access Protocol version 4 (IMAP4). Using IMAP, users can access messages stored on the server without having to download each one.

In an all-in-one configuration, the IMAP service provides access to folders on the local host. IMAP supports both un-encrypted and encrypted (SSL) connections. You can configure the quota warning and idle timeout as needed for your site. To configure IMAP support:

1. Go to **Home > System > Services > IMAP**.



2. Select the **SSL (incoming)** option to allow SSL connections.

3. Leave the **Mode: Normal** default.
4. If desired, change the **Quota Warning** limit. When this folder storage limit is exceeded, the IMAP service issues warnings to clients that open the folder. For example, if the limit is 95 percent and a particular folder has a quota of 100 MB, the IMAP service begins issuing warnings for the folder when it exceeds 95 MB.
5. If desired, change the idle **Timeout**; default is 30 minutes. Idle IMAP connections are disconnected when the timeout is reached.
Click **Modify** to save your changes.
6. If the IMAP service is disabled, click **Enable it**. If the service is stopped, click **Start it**.

Configuring SMTP

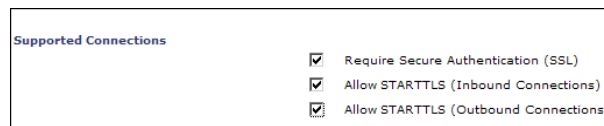
To configure SMTP service options, follow these steps. **Note:** Use the defaults for options not mentioned in this procedure.

1. Go to **Home > System > Services > SMTP > Main Configuration**. Do not enable or start the service until the end of this procedure.



Mirapoint recommends the use of **STARTTLS** and **Secure Authentication** to protect the transmission of passwords across the network.

2. In the **Supported Connections** area, select the following options:
 - ❖ **Require Secure Authentication (SSL):** All communications must be authenticated through the AUTH login (SMTP AUTH RFC 2554).
 - ❖ **Allow STARTTLS (Inbound Connections):** Encrypted incoming connections are supported.
 - ❖ **Allow STARTTLS (Outbound Connections):** Outgoing connections are encrypted.

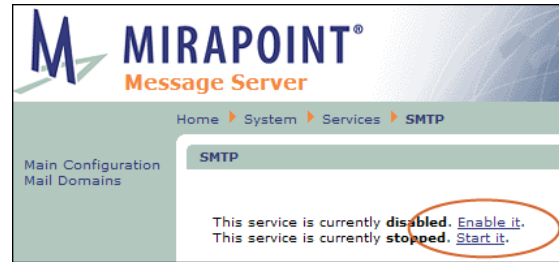


3. In the **Inbound Connection Settings** area, select the **Rewrite From address based on authentication** option and leave the rest of the options set to the defaults. The **Rewrite address based on authentication** option specifies whether sender addresses in message envelopes and **From** headers are rewritten using the login name specified through SMTP authentication. If the connecting system does not authenticate, this setting has no effect.

Inbound Connection Settings	
TCP Port:	25
Maximum Message Size:	31457280 (bytes)
Maximum Recipients per message:	50000
Maximum Messages per connection:	0
Add "For" information to Received header:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Reject Messages for Unknown Recipients:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Reject Messages from Unknown Senders:	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Rewrite From address based on authentication:	<input checked="" type="radio"/> Yes <input type="radio"/> No
FastPath™	Enabled

4. Accept the default settings in these areas of the page:
 - ❖ **Outbound Connection Settings**
 - ❖ **SMTP Authentication Settings**
 - ❖ **Mail Queue Settings**
5. In the **Routing Settings** area, select these options:
 - ❖ **Use LDAP Routing: For All Messages:** Specifies that inbound and outbound messages are routed through LDAP. This allows the system to use the internal LDAP directory that you set up.

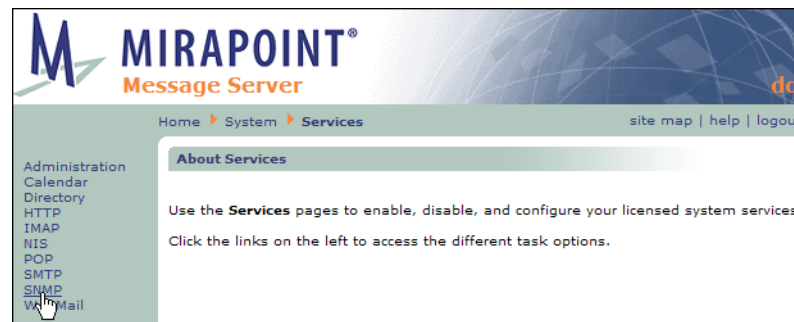
Accept the defaults for the other routing options.
6. Accept the defaults in the **Masquerade Settings** area.
7. Click **Modify** at the bottom of the **SMTP > Main Configuration** page to save your changes.
8. Click **SMTP** in the top navigation bar to return to the main SMTP service page. If the service is disabled, click **Enable it**. If the service is stopped, click **Start it**.



Enabling and Starting Services

Enabled services start automatically when the system boots. The **Administration** and **HTTP** services are always enabled and started. Services you choose not to start will not be available.

1. Go to **Home > System > Services**. Click on the name of a service in the page menu to go to that service's page. Note: Only licensed services display page links. On the main page for each service, if the service is disabled, click **Enable it**. If the service is stopped, click **Start it**.



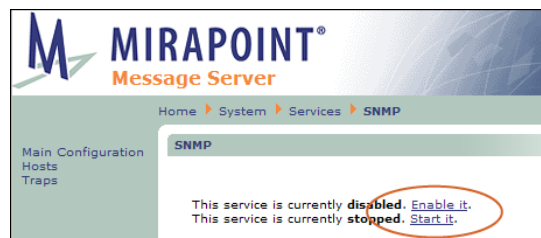
2. At this point, most services have already been enabled and started, the following might still need attention.
 - ❖ **NDMP**—The NDMP service enables backups using the Network Data Management Protocol (NDMP). Your choices include the following:
 - Bakbone: Defaults to version 4

- Legato: Defaults to version 2
- Tivoli: Defaults to version 3
- Veritas: Defaults to version 2

You can read more about these Data Management Applications (DMAs) in the Knowledge Base article #287 on the [Mirapoint Support site](#) (login required).

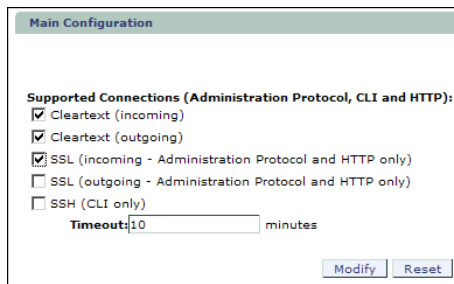
- ❖ **SNMP**–The Simple Network Management Protocol (SNMP) service allows consoles to monitor selected information about Mirapoint systems. This only applies if you have an SNMP management station.

To learn more about SNMP see [“Monitoring External Systems via SNMP” on page 253](#) in the Administration Tasks part of this book.



Resetting the Administration Timeout

Setting the timeout to 60 minutes is recommended for the configuration procedures; however, once you’re done, you’ll want to return to the **Home > System > Services > Administration > Main Configuration** page and set the **Timeout** back to **10 minutes** for security. Click **Modify** to save your changes.



Verifying the All-In-One Setup

Now that you've finished the initial setup and configured your directory service, you need to verify that everything is working properly. To do this, complete the following procedures.

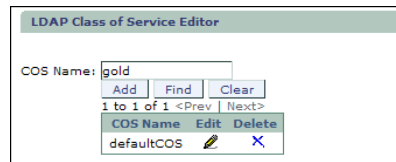
Refresh the Administration Suite

Before you verify your set up, logout of the Administration Suite and then log back in (as administrator). This refreshes the settings and validates the configuration changes you have made.

Create a Class Of Service

Create a Class of Service that can be applied to the users you create.

1. Go to **Home > Class of Service**, enter a name for the COS. For this test, enter **gold** as the **COS Name**. Click **Add**.



2. Click the **Edit** icon for the **gold** COS you just added to open the **COS Editor** page. For this test, you can leave the **Folder Quota** option empty, select these services for the COS:
 - ❖ Calendar
 - ❖ Corporate Edition
 - ❖ Group Calendar
 - ❖ IMAP
 - ❖ WebMail

Click **Add Service**.

3. Click **Done** at the bottom of the page to return to the main **Class of Service** page.

Create User Accounts

To create two user accounts for testing, follow these steps.

1. Go to **Home > Domains > Users**. At the bottom left of the page, you will see an indicator that you are in the **<primary>** domain.
2. To create the first test account, enter **user1** in the **User Name** and **Password** options, select the **gold** Class of Service that you created, and click **Add User**.

- To create a second test account, enter *user2* in the User Name and Password options, select the **gold** Class of Service that you created, and click Add User.

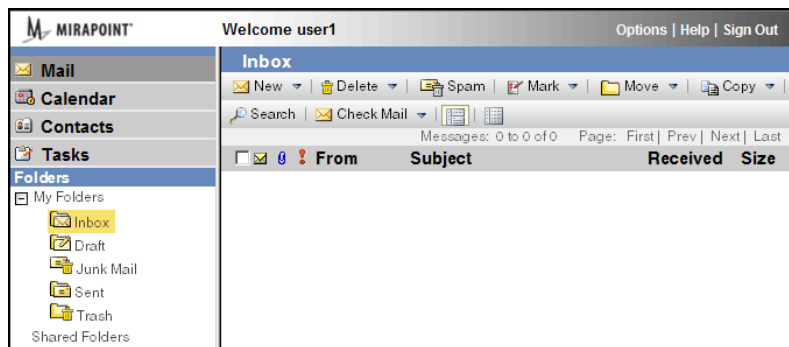
Send a Test Message

To send a test message:

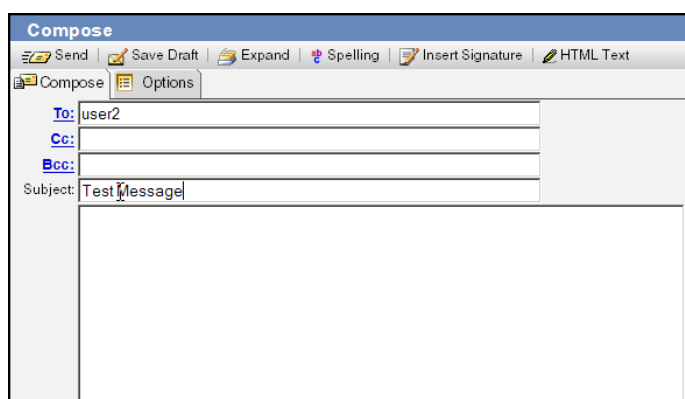
- Open your Message Server's URL in a Web browser; for example, <http://hostname.domain.com>.
- Log into WebMail with the **user1** username and password. Note: In the following examples, Corporate Edition WebMail is shown.



- Click **New** to create and send a test message.

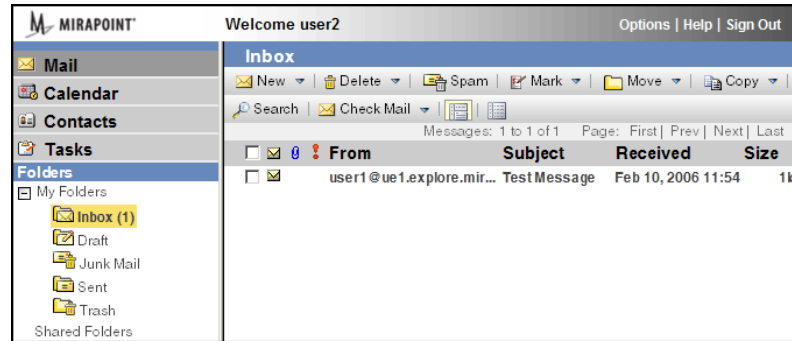


4. Address the message to `user2@hostname.domain.com` and click **Send**.



Receive a Test Message

To receive the test message, log into WebMail with the `user2` username and password. The test message should be listed in user2's Inbox:



If the message is delivered, your Message Server is operating normally. If either user does not receive the test message, refer to “*Troubleshooting*” on page 105.

Verify the Address Book Directory Service

The directory service you added was at the primary domain level. To verify that it was added correctly, follow these steps.

1. Log into WebMail with the **user1** username and password.
2. Go to **Contacts > Tools > Find Directory Service Contacts** (Corporate Edition), or **Address Book > Find Contacts** (Standard Edition).
3. Select from the **Directory Service** (Corporate Edition) or **Find in** (Standard Edition) drop-down list option the directory service you added. If you are using Standard Edition WebMail, click **Select** to use that directory service.
4. Enter an asterisk (*) in the **Name** option, and click **Find**.

If the page displays the directory service contacts, your address book is operating normally.

5. Send a user in the address book a test message (if you add your own company’s address book, you should be an available entry). Then log in as that user to verify that the test message was received.

Create a Calendar Event

To test that Group Calendar is properly set up, create an event.

1. Log into WebMail with the **user1** username and password. Click the **Calendar** link.
2. Click **New > Event**. Title the event **test** and select a time for the event.
3. Go to the **Schedules** tab and add **user2** and your address book user (if you add your own company's address book, you should be an available entry). Add the resource that you configured.
4. Click **Add Event**.
5. Log in as **user2** and verify that you got the event invitation.
6. Log in as your address book user and verify that you got the event invitation.

Optional Configuration Tasks

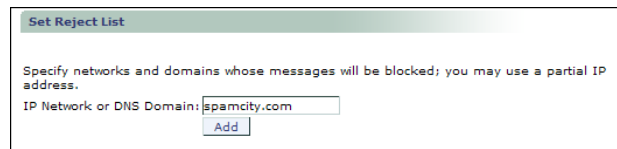
The following sections describe optional configuration tasks that we recommended you perform when you've completed the basic configuration of your Message Server.

Adding Networks or Domains to the Reject List

You can block connections from domains or networks that are known sources of spam or network attacks. The reject list can include specific domain names, IP addresses, or partial IP addresses. For example, if you specify 10.127.1, SMTP service rejects all e-mail from 10.127.1.1 through 10.127.1.128 but accepts e-mail from 10.127.2.1 and so on. To block all mail servers at a fictitious domain called *spamCity.com*,

you could specify the DNS domain name **spamCity.com**. To add a domain or IP address to the reject list:

1. Go to the **Anti-Spam > Reject List** page.



2. Enter the IP Network or domain name. Click the **Add** button.

Setting the HTTP Default Access

The appliance's HTTP default access is initially configured to display the Administration Suite to facilitate the setup process. You need to change the HTTP default access to load the WebMail interface so your users are automatically directed to WebMail when they load the appliance's URL. You did this in the [“Configuring WebMail” on page 91](#) procedure, but you might want to change the HTTP default access, follow these steps.

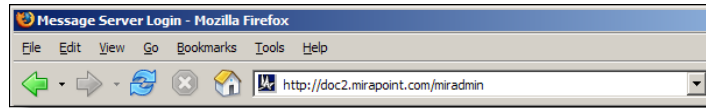
1. Go to **Home > System > Services > HTTP > Main Configuration**.



2. Select **WebMail - Corporate Edition** or **WebMail - Standard Edition** from the drop down list and click the **Modify** button to configure your HTTP default access to point to the WebMail Corporate Edition interface.

Note: To access the administration interface after you've changed the HTTP default access, append

`/miradmin` to the URL. For example, `http://hostname.yourdomain.com/miradmin`. Bookmark this page for easy access to the Administration Suite as the default access will now open WebMail.



Configuring Safe Lists and Blocked Lists

As a message travels through the system, the software first considers Allowed Senders lists, which are sender **From** addresses that should always be delivered. Next the software considers allowed recipients lists, called Allowed Mailing Lists, which are recipient **To** addresses that should always be delivered. Finally the software considers Blocked Senders lists, sender **From** addresses that should never be delivered.

Procedures for setting up these lists are given in the Administration Tasks part of this book; see [“Setting the Allowed Senders List” on page 425](#), [“Setting the Blocked Senders List” on page 428](#), and [“Setting the Allowed Mailing Lists List” on page 431](#). These are tasks that will need to be done regularly as your system develops.

Troubleshooting

This section provides some troubleshooting tips.

LDAP Errors

If you get an Invalid DN error when attempting to add a user through the LDAP-enabled **Add User** page, the base DN specified when you set the LDAP query specifications is incorrect. To see what is currently configured, you can use the LDAP `listaccess` and `getaccess` commands. Check your base DN and reset the query specification.

If you get an Invalid Credentials error, the user name and/or password specified when you added the LDAP access profile is not correct. Check your authentication information and delete and reset the access profile.

If you get an “Bad Search Filter” error, one of your LDAP setqueries was poorly defined. You might have a typo in one of the lines. Try re-entering the setqueries; copy and paste from the online file at <http://www.mirapoint.com/support/allinone.html> if you can.



If an LDAP-related license expires, the LDAP settings will revert to the default once an updated license is applied. Please monitor your system license expiration dates and backup your system configuration to avoid unplanned downtime.

Test Message Send Fails

If you cannot send test messages between user accounts on your Message Server, check the following:

1. Verify that the domain name server(s) you have configured are working:
 - a. Go to the Administration Suite Set Interface page, **Home > System > Network > Interface**.
 - b. Enter a domain name or IP address of an Internet server such as *mirapoint.com* in the **Domain Name/IP** field.

The screenshot shows the 'Set Interface' web page. The 'Set Domain Name Servers' section has a table with one entry: '63.107.133.194'. The 'Test Domain Name Server' section has 'mirapoint.com' in the 'Domain Name/IP' field, circled in red. The 'DNS Server' dropdown is set to 'ANY'.

- c. Click the **Lookup** button. If the lookup fails, you need to configure a valid DNS server. (Have at least two DNS servers

configured in case the first one is unavailable.) To configure an additional DNS server, enter its IP address or URL in the **DNS Server** option and click the **Add** button.

2. Verify that your Message Server services are up and running:
 - a. Go **System > Services**.
 - b. Make sure each service listed in the page menu is enabled and running.



If you continue to have problems, contact Mirapoint Technical Support for assistance at support@mirapoint.com.

Next Steps

Now that you have your Message Server up and running, there are a number of additional features you can configure according to your site requirements:

- ◆ **Schedule Software Updates:** In addition to antivirus and antispam updates, you can schedule MOS update checks through the Administration Suite **System > Utilities > Updates > Update Check** page. For more information, see the Administration Suite online help.
- ◆ **Configure COS Message Undelete and Message Expiration features:** These COS features must be configured at the command line. See [“Setting Up Message Undelete” on page 327](#) and [“Setting Up Message Expiration” on page 328](#) in the Administration Tasks part of this book.

- ◆ **Set up System Backups:** Mirapoint supports a number of different solutions for backing up and restoring user data. For more information, see [“Backup and Restore Tasks” on page 519](#) in the Administration Tasks part of this book.
- ◆ **Quick-Brand Your Site:** You can customize the appearance of the WebMail and WebCal user interfaces by changing the HTML style sheets and providing custom images. For more information about branding your site, see the *Mirapoint Administrator’s Branding Guide*.
- ◆ **Set up SynQ for Outlook Users:** If you have users who maintain their calendars in Microsoft Outlook, they can use SynQ to synchronize with WebCal. For more information about installing and using SynQ, see “Synching Your Calendar with Other Calendars” in the *WebMail/WebCal Corporate Edition User Guide*.

For information about migrating data from another Message Server, see the Mirapoint Support Knowledge Base at <http://support.mirapoint.com> or contact Mirapoint Technical Support at support@mirapoint.com.

RazorGate Security Deployment for Exchange

In this deployment, two RazorGate appliances perform message screening and message routing for an Exchange server using Microsoft Active Directory. For more information on this deployment, refer to the *Mirapoint Administrator's Planning Guide*.

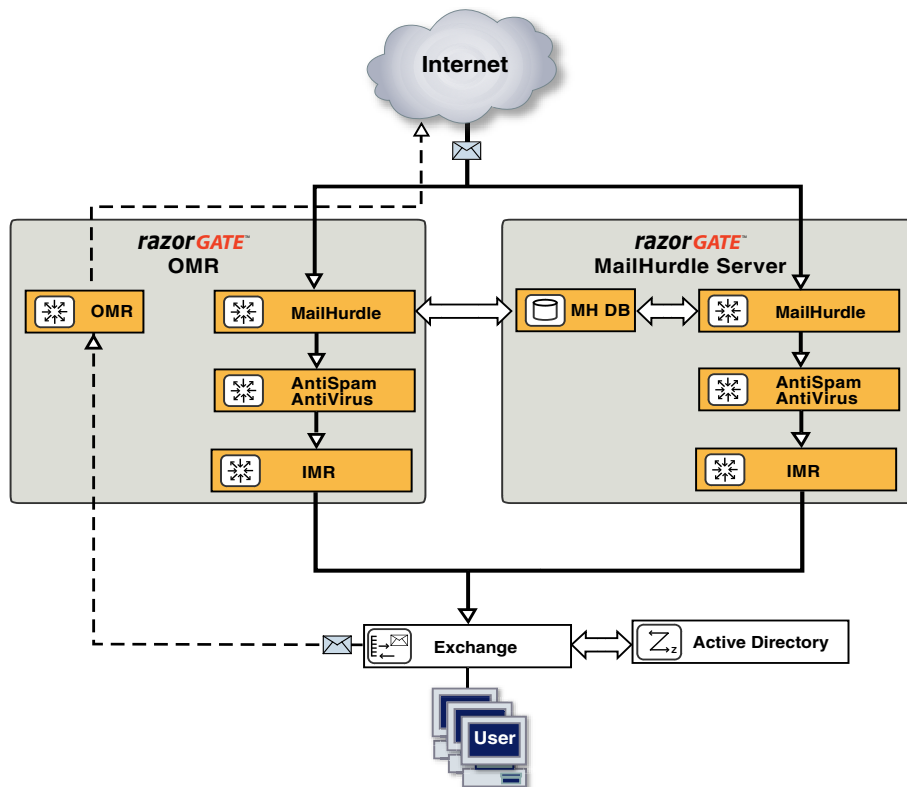


Figure 3 RazorGates Security Deployment Scenario

Before You Begin

Before you begin configuring your RazorGate appliances to secure an Exchange server, make sure that you have read Chapter 1, “All Deployments Start Here and performed the tasks described, including:

- ◆ [Pre-Configuration Checklist](#) (as applicable):
 - ❖ Domain Name System (DNS) servers configured
 - ❖ Lightweight Directory Access Protocol (LDAP) set up
 - ❖ Licenses obtained (licenses are implementation specific)
 - ❖ Backup requirements defined
 - ❖ Secure Sockets Layer (SSL) certificates obtained
- ◆ [Prerequisites](#):
 - ❖ Hardware installation (connected to the Internet)
 - ❖ DNS server database records
 - ❖ Basic system setup (described on the Quick Start Setup card shipped with your appliance)
- ◆ [Initial Setup Common to All Deployments](#):
 - ❖ Secure administrator account set
 - ❖ Appliance clock set
 - ❖ Network settings verified, DNS server(s) added
 - ❖ Licenses installed
 - ❖ Service Reporting options set
 - ❖ Software updates obtained
 - ❖ Administrator access restricted
 - ❖ SSL security for administrator logins set

Information Required for this Configuration

You need the following information to configure your RazorGates to secure an Exchange server, as documented here:

- ◆ A list of senders and recipients (IP addresses, domain names, and email addresses) that you want to **safelist** by adding to your Allowed Senders/Allowed Mailing Lists. For example, vendors you do business with would go on the **Allowed Senders** list, and your

internal helpdesk mailing list would go on the **Allowed Mailing List**. Safelisting senders and recipients ensures that messages sent by or to those addresses is never subject to antispam delays. You will also set priority on the safe lists to override antispam scanning.

- ◆ A list of RBL (Realtime Blackhole List) servers. You can learn more about this through Wikipedia: <http://en.wikipedia.org/wiki/DNSBL>.
- ◆ The IP address and FQDN of the RazorGates, and Exchange server, plus all Exchange mail domain names.
- ◆ The hostname, port number, and baseDN of your Active Directory.
- ◆ IP address for all DNS servers you want to add.
- ◆ **Licenses**—The licenses for this deployment are listed below. Verifying installed licenses and installing licenses is described in step 5 of [“Completing the Setup Wizard” on page 39](#).
 - ❖ Default licenses shipped with RazorGate:
 - User Limit: 20
 - LDAP Routing
 - MailHurdle
 - WebMail: 20
 - POP: 20
 - IMAP: 20
 - RazorGate
 - ❖ Optional licenses (an antivirus license and an antispam license are usually included):
 - Sophos (signature-based) virus filtering
 - F-Secure (signature-based) virus filtering
 - RAPID (predictive-based) virus filtering
 - Antispam (Principal Edition) or Antispam SE (Signature Edition)
 - SSL (Secure Sockets Layer)



Checking your licenses is described below on page 113.

Mirapoint recommends at least one signature-based antivirus and RAPID. Please Note: RAPID antivirus must be used in conjunction with a signature-based antivirus engine (Sophos or F-Secure).

The two Antispam licenses are mutually exclusive.

Configuring Two RazorGates to Secure Exchange

You configure two RazorGates to perform security screening and routing; having two RazorGates is a failover safety measure. Configuring two RazorGates in front of Exchange using Active Directory involves the following tasks:

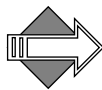
- ◆ Accessing the Administration Suite
- ◆ Checking for Licenses
- ◆ Setting the Administration Timeout
- ◆ Configuring MailHurdle
- ◆ Configuring Anti-Virus Scanning
- ◆ Configuring Anti-Spam Scanning
- ◆ Configuring Inbound Routing—RGs Security Deployment
- ◆ Configuring Outbound Routing—RGs Securing Exchange
- ◆ Enabling and Starting Services
- ◆ Resetting the Administration Timeout

Accessing the Administration Suite

You use the Administration Suite to perform most RazorGate configuration tasks. To access the Administration Suite from a web browser, go to **http://hostname/miradmin**, where *hostname* is your appliance's fully-qualified domain name.

Open two web browser windows and log in as administrator on both RazorGate appliances so you can configure them at the same time.

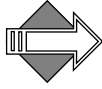
The Administration Suite displays function links at the left and a navigation bar at the top that tracks your current location within the page hierarchy. The **Site Map** link (in the upper right corner) displays links to most pages.



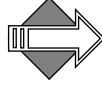
If you are accessing the Administration Suite for the first time, the Setup Wizard displays. You need to use the Setup Wizard to perform the basic configuration tasks described in [“Completing the Setup Wizard” on page 39](#) before continuing.

Checking for Licenses

To verify that you have the licenses you need for this configuration, go to **Home > System > Utilities > License** page to see all the license keys available to you.



The MailHurdle license does not display; it is part of the Anti-Spam license.



LDAP routing requires a license. This license is a prerequisite for many other licensed features including SMTP directory-based routing, IMAP or POP proxying, Group Calendar, and multi-tier shared folders.

Setting the Administration Timeout

You'll want to change the default Administration Suite timeout from 10 minutes to at least 60 minutes while you are configuring the RazorGates.

Go to **Home > System > Services > Administration > Main Configuration** page and change the **Timeout** to at least 60 minutes. You'll want to change it back to 10 minutes once you are done.

Main Configuration

Supported Connections (Administration Protocol, CLI and HTTP):

- Cleartext (incoming)
- Cleartext (outgoing)
- SSL (incoming - Administration Protocol and HTTP only)
- SSL (outgoing - Administration Protocol and HTTP only)
- SSH (CLI only)

Timeout: minutes

Repeat on the other RazorGate.

Configuring Anti-Virus Scanning

Anti-Virus scanning is a licensed feature usually set at the factory.

There are three antivirus scanners you can license and configure; two, **F-Secure** and **Sophos**, are **signature-based**, meaning they use databases of known viruses to categorize messages as containing a virus. The third, **RAPID**, is **predictive-based**, meaning it uses a database of heuristics to categorize messages as *potentially* containing viruses. Because RAPID categorizes messages as containing potential viruses, rather than known viruses, its only available action is quarantine. Those RAPID-quarantined messages are automatically released after a configurable amount of time, allowing one of the signature-based antivirus engines to re-scan the messages and ensure that viruses are caught.



Mirapoint recommends configuring at least one signature-based antivirus scanner and the RAPID antivirus scanner for this deployment. Please Note: RAPID antivirus must be used in conjunction with a signature-based antivirus; used alone it is ineffective in preventing virus attacks. You can run all three antivirus engines in this deployment, one or both signature-based engine plus RAPID on each RazorGate, if you have all three licenses.

Configuring F-Secure or Sophos Anti-Virus

To configure Sophos and/or F-Secure Anti-Virus, follow these steps on each RazorGate. You need to repeat the steps (on each RazorGate) if you are going to use both antivirus engines.

1. Go to **Home > Anti-Virus**, click the link at left for the scanner to be configured, F-Secure or Sophos (only licensed options display). The main page for that virus scanner opens. Click **Configuration**.



2. On the **Anti-Virus > virus scanner > Configuration** page, if the scanner is disabled, click the **Enable It** button. Accept the default **Auto-Clean (Delete)** option. If you want to archive caught viruses, enter an e-mail address in the **Anti-Virus Quarantine** field.



Messages sent to the **Anti-Virus Quarantine** contain live viruses and should not be opened on a desktop computer.

If you select the **Auto Clean (Ignore)** or **Ignore** options, infected messages will be delivered to your users.

Anti-Virus Configuration

The Anti-Virus utility scans all incoming e-mail messages for viruses.

SOPHOS
SOPHOS ANTI-VIR

Anti-Virus is currently enabled.

Select one of these Anti-Virus Actions

Action	Description
<input checked="" type="radio"/> Auto Clean (Delete)	Auto Clean if possible. Otherwise, delete the infected attachment.
<input type="radio"/> Auto Clean (Ignore)	Auto Clean if possible. Otherwise, ignore the virus and process the message normally.
<input type="radio"/> Delete	Delete the infected attachment.
<input type="radio"/> Ignore	Ignore the virus and process the message normally.

Anti-Virus Quarantine

A copy of the original infected message can be quarantined for administrative purposes.
Note that these mail messages will contain live viruses.

E-mail address:

If you make changes, click **Apply** to save your changes.
Repeat on the other RazorGate (if needed).

3. Do not modify the **Anti-Virus > virus scanner > Notifications** page. The defaults are appropriate for this deployment.

4. On the **Anti-Virus > virus scanner > Updates** page, change the default hourly time if it is not good for your site. If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**. When you are done, click **Apply** to save your changes. Repeat on the other RazorGate.

Automatic Update and Proxy Server

Automatically update:

*Hourly: :59 (on the minute)

Daily: 00:00 (on the hour)

Weekly: Sunday (day of week)

Monthly: 1 (on the day)

*Strongly Recommended

Use Proxy Server:

Host: _____

Port: _____

User ID: _____

Password: _____

Apply Update Now

Configuring RAPID Anti-Virus

RAPID Anti-Virus is a licensed feature; it uses a **predictive-based** methodology that immediately categorizes suspect mail as spam based on heuristics maintained in a rulegroup. It must be used in conjunction with a signature-based antispam scanner, F-Secure or Sophos.

There are some file extensions that always trigger the RAPID antivirus quarantine action; for details see [“Modifying Predictive-based \(RAPID\) Anti-Virus” on page 409](#) in the Administration Tasks part of this book.

To configure RAPID Anti-Virus, follow these steps on each RazorGate.

1. Go to **Home > Anti-Virus > RAPID > Configuration**, if the scanner is disabled, click the **Enable It** button.

Anti-Virus is currently **enabled**.

Anti-Virus Quarantine
 All e-mail messages potentially containing a virus are quarantined automatically.
 All other e-mail messages will be delivered to the recipient(s).

Note that these mail messages may contain live viruses.

Quarantine folder: user.UserName[Folder.Folder...]

Note: UserName must have quarantine administrator role.

2. Accept the default **Quarantine folder** address, a subfolder of the **Administrator** account. Later, you can set any valid `user.username.subfolder` e-mail address for an account with the Quarantine Administrator role. For more information, see [“How Antivirus Quarantine Works” on page 398](#), and [“Using Security Quarantine” on page 441](#) in the Administration Tasks part of this book.

When you are done, click **Apply** to save your changes.

Repeat on the other RazorGate.

Afterwards, all messages potentially containing a virus are automatically quarantined for 8 hours to the specified email address; other messages are delivered normally. The auto-release time can be modified using the CLI; see **Help About Antivirus**.

3. Go to **Anti-Virus > RAPID > Notifications** and modify the format of virus notifications as appropriate. Whereas notifications for F-Secure or Sophos-caught viruses are not really needed, because those are known viruses, notifications for RAPID quarantined potential viruses is very important. Users should be made aware that a message is quarantined for a potential virus.



In the **To** option, add the appropriate quarantine administrator email addresses (or just **Administrator** to use the default). The specified administrators are notified when messages are quarantined by RAPID. Use commas (,) as separators to enter multiple email addresses.

When you are done, click **Apply** to save your changes.

Send this notification to the message recipient(s) when a potential virus is found.

This notification is currently disabled.

From:

Subject:

Message: Your mail from \${sender} with subject \${subject} has been quarantined and may have a virus attached to it. Please contact your system administrator if you want this message to be released or re-scanned.

Unicode (UTF-8)

\$(sender)=Sender \$(subject)=Subject \$(action)=Action
\$(attachments)=List of attachments \$(domain)=Current Domain
\$(filtername)=Filter name that triggered the notification

Repeat on the other RazorGate.

4. Go to **Anti-Virus > RAPID > Updates** and change the default hourly time if this is not good for your site.

If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**.

When you are done, click **Apply** to save your changes.

Repeat on the other RazorGate.

Configuring MailHurdle

Mirapoint MailHurdle blocks spam by screening messages from unrecognized sources. When a message is received from an unrecognized source, MailHurdle temporarily fails the message and sends a **retry later** code. A properly-configured mail server automatically re-sends the message, which is then accepted; however, most spam mailers pay no attention to this retry code.

To configure MailHurdle to ensure the timely delivery of valid messages, follow these steps on each RazorGate appliance.

1. Go to **Home > Anti-Spam > Allowed Senders**. For the default **Destination Domain** option, select **Any**. Add domains and SMTP email addresses from which your users often receive email. After each entry, click **Add**.
2. Select the **Immediately pass mail through if the sender is on the Allowed Senders list** option and click **Set** to save your changes. Repeat on the other RazorGate.

Set Allowed Senders

Destination Domain: [Primary](#) | [Any](#) | [Local](#) | [Non-local](#)
Any: Applies to any domain

Mail from a sender on the Allowed Senders list is never identified as Junk Mail. Allowed Senders entries override entries.

E-mail Address or Domain:

1 to 1 of 1 <Prev | Next>

Allowed Senders	
<input type="checkbox"/>	testuser1@yahoo.com

Prioritize Allowed Senders
Set priority to ensure that mail from a sender on the Allowed Senders List is not subject to MailHurdle delays.

Immediately pass mail through if the sender is on the Allowed Senders list.

3. Go to **Anti-Spam > Allowed Mailing Lists**. For the **Destination Domain** option, select **Any**. Add recipients whose email should *not* be subject to MailHurdle screening. For example, you might want to add your support address to the Allowed Mailing Lists so it is always delivered immediately. After each entry, click **Add**.
4. Select the **Immediately pass mail through if the recipient is on the Allowed Mailing Lists** option and click **Set** to save your changes. Repeat on the other RazorGate.

Set Allowed Mailing Lists

Destination Domain: [Primary](#) | [Any](#) | [Local](#) | [Non-local](#)
Any: Applies to any domain

Mail to a recipient on the Allowed Mailing Lists is never subject to Junk Mail filtering. Allowed Mailing List entries override entries.

Mailing List Address or Domain:

1 to 1 of 1 <Prev | Next>

Allowed Mailing List	
<input type="checkbox"/>	DL@example.com

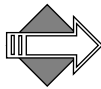
Prioritize Allowed Mailing Lists
Set priority to ensure that mail to a recipient on the Allowed Mailing Lists is not subject to MailHurdle delays.

Immediately pass mail through if the recipient is on the Allowed Mailing Lists.

- Go to **Anti-Spam > MailHurdle > Configuration**. If MailHurdle is disabled, click the **Enable It** button. Several options display once MailHurdle is enabled. Note: You need to enable MailHurdle on both RazorGates and specify the same machine as the **MailHurdle Server** (next step) on both systems.

- On the **MailHurdle > Configuration** page, enter the IP address of the RazorGate that you want to use as the **MailHurdle Server** and click **Add**. Set the same MailHurdle server on both RazorGates.

Repeat on the other RazorGate.



Once you establish a baseline, you might want to deselect the **Pass All Triplets Based on “Active” IP Address** option on the **MailHurdle > Configuration** page if you find that MailHurdle is too lenient.

- Go to **MailHurdle > Allowed Host**, add each cooperating appliance in your messaging network. For this deployment, add the Exchange server and the other RazorGate. For example, on RazorGate A, add RazorGate B’s IP address; on RazorGate B, add RazorGate A’s IP address. After each entry, click **Add**.

Repeat on the other RazorGate.

8. Do not modify the **MailHurdle > Advanced** page. The defaults are appropriate for this deployment.

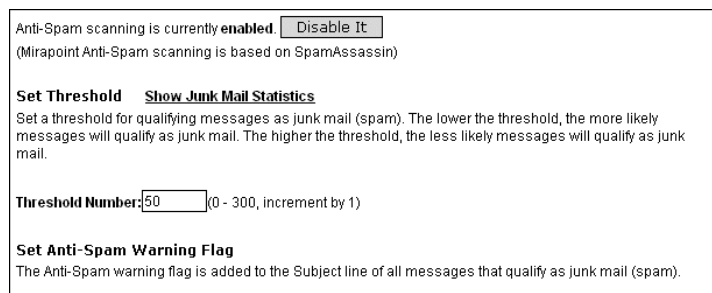
For more detailed information on MailHurdle and all the available options, see [“Working with MailHurdle” on page 388](#) in the Administration Tasks part of this book.

Continue configuring Anti-Spam scanning with the following procedures.

Configuring Anti-Spam Scanning

Anti-Spam scanning is a licensed feature. There are two antispam licenses, **Mirapoint Antispam** (Principal Edition) and **Mirapoint Antispam SE** (Signature Edition). The two scanners, Principal and Signature, are mutually-exclusive; however, the configuration options for both are identical and the update options differ only very slightly. For more information on the two scanners, see [“Principal Edition vs. Signature Edition” on page 417](#). To configure Anti-Spam scanning, follow these steps on each RazorGate.

1. Go to **Home > Anti-Spam > Configuration**, if the scanner is disabled, click the **Enable It** button.



Anti-Spam scanning is currently **enabled**.

(Mirapoint Anti-Spam scanning is based on SpamAssassin)

Set Threshold [Show Junk Mail Statistics](#)

Set a threshold for qualifying messages as junk mail (spam). The lower the threshold, the more likely messages will qualify as junk mail. The higher the threshold, the less likely messages will qualify as junk mail.

Threshold Number: (0 - 300, increment by 1)

Set Anti-Spam Warning Flag

The Anti-Spam warning flag is added to the Subject line of all messages that qualify as junk mail (spam).

The recommended settings for the anti-spam options are:

- ❖ **Threshold Number:** Accept the default threshold of 50. Lower values incur more false positives; higher values miss spam.
- ❖ **Add Warning Flag:** Select this option to add a text string to the message subject that flags the message as spam. The default text is **Spam?**. (This option may be selected on some machines)

- ❖ **Insert Junk Mail Explanation: Select.** This can be useful in debugging. Note: This option only displays for **Mirapoint Antispam** (Principal Edition).
- ❖ **Enable Junk Mail Reporting:** Accept the default (selected); this helps Mirapoint tune the antispam scanning rules.
- ❖ **Scan messages for any recipient:** Accept the default (deselected); this option is not needed for this deployment.

When you are done, click **Apply** to save your changes.
Repeat on the other RazorGate.

2. Go to **Anti-Spam > Updates**. Select the rulegroup for your anti-spam solution, and click **Update Now**:

- ❖ Mirapoint AntiSpam Principal Edition rulegroup: **default**
- ❖ Mirapoint AntiSpam SE (RAPID) rulegroup: **RPDENGINE** or **RPDASIA** (in Asia)

If you do not see the appropriate rulegroup, enter the **Rule Group Name** and click **Install**. When you click **Update Now**, the installed rulegroup is updated. When you click **Install**, the latest version of the specified rulegroup is installed. Note: Updating or installing rulegroups can take a few minutes.

Anti-Spam Updates

Install/Update Rule Groups

Rule Group Name:

	Rule Group Name	Expiration Date	Delete
<input checked="" type="checkbox"/>	default	2007-09-24	✘
<input type="checkbox"/>	mtaverify	2006-03-15	✘

(Warning: Installing or updating rule group(s) will interrupt the services.)

Set Automatic Update & Proxy Server

Update all rule groups every week

Use Proxy Server:

Host:

Port:

User ID:

Password:

3. Select **Update all rule groups every week**. If your site has a proxy server, select **Use Proxy Server** and designate its **Host** and **Port**. When you are done, click **Apply** to save your changes. Repeat on the other RazorGate.
4. Go to **Anti-Spam > Relay List**. Enter the IP address of each Exchange server from which this router should accept messages for transmission to the Internet. (You could enter the hostnames of the Exchange servers, but IP addresses are more reliable.) Click **Add** for each address you enter. Repeat on the other RazorGate.

Set Relay List

Specify networks and domains whose messages may be relayed to remote hosts.

IP Network or DNS Domain:

1 to 1 of 1 <Prev | Next>

IP Network or DNS Domain
<input type="checkbox"/> 10.0.12.97

5. Go to **Anti-Spam > RBL Host List**. If the service is disabled, click **Enable it**. If you have subscribed to an RBL service, add the service's host name to the **RBL Host List** page. Mirapoint recommends subscribing to an RBL service, or setting up a local RBL server to block connections from known spam propagators by checking the connection source against a list maintained by a trusted third-party. See the Wikipedia article on [DNSBL](#) for more information. Repeat on the other RazorGate.

i

6. Optional: If you plan to set up Junkmail filtering, select the **Insert “X-Junkmail:RBL” header to the message** option.

When you are done, click **Apply** to save your changes.
Repeat on the other RazorGate.

7. Go to **Anti-Spam > Reject List**. Enter the domain name of any known spam sites if your site lacks access to RBL service or there are sites that you know you want to block. Click **Add** for each address you enter.
Repeat on the other RazorGate.

When you are done, continue your set up with [“Configuring Inbound Routing—RGs Security Deployment,”](#) next.

Configuring Inbound Routing—RGs Security Deployment

Inbound routing is handled by the two RazorGates that are also screening the incoming messages. This involves two RazorGate

appliances, both run MailHurdle, Antivirus and Antispam; both are inbound routers. One is set up to be the MailHurdle server and outbound router.

About Exchange and Active Directory

You will need the hostname and IP address of your Exchange server(s), and if different, the hostname and IP address of your Active Directory server. Enable global catalog on Active Directory port 3268.

You also might need the **bindDN** (bind distinguished name) of the Active Directory database tree. Steps to determine this information are presented in [“Getting the Active Directory bindDN,”](#) next.

These instructions work best when your site has a one-to-one mapping from DNS domain to Exchange server. That is to say, each Exchange box serves only one domain. These instructions also work well when one Exchange box services multiple domains.

However, when a domain spans multiple Exchange boxes (that is, when users in the same domain reside on different Exchange servers) you will be forced to set up per-user domain routing. To do this, Mirapoint recommends that you find an unused attribute in Active Directory, use it to record the user setting for Mailhost, and set up custom mappings for **Ldap Setquery user:Mailhost** on the **LDAP User Queries** page; see step 2 of [“Setting Active Directory LDAP Routing—RGs Security,”](#) next.

Getting the Active Directory bindDN

If you do not know the Active Directory bindDN, you can query your Active Directory server as follows

1. Connect to your Active Directory server and log in to the system.
2. Go to the command prompt window (**Start > All Programs > Accessories > Command Prompt**) and run the **ldifde** command to get the entry for a user defined in the directory, such as **Administrator**:

```
ldifde -r cn=Administrator -f output.ldif
```

3. Open the **output.ldif** file. (This file is saved to the directory where the `ldifde` command is run, for example `C:\Documents and Settings\Administrator\`.)

4. The first line in the **output.ldif** file contains the Active Directory's DN information. For example:

```
dn: CN=Administrator, CN=Users, DC=adhostname, DC=yourdomain, DC=com
```

In this example, the **base DN** is **DC=adhostname, DC=yourdomain, DC=com**. To use the **Administrator** account to authenticate the Message Server to the Active Directory server, the entire DN is specified as the **bind DN**: **CN=Administrator, CN=Users, DC=adhostname, DC=yourdomain, DC=com**.

Setting Active Directory LDAP Routing—RGs Security

On each RazorGate use the **System > Routing** pages to configure Active Directory LDAP routing by following these steps.

1. Go to **Home > System > Routing > Routing Method**. Select **Route via Microsoft Active Directory**. A new page (with red text) asks you to confirm this choice.
For the **LDAP Server** option, type the name of at least one Active Directory server plus the port (usually 3268). For example,

ldap://exchange.example.com:3268

Repeat on the other RazorGate.

2. Go to **Routing > User Queries**. Under the heading **Set Base DN**, click **Use Default BaseDN**. All of the user query filter and attribute names appear automatically. (If needed, you can use the **MailHost attribute** option for custom mappings as described in [“About Exchange and Active Directory” on page 126](#)).

3. In the **Set Credentials** area, enter the bindDN of the Active Directory DIT. For example, **CN=Administrator, CN=Users, DC=exchange, DC=example, DC=com** and the corresponding Administrator password. Note: This is not optional for Active Directory. Click **Set**. For instructions on getting the Active Directory bindDN, see [“Getting the Active Directory bindDN” on page 126](#).

Set Credentials (Optional)
 Specify the Bind DN and password to access your user records. Leave blank if your LDAP server supports anonymous

Bind DN:

Password:

- Under the **Test Query** heading, type a valid user e-mail address in your Active Directory database and click **Test**. The **mail** and **cn** (full name) values appear for that e-mail address.

Test Query
 Use this tool to send a test query to your LDAP servers.

E-mail address:

Result:

Attribute	Value
mail	test1@example.com
cn	Test1

Repeat on the other RazorGate.

- Do not modify the **Routing > Mail Group Queries** page. Mail group queries do not have to be configured at this time. (Configuring mail groups requires additional information about the Active Directory schema.)
- Go to **Routing > Mail Host Mapping**. Enter all Exchange mail domains, and the IP address of the Exchange server. Click **Add** after each entry.
 Repeat on the other RazorGate.

Setting Default Authentication

You must use the CLI to set the authentication. Telnet to both RazorGates and log in as administrator; replace *hostname.yourdomain.com* with the name of the RazorGate appliance each time:

```
User: telnet hostname.yourdomain.com
OK hostname.yourdomain.com admin 3.8 server ready
User: Administrator
Password:
OK User logged in
```

Enter the **auth set** command on each RazorGate to set the authentication mechanism:

```
hostname.com> Auth Set Default Plaintext:Ldap
OK Completed
```

Exit the CLI by typing **exit**.

Continue the deployment configuration using the Administration Suite browser windows and completing the following sections.

Setting SMTP Security Checks and Mail Domains

To configure SMTP service options, follow these steps. Leave at default options not mentioned in this procedure.



When transmission security is important, use of SSL is recommended. Within open organizations protected by firewall, it's less of an issue. Individual messages can be encrypted using alternate methods.

1. Go to **Home > System > Services > SMTP > Main Configuration**.
Note: Do not enable or start the service until the end.
2. In the **Supported Connections** area, select these options:
 - ❖ **Allow STARTTLS (Inbound Connections):** Encrypted incoming connections are supported.
 - ❖ **Allow STARTTLS (Outbound Connections):** Outgoing connections are encrypted.

Leave **Require Secure Authentication (SSL)** deselected.

Supported Connections	
<input type="checkbox"/>	Require Secure Authentication (SSL)
<input checked="" type="checkbox"/>	Allow STARTTLS (Inbound Connections)
<input checked="" type="checkbox"/>	Allow STARTTLS (Outbound Connections)

3. Accept the defaults for:
 - ❖ **Inbound Connection Settings**
 - ❖ **Outbound Connection Settings**
 - ❖ **SMTP Authentication Settings**
 - ❖ **Mail Queue Settings**

4. In the **Routing Settings** area, select **Use LDAP Routing: For All Messages**. This causes all inbound and outbound messages to be routed through LDAP. Accept the defaults for the other options.

Routing Settings

Use LDAP Routing: For All Messages

When using LDAP Routing, use: "MX" Record "A" Record

Local Message Router:

Outbound Message Router:

5. In the **Masquerade Settings** area, set the following options:
 - ❖ **Masquerade all messages as this domain:** If your site has multiple Exchange servers in different subdomains, and you want outgoing e-mail to be addressed from your main domain, type your site's primary (standard) domain name. **Note:** When you set a masquerade, the masquerade name must be on the list of Mail Domains; this is described in the next step.
 - ❖ **Use LDAP for masquerade information:** No. This option would cause the RazorGate to get masquerade information from Active Directory, something you probably do not need to do.
 - ❖ (optional) **Do NOT masquerade these headers:** You could select the Sender option; Mirapoint recommends masquerading the To and Reply-To headers, so leave those unselected.

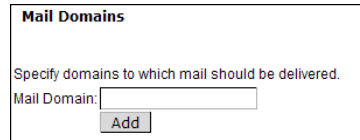
Masquerade Settings

Masquerade all messages as this domain: example.com

Use LDAP for masquerade information: Yes No

Do NOT masquerade these headers: From Reply-To Sender

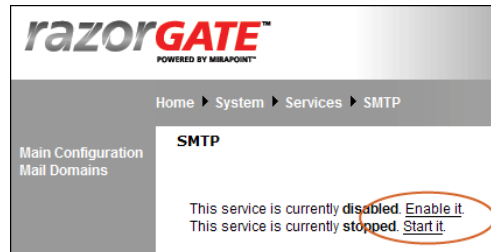
6. Click **Modify** at the bottom of the **SMTP > Main Configuration** page to save any changes you make.
Repeat on the other RazorGate.
7. Click **Mail Domains** in the page menu to open the **SMTP > Mail Domains** page. Type the name of each mail domain for which this router delivers e-mail; also enter the masquerade name you configured in step 5. Give the full domain name: everything after the at-sign (@). Click **Add** after each entry.



Repeat on the other RazorGate.

8. Click **SMTP** in the top navigation bar to return to the SMTP service page. If the service is disabled, click **Enable it**. If the service is stopped, click **Start it**.

Repeat on the other RazorGate.



Configuring Outbound Routing—RGs Securing Exchange



Configuring outbound routing involves setting a RazorGate server as “Smart Host” (outbound router) on the Exchange server.

To load balance, have one RazorGate act as the MailHurdle server and the other as the outbound router.

You might want to refer to one of these Knowledge Base articles first.

For Microsoft Exchange 2003 (KB Article 821911):

<http://support.microsoft.com/kb/821911>

For Microsoft Exchange 2000 (KB Article 257426):

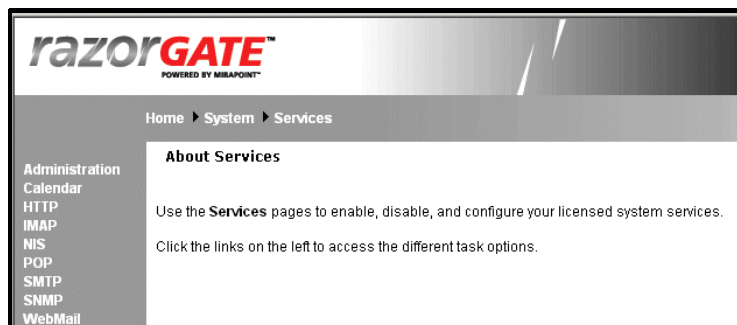
<http://support.microsoft.com/kb/257426>

1. Log in to your Exchange server as administrator and go to **Exchange System Manager**. A two-paned window opens.
2. In the left pane tree view, click **Servers > *ServerName* > Protocols > SMTP > Default SMTP Server**; where *ServerName* is the name of the Exchange server.
3. Right-click **Default SMTP Server** and point to **Properties**. The **Default SMTP Server Properties** dialog box opens.
4. Open the **Delivery** tab and click **Advanced**. The **Advanced Delivery** dialog box opens.
5. In the **Smart Host** option enter the fully-qualified hostname of the RazorGate that you did **not** set as the MailHurdle server in step 6 of [“Configuring MailHurdle” on page 119](#). Click **OK**.
6. The **Default SMTP Server Properties** dialog box re-opens, click **OK** again.

Enabling and Starting Services

Enabled services start automatically when the system boots. The **Administration** and **HTTP** services are always enabled and started. Services you choose not to start will not be available.

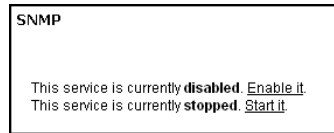
1. Go to **Home > System > Services**. Click on the name of a service in the page menu to go to that service’s page. Note: Only licensed services display page links.



2. At this point, most services have already been enabled and started, the following might still need attention.

- ❖ Ensure that **Calendar**, **IMAP**, **NIS**, and **POP** are disabled by navigating to those pages.
- ❖ **SNMP**—The Simple Network Management Protocol (SNMP) service allows consoles to monitor selected information about Mirapoint systems. This only applies if you have an SNMP management station.

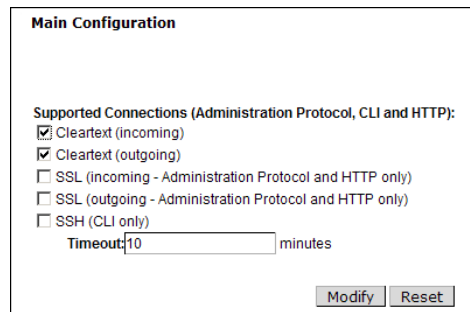
To read more about SNMP see [“Monitoring External Systems via SNMP” on page 253](#) in the Administration Tasks part of this book.



Resetting the Administration Timeout

Setting the timeout to 60 minutes is recommended for the configuration procedures; however, once you're done, you'll want to return to the **Home > System > Services > Administration > Main Configuration** page and set the **Timeout** back to **10 minutes** for security.

Click **Modify** to save your changes.



This completes the configuration of the RazorGate Security Deployment for Exchange. Finish by verifying the configuration by completing the following steps.

Verifying the RazorGate Security Setup

Now that you've finished the initial setup and configured your directory service, you need to verify that everything is working properly. To do this, you'll send two test mails, one should be tagged as Spam, the other, not.

1. Log in to an external mail client, such as Yahoo, and send a regular (non-spam) test message to an Exchange user account for which you have the login; for example, **test1@exchange.example.com**. This email should be delivered to the user's Inbox. To check, log into Exchange (<http://exchangehostname/exchange>) as that user and look for message.
2. Send a GTUBE test message to the account (information below). This email should be delivered but tagged as spam. Also go to **Home > Logs/Reports > Mail > Detailed** to see how the test message was handled.

You can download GTUBE (Generic Test for Unsolicited Bulk Email) from <http://gtube.net/gtube.txt>. The test message looks like this:

```
Body: This is the GTUBE, the
Generic
Test for
Unsolicited
Bulk
Email
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-
EMAIL*C.34X
```

Optional Configuration Options

The following optional configuration task can be completed, if needed, when you've finished the basic set up of your RazorGates.

Setting Connection Proxies

If you want the RazorGate appliances to proxy IMAP or POP connections, follow these steps on each RazorGate appliance:

1. Go to **Home > System > Services > IMAP**. If the service is neither enabled nor running, enable and start it.
2. Select **Mode: Proxy**. With this set, the RazorGate appliances use the **User:Routingaddr** and **Mailhost** configured LDAP attributes to do proxying, as they would for routing.

When you are done, click **Modify** to save your changes.

Note: You must have LDAP Routing licensed to use this option.

IMAP

This service is currently **enabled**. [Disable it](#).
This service is currently **running**. [Stop it](#).

Configuration

Supported Connections:

Cleartext (incoming)
 Cleartext (outgoing)
 SSL (incoming)
 SSL (outgoing)

Mode: Normal Proxy

Quota Warning: % full

Timeout: minutes

3. Go to **Home > System > Services > POP**. If the service is neither enabled nor running, enable and start it.
4. Select **Mode: Proxy**. With this set, the RazorGate appliances use the **User:Routingaddr** and **Mailhost** configured LDAP attributes to do proxying, as they would for routing.

When you are done, click **Modify** to save your changes.

Note: You must have LDAP Routing licensed to use this option.

POP

This service is currently **enabled**. [Disable it.](#)
This service is currently **running**. [Stop it.](#)

Configuration

Supported Connections:

Cleartext (incoming)
 Cleartext (outgoing)
 SSL (incoming)
 SSL (outgoing)

Mode: Normal Proxy

Min Poll Time: minutes

Timeout: minutes

Next Steps, RG Security Deployment

Now that you have your RazorGates up and running, there are a number of additional features you can configure according to your site requirements:

- ◆ **Schedule Software Updates:** In addition to antivirus and antispam updates, you can schedule MOS update checks through the Administration Suite **System > Utilities > Updates > Update Check** page. For more information, see the Administration Suite online help.
- ◆ **Limit TCP Connections:** Mirapoint recommends limiting TCP connections. See [“Limiting TCP Connections” on page 90](#) for how to deter denial-of-service attacks.





RazorGate with Junk Mail Manager Security Deployment for Exchange

In this deployment, two RazorGate appliances, enabled with Junk Mail Manager (JMM), perform message screening and message routing for an Exchange server using Active Directory. How to set up these functions is described in this chapter. For more information on this deployment, refer to the *Mirapoint Administrator's Planning Guide*.

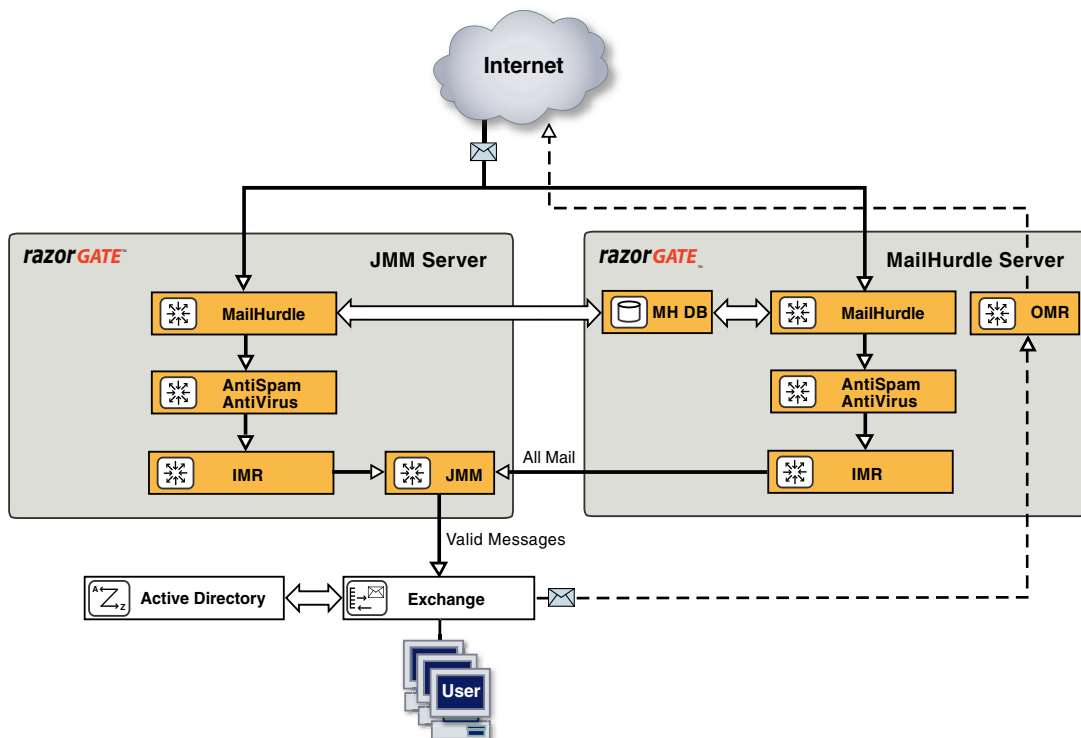


Figure 4 RazorGate with JMM Security Deployment for Exchange

Before You Begin

Before you begin configuring the RazorGate appliances to secure an Exchange server, make sure to read [Chapter 1, “All Deployments Start Here,”](#) and perform the tasks described there, including:

- ◆ [Pre-Configuration Checklist](#) (as applicable):
 - ❖ Domain Name System (DNS) servers configured
 - ❖ Lightweight Directory Access Protocol (LDAP) set up
 - ❖ Licenses obtained (licenses are implementation specific)
 - ❖ Backup requirements defined
 - ❖ Secure Sockets Layer (SSL) certificates obtained
- ◆ [Prerequisites](#):
 - ❖ Hardware installation (connected to the Internet)
 - ❖ DNS server database records
 - ❖ Basic system setup (described on the Quick Start Setup card shipped with your appliance)
- ◆ [Initial Setup Common to All Deployments](#):
 - ❖ Secure administrator account set
 - ❖ Appliance clock set
 - ❖ Network settings verified, DNS server(s) added
 - ❖ Licenses installed
 - ❖ Service Reporting options set
 - ❖ Software updates obtained
 - ❖ Administrator access restricted
 - ❖ SSL security for administrator logins set

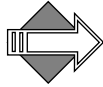
Information Required for this Configuration

You need the following information to configure RazorGate appliances with JMM to secure an Exchange server, as documented here:

- ◆ A list of senders and recipients (IP addresses, domain names, and email addresses) that you want to **safelist** by adding to your Allowed Senders/Allowed Mailing Lists. Safelisting senders/recipients ensures that mail from or to, respectively, those addresses

is never subject to antispam delays. You will also set priority on the safe lists to override antispam scanning.

- ◆ A list of RBL (Realtime Blackhole List) servers. This is configured on the **Anti-Spam > RBL Host List** page. You can learn more about this through Wikipedia: <http://en.wikipedia.org/wiki/DNSBL>.
- ◆ The IP address and FQDN (fully-qualified domain name) of the RazorGates, and Exchange server, plus all Exchange mail domain names (these will be entered as JMM domains).
- ◆ The hostname, port number, and bindDN (distinguished name for locating the database) of your Active Directory server.
- ◆ The hostname, port number, and authentication credentials (if appropriate) for your Proxy Server if your site blocks outgoing HTTP and FTP connections. This is required to get system updates, antivirus updates, and antispam updates.
- ◆ IP address for all DNS servers you want to add.
- ◆ Licenses required for this deployment are listed below. Verifying installed licenses and installing licenses is described in step [5](#) of [“Completing the Setup Wizard” on page 39](#).
 - ❖ Default licenses shipped with RazorGate:
 - User Limit: 20
 - LDAP Routing
 - MailHurdle (not listed on licenses page)
 - WebMail: 20
 - POP: 20
 - IMAP: 20
 - RazorGate
 - Junk Mail Manager
 - ❖ Optional licenses (an antivirus license and an antispam license are usually included):
 - Sophos (signature-based) virus filtering
 - F-Secure (signature-based) virus filtering
 - RAPID (predictive-based) virus filtering
 - Antispam (Principal Edition) or Antispam SE (Signature Edition)
 - SSL (Secure Sockets Layer)



The two Antispam licenses are mutually exclusive.



Mirapoint recommends at least one signature-based antivirus scanner and RAPID. Please Note: RAPID antivirus must be used in conjunction with a signature-based antivirus engine (Sophos or F-Secure).

Checking your licenses is described below on page 147.

DNS Records Required for JMM Configuration

In this deployment, one RazorGate acts as the JMM server and the other acts as the MailHurdle server and outbound router. By default, all inbound mail received by the MailHurdle server is routed through the JMM server, which quarantines spam and passes valid messages on to the Exchange server.

To ensure that mail is delivered even if the JMM server is unavailable, you set up DNS records for a “pseudo-host” to define a primary route through the JMM server and a secondary route directly to the Exchange server, as shown in Figure 5.

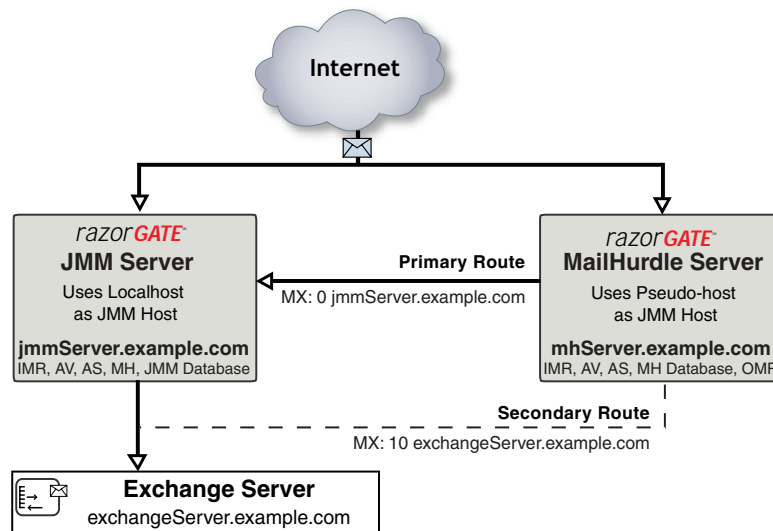


Figure 5 Example Pseudo-host DNS Records

The DNS entries for the pseudo-host map a unique name such as **jmmServer-exchangeServer.example.com** to the same IP address used by the JMM server. The primary and secondary routes are defined by creating two MX records for the pseudo-host: a high-priority record that points to the JMM server, and a low priority record that points directly to the Exchange server.

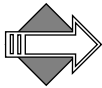
When you configure JMM on the MailHurdle server, you specify the pseudo-host as its JMM host. If the JMM server is not available, the low priority MX record ensures that mail will still be delivered (a **fail-open** solution). Spam is not quarantined if the JMM server is unavailable, but as long as the **Set Anti-Spam Warning Flag** option is selected it is tagged as spam and can be filtered.

DNS “A” and “PTR” records need to be set for both RazorGate appliances and all Exchange servers. For the pseudo-host:

1. Create an “A” record such as **jmmServer-exchangeServer.example.com** with the same IP address as the JMM server.
2. Create dual MX records for the pseudo-host, one with high priority (a lower number) that points to the JMM server, and another with low priority (a higher number) that points to the Exchange server. For example:

```
MX: 0 jmmServer.example.com
MX: 10 exchangeServer.example.com
```

See Figure 5 for an illustration.



An experienced DNS administrator is usually responsible for modifying a site’s DNS configuration to support new hardware deployments.

Differences in the Setup

Most options you set will be identical on the MailHurdle server/ outbound router and the JMM server; however, a few are different. Those differences are described in Table 9.

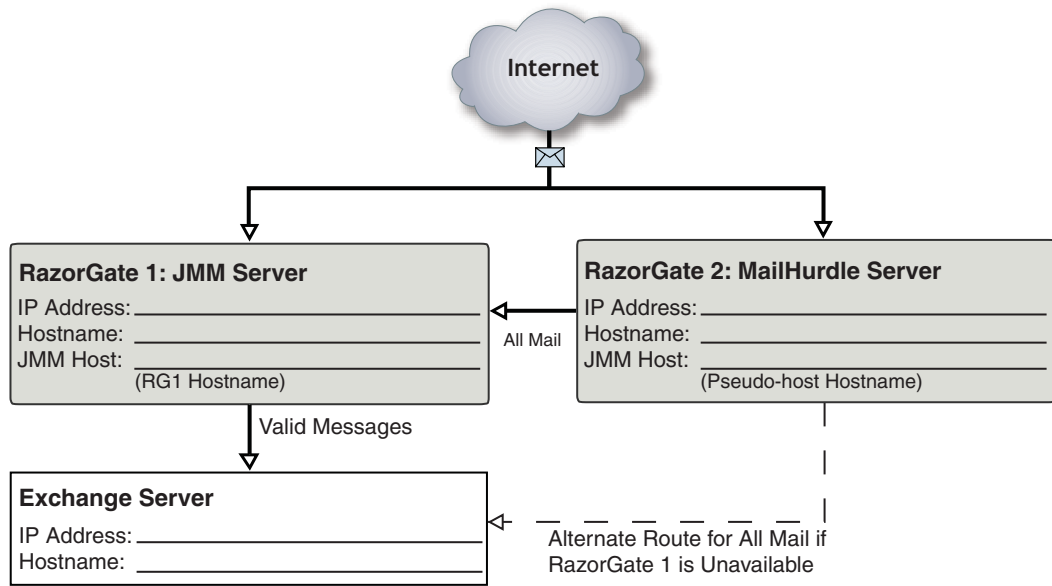
Table 9 Differences in Setup of MailHurdle Server and JMM Server

Administration Suite Page	Option	MailHurdle Server	JMM Server
MailHurdle > Configuration	MailHurdle Server	localhost (MailHurdle server)	MailHurdle server
Anti-Spam > Configuration	Scan Messages for any recipient	Select	Leave de-selected
	Masquerade all messages as this domain	Set to the Exchange server's mail domain name	Leave un-set
Setup Wizard > Junk Mail Manager Domain to Host Mapping	Junk Mail Manager Host	Pseudo-host	localhost

Worksheet



The following worksheet is provided to help you gather the information you need to complete this configuration. We highly recommend using it to record your domain and server information and referring to it when you are configuring the RazorGates, in particular, the Junk Mail Manager setup.



Pseudo-Host DNS Record

IP Address: _____ (Same as JMM Server)
 Hostname: _____ (For example, jmm-exchange.example.com)
 MX : 0 _____ (RazorGate 1, JMM Server)
 MX : 10 _____ (Exchange Server)

Active Directory Server

FQDN: **ldap://** _____ **:3268**
 Bind DN: _____ (Account used for authentication, such as administrator)
 Bind PW: _____

Masquerade

Hostname: _____

Configuring Two RazorGates with JMM to Secure Exchange

In this deployment, both RazorGates perform antivirus and antispam scanning, but one is designated as the Junk Mail Manager server and

the other acts as the MailHurdle server and outbound router. JMM is enabled on both RazorGates and the MailHurdle server is configured to route all mail through the JMM server. If the JMM server is not available, a secondary route delivers mail directly to the Exchange server after it is scanned for viruses and spam.

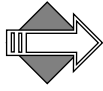
This configuration provides message screening and Junk Mail Manager functionality while ensuring message delivery even if the JMM server is not available. To configure your message network for this deployment, you need to perform the following tasks:

- ◆ Accessing the Administration Suite
- ◆ Checking for Licenses
- ◆ Setting the Administration Timeout
- ◆ Configuring MailHurdle
- ◆ Configuring Anti-Virus Scanning
- ◆ Configuring Anti-Spam Scanning
- ◆ Setting SMTP Security Checks
- ◆ Configuring Inbound Routing—RGs + JMM Security Deployment
- ◆ Configuring Outbound Routing
- ◆ Enabling and Starting Services
- ◆ Resetting the Administration Timeout

Accessing the Administration Suite

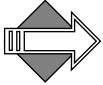
You use the Administration Suite to perform most RazorGate configuration tasks. To access the Administration Suite from a web browser, go to **`http://hostname/miradmin`** where *hostname* is your appliance's fully-qualified domain name.

Open two web browser windows and log in as administrator on both RazorGate appliances so you can configure them at the same time. The Administration Suite displays function links at the left and a navigation bar at the top that tracks your current location within the page hierarchy. The **Site Map** link (in the upper right corner) displays links to most pages.

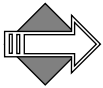


If you are accessing the Administration Suite for the first time, the Setup Wizard displays. You need to use the Setup Wizard to perform the basic configuration tasks described in [“Completing the Setup Wizard” on page 39](#) before continuing.

Checking for Licenses



To verify that you have the licenses you need for this configuration, go to the **Home > System > Utilities > License** page to see all the license keys available to you.



The MailHurdle license does not display; it is part of the Anti-Spam license.

LDAP routing requires a license. This license is a prerequisite for many other licensed features including SMTP directory-based routing, IMAP or POP proxying, Group Calendar, and multi-tier shared folders.

Setting the Administration Timeout

We recommend changing the default Administration Suite timeout from 10 minutes to at least 60 minutes while you are configuring the JMM appliances. Otherwise the browser connections will time out.

Go to the **Home > System > Services > Administration > Main Configuration** page. Change **Timeout** to 60 minutes or more. To apply the change, click **Modify**.

Change the timeout back to 10 minutes after you are done setting up the system.

Main Configuration

Supported Connections (Administration Protocol, CLI and HTTP):

- Cleartext (incoming)
- Cleartext (outgoing)
- SSL (incoming - Administration Protocol and HTTP only)
- SSL (outgoing - Administration Protocol and HTTP only)
- SSH (CLI only)

Timeout: minutes

Repeat on the other RazorGate.

Configuring Anti-Virus Scanning

Anti-Virus scanning is a licensed feature usually set at the factory.

There are three antivirus scanners you can license and configure. Two, **F-Secure** and **Sophos**, are **signature-based**, meaning they use databases of known viruses to categorize messages as containing a virus. The third, **RAPID**, is **predictive-based**, meaning it uses a database of heuristics to categorize messages as *potentially* containing viruses. Because RAPID categorizes messages as containing potential viruses, rather than known viruses, its only available action is quarantine. Those RAPID-quarantined messages are automatically released after a configurable amount of time, allowing one of the signature-based antivirus engines to re-scan the messages.

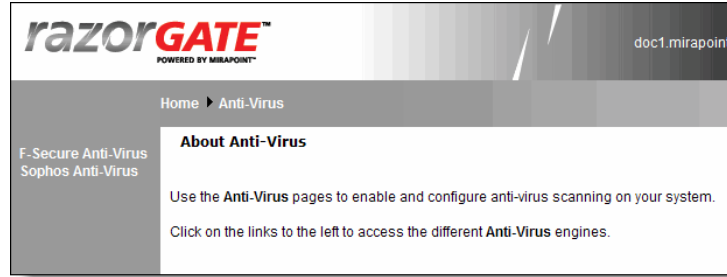


Mirapoint recommends configuring at least one signature-based antivirus scanner and the RAPID antivirus scanner for this deployment. Please note: RAPID antivirus must be used in conjunction with a signature-based antivirus; used alone it is ineffective in preventing virus attacks. You can run all three antivirus engines in this deployment, one or both signature-based engine plus RAPID on each RazorGate, if you have all three licenses.

Configuring F-Secure or Sophos Anti-Virus

To configure Sophos and/or F-Secure Anti-Virus, follow these steps on each RazorGate. You need to repeat the steps (on each RazorGate) if you are going to use both antivirus engines.

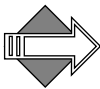
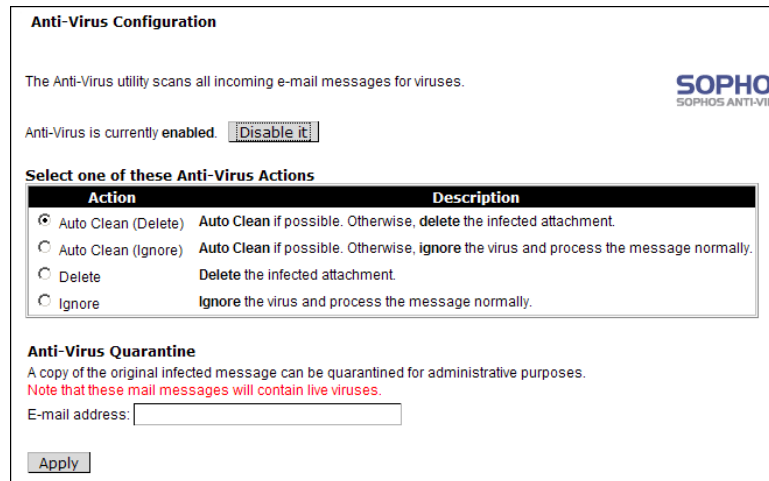
1. Go to **Home > Anti-Virus**, click the link at left for the scanner to be configured, F-Secure or Sophos (only licensed options display). The main page for that virus scanner opens. Click **Configuration**.



2. On the **Anti-Virus > virus scanner > Configuration** page, if the scanner is disabled, click the **Enable It** button. Accept the default **Auto-Clean (Delete)** option. If you want to archive caught viruses, enter an e-mail address in the **Anti-Virus Quarantine** field.



Messages sent to the **Anti-Virus Quarantine** contain live viruses and should not be opened on a desktop computer.



If you select the **Auto Clean (Ignore)** or **Ignore** options, infected messages will be delivered to your users.

If you make changes, click **Apply** to save your changes.

Repeat on the other RazorGate (if needed).

3. Do not modify the **Anti-Virus > virus scanner > Notifications** page. The defaults are appropriate for this deployment.

4. On the **Anti-Virus > virus scanner > Updates** page, change the default hourly time if it is not good for your site.

If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**.

When you are done, click **Apply** to save your changes.

Repeat on the other RazorGate.

Automatic Update and Proxy Server

Automatically update:

*Hourly: :59 (on the minute)

Daily: 00:00 (on the hour)

Weekly: Sunday (day of week)

Monthly: 1 (on the day)

*Strongly Recommended

Use Proxy Server:

Host: _____

Port: _____

User ID: _____

Password: _____

Apply Update Now

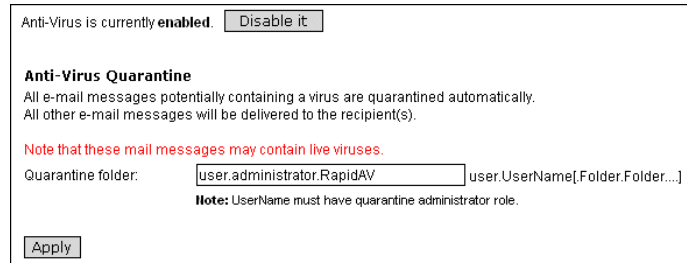
Configuring RAPID Anti-Virus

RAPID Anti-Virus is a licensed feature, it uses a **predictive-based** methodology that immediately categorizes suspect mail as spam based on heuristics maintained in a rulegroup. It must be used in conjunction with one of the signature-based antivirus scanners, F-Secure or Sophos, to be effective. Alone, RAPID is not an effective antivirus solution.

There are some file extensions that always trigger the RAPID antivirus quarantine action; for details see [“Modifying Predictive-based \(RAPID\) Anti-Virus” on page 409](#) in the Administration Tasks part of this book.

To configure RAPID Anti-Virus, follow these steps on each RazorGate.

1. Go to **Home > Anti-Virus > RAPID > Configuration**, if the scanner is disabled, click the **Enable It** button.



2. Accept the default **Quarantine folder** address, a subfolder of the **Administrator** account. Later, you can use any valid *user.username.subfolder* e-mail address for an account with the Quarantine Administrator role. For more information, see [“How Antivirus Quarantine Works” on page 398](#), and [“Using Security Quarantine” on page 441](#) in the Administration Tasks part of this book. When you are done, click **Apply** to save your changes.

Repeat on the other RazorGate.

Afterwards, all messages potentially containing a virus are automatically quarantined for 8 hours to the specified email address; other messages are delivered normally. The auto-release time can be modified using the CLI; see **Help About Antivirus**.

3. Go to **Anti-Virus > RAPID > Notifications** and modify the format of virus notifications as appropriate. Whereas notifications for F-Secure or Sophos-caught viruses are not really needed, because those are known viruses, notifications for RAPID quarantined potential viruses is very important. Users should be made aware that a message is quarantined for a potential virus.



In the **To** option, add the appropriate quarantine administrator email addresses (or just **Administrator** to use the default). The specified administrators are notified when messages are quarantined by RAPID. Use commas (,) as separators to enter multiple email addresses.

When you are done, click **Apply** to save your changes.

Send this notification to the message recipient(s) when a potential virus is found.
This notification is currently disabled.

From:

Subject:

Message:

Unicode (UTF-8)

\$(sender)=Sender \$(subject)=Subject \$(action)=Action
\$(attachments)=List of attachments \$(domain)=Current Domain
\$(filtername)=Filter name that triggered the notification

Repeat on the other RazorGate.

- Go to **Anti-Virus > RAPID > Updates** and change the default hourly time to be a half hour different than the other RazorGate. If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**.

When you are done, click **Apply** to save your changes.
Repeat on the other RazorGate.

About RAPID Anti-Virus
rpdengine

Automatic Update and Proxy Server

Automatically update:

*Hourly: (on the minute)

Daily: (on the hour)

Weekly: (day of week)

Monthly: (on the day)

**Ruleset Name:

**Required for RAPID AV Updates
*Strongly Recommended

Use Proxy Server:

Host:

Port:

User ID:

Password:

Configuring MailHurdle

Mirapoint MailHurdle blocks spam by screening messages from unrecognized sources. When a message is received from an unrecognized source, MailHurdle temporarily fails the message and sends a **retry later** code. A properly-configured mail server automatically resends the message, which is then accepted by MailHurdle; however, most spam mailers pay no attention to this retry request code.

To configure MailHurdle to ensure the timely delivery of valid messages, follow these steps on each RazorGate appliance.

1. Go to **Home > Anti-Spam > Allowed Senders**. For the default **Destination Domain** option, select: **Any**. Enter domains and SMTP email addresses from which your users often receive email. After each entry, click **Add**.
2. Select the **Immediately pass mail through if the sender is on the Allowed Senders list** option and click **Set** to save your changes. Repeat on the other RazorGate.

Set Allowed Senders

Destination Domain: [Primary](#) | [Any](#) | [Local](#) | [Non-local](#)
 Any: Applies to any domain

Mail from a sender on the Allowed Senders list is never identified as Junk Mail. Allowed Senders entries override entries.

E-mail Address or Domain:

1 to 1 of 1 <Prev|Next>

Allowed Senders
<input type="checkbox"/> testuser1@yahoo.com

Prioritize Allowed Senders
 Set priority to ensure that mail from a sender on the Allowed Senders List is not subject to MailHurdle delays.

Immediately pass mail through if the sender is on the Allowed Senders list.

3. Go to **Anti-Spam > Allowed Mailing Lists**. For the default **Destination Domain** option, select **Any**. Enter any recipients whose email should *not* be subject to MailHurdle screening. For example, you might want to add your support address to the Allowed

Mailing Lists so it is always delivered immediately. After each entry, click **Add**.

4. Select the **Immediately pass mail through if the recipient is on the Allowed Mailing Lists** option and click **Set** to save your changes. Repeat on the other RazorGate.

Set Allowed Mailing Lists

Destination Domain: [Primary](#) | [Any](#) | [Local](#) | [Non-local](#)
Any: Applies to any domain

Mail to a recipient on the Allowed Mailing Lists is never subject to Junk Mail filtering. Allowed Mailing List entries Senders entries.

Mailing List Address or Domain:

1 to 1 of 1 <Prev|Next>

Allowed Mailing List
<input type="checkbox"/> DL@example.com <input type="button" value="Remove"/>

Prioritize Allowed Mailing Lists
Set priority to ensure that mail to a recipient on the Allowed Mailing Lists is not subject to MailHurdle delays.

Immediately pass mail through if the recipient is on the Allowed Mailing Lists.

5. Go to **Anti-Spam > MailHurdle > Configuration**, if MailHurdle is disabled, click the **Enable It** button. Several options display once MailHurdle is enabled. Note: You need to enable MailHurdle on both RazorGates but specify only one, on both, as the **MailHurdle Server** (next step). Repeat on the other RazorGate.

Configuration

Use this page to configure MailHurdle servers, timeout periods, and server cache.

MailHurdle is currently **enabled**.

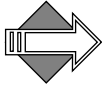
(Warning: Enabling MailHurdle may cause occasional mail delays to critical e-mail. [MailHurdle FAQ](#))

MailHurdle Server:

1 to 1 of 1

MailHurdle Server
<input type="checkbox"/> 10.0.2.85 <input type="button" value="Remove"/>

6. On the **MailHurdle > Configuration** page, enter the IP address of the RazorGate that you want to use as the **MailHurdle Server** and click **Add**. Set the same MailHurdle server on both RazorGates. Repeat on the other RazorGate.



Once you establish a baseline, you might want to deselect the **Pass All Triplets Based on “Active” IP Address** option on the **MailHurdle > Configuration** page if you find that MailHurdle is too lenient.

7. Go to **MailHurdle > Allowed Host**, add the hostname of each cooperating appliance in your messaging network. For this deployment, add the other RazorGate. For example, on RazorGate A, add RazorGate B’s hostname; on RazorGate B, add RazorGate A’s hostname. After each entry, click **Add**. Repeat on the other RazorGate.

Allowed Host

Specify hosts that are allowed to make queries to the MailHurdle server.

Allowed Host:

8. Do not modify the **MailHurdle > Advanced** page. The defaults are appropriate for this deployment.

For more detailed information on MailHurdle and all the available options, see [“Working with MailHurdle” on page 388](#) in the Administration Tasks part of this book.

Continue configuring Anti-Spam scanning with the following procedures.

Configuring Anti-Spam Scanning

Anti-Spam scanning is a licensed feature. There are two antispam licenses, **Mirapoint Antispam** (Principal Edition) and **Mirapoint Antispam SE** (Signature Edition). The two scanners, Principal and Signature, are mutually-exclusive; however, the configuration options for both are identical and the update options differ very slightly. For more information on the two scanners, see [“Principal Edition vs. Signature Edition” on page 417](#).

To configure Anti-Spam scanning, follow these steps on each RazorGate.

1. Go to **Home > Anti-Spam > Configuration**, if the scanner is disabled, click the **Enable It** button.

Anti-Spam scanning is currently **enabled**.

(Mirapoint Anti-Spam scanning is based on SpamAssassin)

Set Threshold [Show Junk Mail Statistics](#)

Set a threshold for qualifying messages as junk mail (spam). The lower the threshold, the more likely messages will qualify as junk mail. The higher the threshold, the less likely messages will qualify as junk mail.

Threshold Number: (0 - 300, increment by 1)

Set Anti-Spam Warning Flag

The Anti-Spam warning flag is added to the Subject line of all messages that qualify as junk mail (spam).

Recommended settings for the anti-spam options are:

- ❖ **Threshold Number:** Accept the default threshold of 50. Lower values incur more false positives; higher values miss spam.
- ❖ **Add Warning Flag:** Select this option to add a text string to the message subject that flags the message as spam. The default text is **Spam?**. (This option may be selected on some machines)
- ❖ **Insert Junk Mail Explanation:** **Select**. This can be useful in debugging. Note: This option only displays for **Mirapoint Antispam** (Principal Edition).
- ❖ **Enable Junk Mail Reporting:** Accept the default (selected), this helps Mirapoint tune the antispam scanning rules.
- ❖ **Scan messages for any recipient:** For the JMM server: Accept the default (deselected). For the MailHurdle server: **Select**.

When you are done, click **Apply** to save your changes.

Repeat on the other RazorGate.

2. Go to **Anti-Spam > Updates**. Select the rulegroup for your anti-spam solution, and click **Update Now**:
 - ❖ Mirapoint AntiSpam Principal Edition rulegroup: **default**
 - ❖ Mirapoint AntiSpam SE (RAPID) rulegroup: **RPDENGINE** or **RPDASIA** (in Asia)

If you do not see the appropriate rulegroup, enter the **Rule Group Name** and click **Install**. When you click **Update Now**, the installed rulegroup is updated. When you click **Install**, the latest version of the specified rulegroup is installed. Note: Updating or installing rulegroups can take a few minutes.

Anti-Spam Updates

Install/Update Rule Groups

Rule Group Name:

	Rule Group Name	Expiration Date	Delete
<input checked="" type="checkbox"/>	default	2007-09-24	×
<input type="checkbox"/>	mtaverify	2006-03-15	×

(Warning: Installing or updating rule group(s) will interrupt the services.)

Set Automatic Update & Proxy Server

Update all rule groups every week

Use Proxy Server:

Host:

Port:

User ID:

Password:

3. Select **Update all rule groups every week**. If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**. When you are done, click **Apply** to save your changes. Repeat on the other RazorGate.
4. Go to **Anti-Spam > Relay List**. Enter the IP address of each Exchange server from which this router should accept messages for transmission to the Internet. (You could enter the hostnames of the Exchange servers, but IP addresses are more reliable.) Click **Add** for each address you enter. Repeat on the other RazorGate.

Set Relay List

Specify networks and domains whose messages may be relayed to remote hosts.

IP Network or DNS Domain:

1 to 1 of 1 <Prev | Next>

<input type="checkbox"/>	10.0.12.97	IP Network or DNS Domain
<input type="checkbox"/>	10.0.12.97	IP Network or DNS Domain

- Go to **Anti-Spam > RBL Host List**. If the service is disabled, click **Enable it**. If you have subscribed to an RBL service, add the service's host name to the **RBL Host List** page. Mirapoint recommends subscribing to an RBL service, or setting up a local RBL server to block connections from known spam propagators by checking the connection source against a list maintained by a trusted third-party. See the Wikipedia article on [DNSBL](#) for more information.

Repeat on the other RazorGate.

Set RBL Host List

Use this page to configure Realtime Blackhole List checking so all incoming mail is checked against the RBL boycott list and acted on as specified.

RBL checking is currently disabled.

RBL Host:

No items in list

Set RBL Check Action

Reject the message and send a "bounced" message to the sender

Insert "X-Junkmail: RBL" header to the message

(Note: Other Anti-Spam functions may remove this header)

- Optional: If you plan to set up Junkmail filtering, select the **Insert "X-Junkmail:RBL" header to the message** option.

When you are done, click **Apply** to save your changes.

Repeat on the other RazorGate.

- Go to **Anti-Spam > Reject List**. Enter the domain name of any known spam sites if your site lacks access to RBL service or there

are sites that you know you want to block. Click **Add** for each address you enter.

Repeat on the other RazorGate.

Set Reject List

Specify networks and domains whose messages will be blocked; you may use a partial IP address.

IP Network or DNS Domain:

1 to 1 of 1 <Prev | Next>

IP Network or DNS Domain
<input type="checkbox"/> spamCity.com

Setting SMTP Security Checks

To configure SMTP service options, follow these steps on each RazorGate.

Leave at default options not mentioned in this procedure.



When transmission security is important, use of SSL is recommended. Within open organizations protected by firewall, it is less of an issue. Individual messages can be encrypted using alternate methods.

1. Go to **Home > System > Services > SMTP > Main Configuration**. Do not enable or start the service until the end of this procedure.
2. In the **Supported Connections** area, select these options:
 - ❖ **Allow STARTTLS (Inbound Connections)**: Encrypted incoming connections are supported.
 - ❖ **Allow STARTTLS (Outbound Connections)**: Outgoing connections are encrypted.

Leave **Require Secure Authentication (SSL)** deselected.

Supported Connections

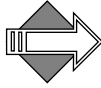
Require Secure Authentication (SSL)

Allow STARTTLS (Inbound Connections)

Allow STARTTLS (Outbound Connections)

3. Accept the default settings in these areas of the page:

- ❖ Inbound Connection Settings
 - ❖ Outbound Connection Settings
 - ❖ SMTP Authentication Settings
 - ❖ Mail Queue Settings
4. In the **Routing Settings** area, select **Use LDAP Routing: For Junk Mail Manager** and click **Modify**. Then select **When using LDAP Routing, use: "MX" record**.



The MX record option allows the pseudo-host MX record to be used to route messages to the Exchange server if the JMM server is unavailable.

Routing Settings

Use LDAP Routing:

When using LDAP Routing, use: "MX" Record "A" Record

Local Message Router:

Outbound Message Router:

Accept the defaults for the other routing options.

Repeat on the other RazorGate.

5. MailHurdle server only: In the **Masquerade Settings** area:
- ❖ **Masquerade all messages as this domain:** If your site has multiple Exchange servers in different subdomains, and you want outgoing e-mail to be addressed from your main domain, type your site's primary (standard) domain name. **Note:** When you set a masquerade, the masquerade name must be a valid Exchange mail domain.
 - ❖ **Use LDAP for masquerade information:** No. This option would cause the RazorGate to get masquerade information from Active Directory, something you probably do not need to do.
 - ❖ (optional) **Do NOT masquerade these headers:** You could select the Sender option; Mirapoint recommends masquerading the From and Reply-To headers, so leave those unselected.

Masquerade Settings

Masquerade all messages as this domain:

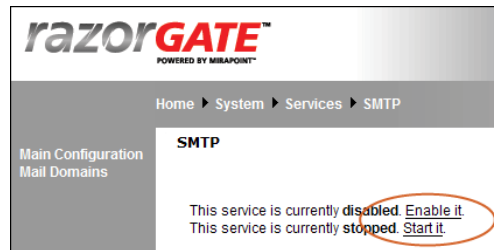
Use LDAP for masquerade information: Yes No

Do NOT masquerade these headers: From Reply-To Sender

Click **Modify** at the bottom of the **SMTP > Main Configuration** page to save any changes you make.

6. Click **SMTP** in the top navigation bar to return to the SMTP service page. If the service is disabled, click **Enable it**. If the service is stopped, click **Start it**.

Repeat on the other RazorGate.



Configuring Inbound Routing—RGs + JMM Security Deployment

Inbound routing and security screening is done on both RazorGate appliances. One acts as the JMM server and the other routes mail through it so spam can be quarantined. This configuration ensures that mail continues to flow even if one of the RazorGate appliances fails (although spam is not quarantined if the JMM server is down).

JMM is enabled on both RazorGate appliances. Both run MailHurdle, Antivirus, Antispam, and are inbound routers. One is designated as the JMM server and is set up to host JMM users. The other is designated as the MailHurdle server and outbound router.

The MailHurdle server screens mail and then sends all messages to the JMM server. The JMM server quarantines spam and sends valid messages to the Exchange server. A **trusted host** relationship allows the two RazorGate appliances to scan for each other.

About Exchange and Active Directory

You will need the hostname and IP address of your Active Directory server and each Exchange server in your messaging network. (Your

Active Directory server might be on the same machine as your Exchange server.) Enable global catalog on Active Directory port 3268.

You also need the **bindDN** (bind distinguished name) of the Active Directory database tree. Steps to determine this information are presented in [“Getting the Active Directory bindDN” on page 126](#).

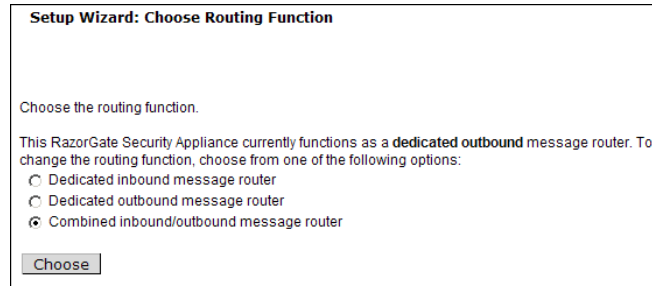
If each of your site’s Exchange servers serves a single domain, or a single Exchange server services multiple domains, you can use the LDAP configuration as described in the following sections. However, if a single domain spans multiple exchange servers and users in the same domain reside on different Exchange servers, you must set up per-user domain routing. To do this, Mirapoint recommends that you find an unused attribute in Active Directory, use it to record the user setting for Mailhost, and set up custom mappings for **Ldap Setquery user:Mailhost** on the **LDAP User Queries** page. This is step 7 of the [“Setting Active Directory Routing—RGs + JMM Security,”](#) procedure.

Setting Active Directory Routing—RGs + JMM Security

On each RazorGate use the **Setup Wizard** to configure JMM with Active Directory LDAP routing by following these steps.

1. Go to **Home > System > Setup Wizard**. Navigate through the initial Setup Wizard pages by clicking **Next**. The first several pages provide options that you should have already set in the Basic system setup described on the Quick Start Setup card shipped with your appliance or in the procedures outlined in the [“Initial Setup Common to All Deployments” on page 38](#).
2. On the **Choose Routing Function** page, select **Combined inbound/outbound message router**. Click **Choose** to confirm your selection. Click **Next** to continue.

Repeat on the other RazorGate.

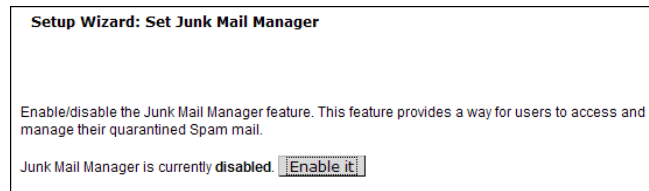


3. On the **Set Disk Write Cache** page, you do not need to make any changes; click **Next** to continue.
4. On the **Set Relay List** page, an IP address should already be set (you did this in step 4 on [page 157](#)). If not set, enter each host IP address or network that the RazorGates should accept messages from for transmission, click **Add** after each entry. For class A networks, use the first octet; for class B networks, the first two octets; for class C networks, the first three octets.
Click **Next** to continue.

Repeat on the other RazorGate.

5. On the **Set Junk Mail Manager** page, click the **Enable it** button. This takes some time to complete. Click **Next** to continue.

Repeat on the other RazorGate.



6. On the **Choose Routing Method** page, select **Route via Microsoft Active Directory**.

A confirmation page with red text displays. Click **Confirm**.

For the **LDAP Server** option, type the name of at least one Active Directory server plus the port (usually 3268). For example, **ldap://exchange.example.com:3268**, and click **Add**.

Repeat on the other RazorGate.

Click **Next** to continue.

Setup Wizard: Choose Routing Method

Choose the method used to route local messages to their mailboxes.

Route via Microsoft Active Directory

- On the **LDAP User Queries** page, under the heading **Set Base DN**, click **Use Default BaseDN**. All the user query filter and attribute names appear automatically. (If needed, you can use the **MailHost attribute** option for custom mappings as described in [“About Exchange and Active Directory”](#) on page 161).

Set Base DN

The Base DN (Distinguished Name) specifies a subset of entries in the LDAP server that will be used in an LDAP query. Click **Use Default Base DN** to get default Base DN from your LDAP server.

Base DN: DC=exchange,DC=example,DC=com

Set Use Default Base DN

- In the **Set Credentials** area, enter the bindDN for accessing Active Directory. For example, **CN=Administrator, CN=Users, DC=exchange, DC=example, DC=com** and the corresponding administrator password. Note: This is not optional for Active Directory. Click **Set**. For instructions on getting the Active Directory bindDN, see [“Getting the Active Directory bindDN”](#) on page 126.

Set Credentials (Optional)

Specify the Bind DN and password to access your user records. Leave blank if your LDAP server supports anonymous

Bind DN: CN=admin, CN=Users, DC=doce

Password: *****

Set

- Under the **Test Query** heading, type a valid user e-mail address in your Active Directory database and click **Test**. The **mail** and **cn** (full name) values appear for that e-mail address.

Test Query
 Use this tool to send a test query to your LDAP servers.

E-mail address:

Test:

Result:

Attribute	Value
mail	test1@example.com
cn	Test1

Click **Next** to continue.

Repeat on the other RazorGate.

10. Do not modify the **LDAP Mail Group Queries** page. Mail group queries do not have to be configured at this time. (Configuring mail groups requires additional information about the Active Directory schema.)

Click **Next** to continue.

11. On the **Junk Mail Manager Domain to Host Mapping** page, add each mail domain at your site as a **JMM Domain**; repeat as needed. Refer to the “Worksheet” on page 144 for the necessary information. (Table 10 shows the correct settings for an example domain).



This is a critical part of the configuration, failing to set these options correctly could result in a failed configuration requiring re-install.

To map a JMM domain for each Exchange mail domain:

- a. **Junk Mail Manager Domain:** Enter the fully-qualified name of the Exchange mail domain. (This will create a JMM domain that corresponds to the specified mail domain.)
- b. **Junk Mail Manager Host:** On the JMM server, enter **localhost**. On the MailHurdle server, enter the fully-qualified pseudo-host name. Dual MX records must exist for the pseudo-host that define a primary route to the JMM server and a secondary route directly to the Exchange server, as described in [“DNS Records Required for JMM Configuration” on page 142](#).
- c. **Mail Host:** Enter the fully-qualified hostname of the Exchange server. (This is used for Active Directory schemas that do not provide this LDAP attribute.)
- d. Click **Add** to create the JMM domain.

If the Exchange server has users in multiple DNS domains, repeat the above substeps to create a JMM domain for each.

Table 10 Settings for Domain, JMM Host, and Mailhost

Option	MailHurdle Server	JMM Server
JMM Domain	example.com	example.com
JMM Host	jmmServer-exchangeServer.example.com (pseudo-host)	jmmServer.example.com (local host)
Mail Host	exchangeServer.example.com	exchangeServer.example.com

Repeat on the other RazorGate.

- Click **Close** to exit the Setup Wizard. (To view the configuration summary before exiting the Setup Wizard, click **Next** four times to navigate through the remaining setup wizard pages.)

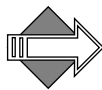
Adding Junk Mail Manager User Accounts

The Junk Mail Manager server must have special user accounts set up for it to quarantine mail properly. You can add JMM user accounts several different ways. We recommend using Active Directory LDAP to autoprovision users:

Go to **Home > Junk Mail Manager > Configuration** and enable **LDAP Autoprovisioning** by clicking the **Enable it** button. This allows JMM user accounts to be automatically created when spam mail is identified for any users in the Active Directory database.

Repeat on the other RazorGate.

Alternately, you can create a comma separated text file of user accounts and import it to add the user accounts. To bulk add user accounts from a text file you create, see [“Bulk Account Provisioning for JMM” on page 461](#) in the Administration Tasks part of this book.



There are many configuration options for Junk Mail Manager, which are fully discussed in [Chapter 10, “Using Junk Mail Manager \(JMM\)”](#) of the Administration Tasks part of this book.

Setting Default Authentication

You must use the CLI to set the authentication. Telnet to each RazorGate and log in as administrator; replace *hostname* with the name of the RazorGate appliance each time:

```
User: telnet hostname.yourdomain.com
OK hostname.yourdomain.com admin 3.8 server ready
User: Administrator
Password:
OK User logged in
```

Enter this command on each RazorGate to set the authentication type:

```
hostname.com> Auth Set Default Plaintext:Ldap
OK Completed
```

Repeat on the other RazorGate.

Keep your CLI window open for the next two procedures.

Setting Trusted Hosts for Multi-Tier Installations

JMM requires that you establish trust relationships between the various appliances in your messaging network. This involves two CLI commands, **Key New** and **Trustedhost Add**.

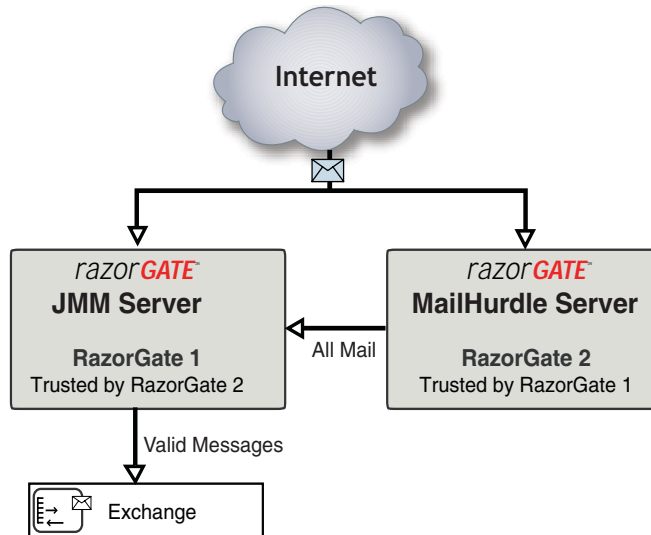


Figure 6 Trusted Host Relationships In A Multi-Tier Environment

To configure trust relationships, follow these steps:

1. On each RazorGate, run the **Key New Mta** command to create a public key for the local Mail Transfer Agent (MTA). This command creates a public key that establishes the trusted host relationship.

```
hostname.com> Key New Mta "" "" ""  
OK Completed
```

2. Make sure DNS "A" and "PTR" records exist for each host that is to be in the trusted host group. On the JMM server, use the **Dns Lookup** command to verify that the appropriate DNS records exist for the MailHurdle server. On the MailHurdle server, use **Dns Lookup** to verify that the appropriate DNS records exist for the JMM server. For example, enter the following commands where *hostname* is the hostname of the appliance you want to verify and *ipaddress* is the numeric address returned by the **type=A** lookup:

```
hostname.com> Dns Lookup hostname type=A  
OK Completed  
hostname.com> Dns Lookup ipaddress type=Ptr  
OK Completed
```

Repeat on the other RazorGate.

3. On each RazorGate, use the **TrustedHost Add** command to add the other RazorGate as a trusted host. The *hostname* is the appliance at the other end of the connection:

```
hostname.com> Trustedhost Add mtagroup hostname.example.com "http:"  
OK Completed
```

The **http:** argument says to retrieve the public key from the HTTP server on *hostname*, which must be DNS resolvable. Until you run **Key New** on that host (step 1), the public key does not exist.

Repeat on the other RazorGate.

This completes the CLI setup of this deployment. Enter **exit** in each window and return to your browsers on each RazorGate to finish the setup by following the remaining procedures.

Configuring Outbound Routing

Configuring outbound routing involves setting a RazorGate server as “Smart Host” (outbound router) on the Exchange server.



We recommend setting the MailHurdle server as the outbound router in this deployment.

To set outbound routing on the Exchange server, follow these steps to specify which RazorGate acts as the outbound router (“Smart Host”). You might want to refer to one of these Knowledge Base articles first.

For Microsoft Exchange 2003 (KB Article 821911):

<http://support.microsoft.com/kb/821911>

For Microsoft Exchange 2000 (KB Article 257426):

<http://support.microsoft.com/kb/257426>

1. Log in to your Exchange server as administrator and go to **Exchange System Manager**. A two-paned window opens.
2. In the left pane tree view, click **Servers > *ServerName* > Protocols > SMTP > Default SMTP Server**; where *ServerName* is the name of the Exchange server.
3. Right-click **Default SMTP Server** and point to **Properties**. The **Default SMTP Server Properties** dialog box opens.
4. Open the **Delivery** tab and click **Advanced**. The **Advanced Delivery** dialog box opens.
5. In the **Smart Host** option enter the fully-qualified hostname of the RazorGate that you set as the MailHurdle server and click **OK**.
6. The **Default SMTP Server Properties** dialog box re-opens, click **OK** again.

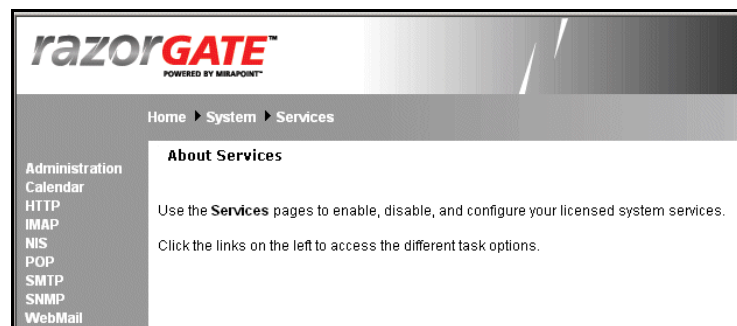
This completes the needed configuring on the Exchange server for this deployment.

Enabling and Starting Services

Enabled services start automatically when the system boots. The **Administration** and **HTTP** services are always enabled and started. Services you choose not to start will not be available.

To enable and start services, follow these steps on each RazorGate.

1. Go to **Home > System > Services**. Click the name of a service in the page menu to access the service's main page. Note: Only licensed services display page links.



2. At this point, most services have already been enabled and started. The following might still need attention.
 - ❖ Ensure that **Calendar** and **NIS** (if present) are disabled.
 - ❖ **POP** and/or **IMAP** must be enabled and started if you set a proxy (described in [“Setting Connection Proxies” on page 136](#)). On the main page for each service, click the **Enable It** link to enable the service if it is not already enabled, then click the **Start It** link.
 - ❖ **SNMP**—Simple Network Management Protocol (SNMP) service allows consoles to monitor selected information about Mirapoint systems. This is useful if your site has an SNMP management facility.

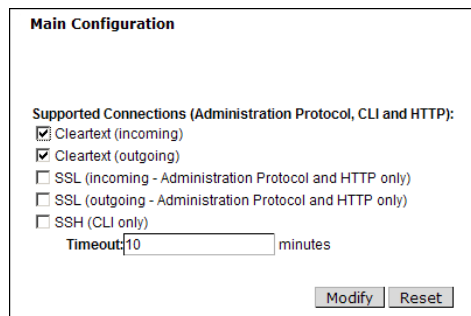
To read more about SNMP see [“Monitoring External Systems via SNMP” on page 253](#) in the Administration Tasks part of this book.



Resetting the Administration Timeout

Setting the timeout to 60 minutes is recommended while you are configuring the system. Once you have completed the configuration procedures, return to the **Home > System > Services > Administration > Main Configuration** page and set the **Timeout** back to **10 minutes** for security.

Click **Modify** to save your changes.



This completes the configuration of the RazorGate with Junk Mail Manager Security Deployment for Exchange. Finish by verifying the configuration by completing the following steps.

Verifying the RazorGate with JMM Security Setup

Now that you have finished configuring Junk Mail Manager and your directory service, please verify that everything is working properly.

1. Log in to an external mail client, such as Yahoo, and send a regular (non-spam) test message to an Exchange user account for which you have the login; for example, **test1@exchange.example.com**.

This email should be delivered to the user's Inbox. To check, log into Exchange (<http://exchangehostname/exchange>) as that user and look for message. Also go to **Home > Logs/Reports > Mail > Detailed** to see how the test message was handled.



Due to MailHurdle delay, you must expect to wait at least 5 minutes before the mail arrives.

2. Send a GTUBE test message to the account (information below). This email should be tagged as spam and sent to the user's Junk Mail Manager folder. To check, log into Exchange as that user and look for the JMM **Welcome** message, and click the JMM link. Also go to **Home > Logs/Reports > Mail > Detailed** to see how the test message was handled.

You can download GTUBE (Generic Test for Unsolicited Bulk Email) from <http://gtube.net/gtube.txt>. The test message looks like this:

```
Body: This is the GTUBE, the
Generic
Test for
Unsolicited
Bulk
Email
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-
EMAIL*C.34X
```

Next Steps, RG with JMM Security Deployment

Now that you have your RazorGates up and running, there are a number of additional features you can configure according to your site requirements:

- ◆ **Schedule Software Updates:** In addition to antivirus and antispam updates, you can schedule MOS update checks through the Administration Suite **System > Utilities > Updates > Update Check** page. For more information, see the Administration Suite online help.
- ◆ **Refine Junk Mail Manager:** There are many configuration options that you can set for Junk Mail Manager. See [“Using Junk Mail](#)



[Manager \(JMM\)” on page 443](#) procedures given to finish setting up your Junk Mail Manager RazorGate.

- ◆ **Limit TCP Connections:** Mirapoint recommends limiting TCP connections. See [“Limiting TCP Connections” on page 90](#) for how to deter denial-of-service attacks.
- ◆ **Set IMAP and/or POP Connection Proxies:** If you want the RazorGate appliances to proxy IMAP or POP connections, see [“Setting Connection Proxies” on page 136](#) for details.



Multi-Tier, Multi-Appliance Deployment

In a multi-tier deployment, multiple appliances are used to perform the various security and messaging functions. You configure the necessary functions on each machine and define trusted relationships between the machines so they can share data. This chapter describes how to set up each function. For more information about multi-tier deployments, refer to the *Mirapoint Administrator's Planning Guide*.

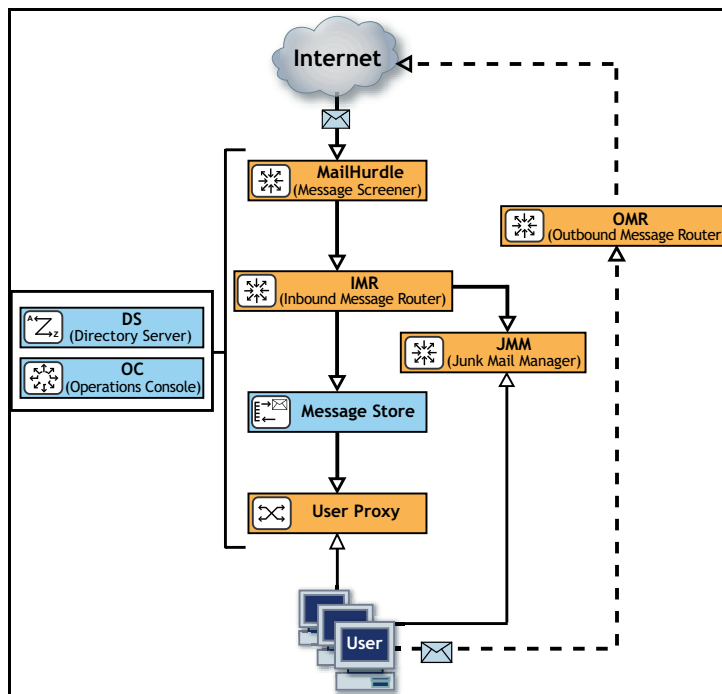


Figure 7 Multi-tier Deployment Example

Before You Begin

Before you begin configuring your multi-tier appliances, make sure that you have read [Chapter 1, “All Deployments Start Here,”](#) and completed the tasks described, including:

- ◆ [Pre-Configuration Checklist](#) (as applicable):
 - ❖ Domain Name System (DNS) setup
 - ❖ Lightweight Directory Access Protocol (LDAP) setup
 - ❖ License requirements defined (licenses are implementation specific)
 - ❖ Backup requirements defined
 - ❖ Secure Sockets Layer (SSL) certificates purchased
- ◆ [Prerequisites](#):
 - ❖ Hardware installation
 - ❖ DNS server database records setup
 - ❖ Basic system setup (described on the Quick Start Setup card shipped with your appliance)
- ◆ [Initial Setup Common to All Deployments](#):
 - ❖ Secure administrator account setup
 - ❖ Appliance clock setup
 - ❖ Network settings verification, redundant DNS server setup
 - ❖ License installation
 - ❖ Service reporting setup
 - ❖ Software update installation
 - ❖ Restricted administrator access setup
 - ❖ Secure administrator login (SSL) setup

Multi-Tier Terminology

The following terms are used to describe multi-tier configurations:

- ◆ **Function**—A security or messaging task performed by one or more appliances in the Mirapoint messaging network. The eight primary functions are:
 - ❖ Security Screening (MailHurdle, Anti-Spam, Anti-Virus)
 - ❖ Junk Mail Manager (JMM)
 - ❖ Inbound Message Router (IMR)
 - ❖ Directory Server (LDAP)
 - ❖ Message Store
 - ❖ User Connection Proxy (User Proxy)
 - ❖ Outbound Message Router (OMR)
 - ❖ Operations Console (OC)
- ◆ **Tier**—One or more appliances performing the same functions. The functions listed above can be distributed across one to eight tiers.

Configuring a Multi-Tier Deployment

In a multi-tier deployment, you need to configure each appliance according to its role in the messaging network.

The Getting Started below describes actions you need to take to configure each appliance. The function-specific configuration tasks you need to perform are then presented according to the path a message takes through the messaging network:

1. Security Screening (RazorGate Appliances).
2. Directory Services for User Data (Mirapoint Appliances).
3. Routing (RazorGate Appliances)
4. Message Store and Calendar (Mirapoint Appliances)

Getting Started

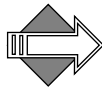
To get started with your multi-tier configuration, perform the tasks described in the following sections:

- ◆ Accessing the Administration Suite
- ◆ Accessing the Command Line Interface (CLI)
- ◆ Checking for Licenses
- ◆ Setting the Administration Timeout

Accessing the Administration Suite

You use the Administration Suite to perform most RazorGate and Message Server configuration tasks. To access the Administration Suite, go to **http://hostname/miradmin**, where *hostname* is your appliance's fully-qualified domain name. If you need to configure multiple systems, you might want to open multiple browser windows and log in as administrator to each system so you can configure them at the same time.

The Administration Suite displays function links at the left and a navigation bar at the top that tracks your current location within the page hierarchy. The **Site Map** link (in the upper right corner) displays links to most pages.



If you are accessing the Administration Suite for the first time, the Setup Wizard displays. You need to use the Setup Wizard to perform the basic configuration tasks described in [“Completing the Setup Wizard” on page 39](#) before continuing.

Accessing the Command Line Interface (CLI)

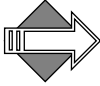
To access the CLI, telnet to the appliance on the default telnet port (port 23) and log in to the CLI as the **Administrator**:

```
User: telnet hostname.domain.com
OK hostname.domain.com admind 3.8 server ready
User: Administrator
Password: password
OK User logged in
```

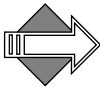
The *hostname* is the appliance's fully-qualified domain name, and the *password* is the secure password you configured.

Checking for Licenses

To verify that you have the licenses you need, go to **Home > System > Utilities > License** page on each appliance to view the installed license keys. Which licenses you need for a particular appliance depends on the functions that it will perform in your multi-tier deployment.



The MailHurdle license does not display; it is part of the Anti-Spam license.



LDAP routing requires a license. This license is a prerequisite for many other licensed features including SMTP directory-based routing, IMAP or POP proxying, Group Calendar, and multi-tier shared folders.

Setting the Administration Timeout

You'll want to change the default Administration Suite timeout from 10 minutes to at least 60 minutes while you are configuring each appliance.

Go to **Home > System > Services > Administration > Main Configuration** page and change the **Timeout** to at least 60 minutes. You'll want to change it back to 10 minutes once you are done.

Main Configuration

Supported Connections (Administration Protocol, CLI and HTTP):

- Cleartext (incoming)
- Cleartext (outgoing)
- SSL (incoming - Administration Protocol and HTTP only)
- SSL (outgoing - Administration Protocol and HTTP only)
- SSH (CLI only)

Timeout: minutes

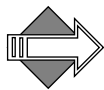
Security Screening (RazorGate Appliances)

Configure the security screening functions on tiers of RazorGates:

- ◆ “MailHurdle” on page 180
- ◆ “Message Screening” on page 181
- ◆ “Junk Mail Manager” on page 185

MailHurdle

When you activate MailHurdle, it can initially delay the delivery of incoming messages. To minimize the impact on existing users, follow this preparation procedure.



If you are deploying a messaging system for the first time, you might not need to perform these preparation steps. Go to “Configuring MailHurdle” on page 181 to configure MailHurdle.

Preparing for MailHurdle Deployment

To prepare existing users for MailHurdle, follow these steps:

1. Using remote mail logs, develop a list of known sites with which your users often correspond. On the **Anti-Spam > Allowed Senders** page, add these sites to allowed senders list and select the **Prioritize** option.
2. Determine which users must have minimal delays imposed on their inbound e-mail. On the **Anti-Spam > Allowed Mailing Lists** page, add these users to the allowed mailing list and select the **Prioritize** option.
3. Alert your users how and when MailHurdle will be enabled.

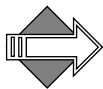
Some users might choose to opt out of MailHurdle—add these users to the Allowed Mailing Lists as described in step 2. Inform users that if they are expecting important e-mail during the transition phase, senders can send a short message first to prime MailHurdle with the appropriate triplet. The priming e-mail might be delayed while the system waits for it to be retried by the sender’s server, but subsequent messages will be delivered quickly.

4. Instruct users to notify an administrator if important e-mail fails to arrive. It is possible that the sending system is not SMTP conformant and needs to be added to the list of known good-mailers. Mirapoint provides a list of nonconformant mailers that is included in the **Mtaverify** rule group.

Configuring MailHurdle

To configure MailHurdle, follow these steps:

1. On the **Anti-Spam > MailHurdle > Configuration** page, if MailHurdle is disabled, click the **Enable It** button.
2. Unless you have separate appliance(s) performing MailHurdle screening, leave the **MailHurdle Server** unset. If you have a separate tier performing MailHurdle screening, add the fully-qualified domain name(s) to the **MailHurdle Server** option.
3. Accept the default **Triplet Timeouts**.
4. On the **Anti-Spam > MailHurdle > Allowed Host** page, if you are configuring a separate tier to perform MailHurdle screening, add the fully-qualified host name(s) of cooperating appliances.
5. On the **Anti-Spam > MailHurdle > Advanced** page, we recommend accepting all the defaults to start with. If you have established reliable lists of Allowed Senders or Allowed Mailing Lists, you might want to enable the **Prioritize** options for them. This bypasses MailHurdle processing for the specified senders and recipients.



Later, you might want to unselect the **Allow Entire IP** option if you find that MailHurdle is too lenient.

Message Screening

The message screener scans messages for spam and viruses:

- ◆ There are two different antispam scanners you can license and configure, **Mirapoint Antispam** (Principal Edition) or **Mirapoint Antispam SE** (Signature Edition). Only one antispam scanner can be

used at a time. For more information about the two scanners, see [“Principal Edition vs. Signature Edition” on page 417](#).

- ◆ There are three antivirus scanners you can license and configure, F-Secure, Sophos, and RAPID. F-Secure and Sophos are **signature-based**, meaning they use databases of known viruses to identify infected messages. RAPID, is **predictive-based**, meaning it uses a database of heuristics to identify messages that *potentially* contain viruses. Because RAPID identifies messages that potentially contain a threat, rather than identifying known viruses, it can only quarantine suspect messages. RAPID-quarantined messages are automatically released after a configurable amount of time, allowing one of the signature-based antivirus engines to re-scan the messages and ensure that viruses are caught.



Mirapoint recommends configuring one signature-based antivirus scanner and the RAPID antivirus scanner. RAPID antivirus must be used in conjunction with a signature-based antivirus scanner; used alone it is ineffective in blocking virus attacks. You can run all three antivirus engines on one system if you have all three licenses.

Configuring Signature-Based Virus Protection

To configure Sophos or F-Secure Antivirus, follow these steps:

1. On the **Anti-Virus** page, select the virus scanner to be configured, Sophos or F-Secure. Only licensed virus scanners are listed.
2. On the **Anti-Virus > Configuration** page, if the scanner is disabled, click the **Enable It** button.

We recommend that you accept the default **Auto-Clean (Delete)** option. You could specify the e-mail address of a Virus Quarantine account if you want to study viruses, but accessing messages with live viruses can be risky.

3. You can modify the formats of your virus notification messages on the **Anti-Virus > Notifications** page. Virus notifications (for the **virus-alerts** DL, sender, and recipients) are disabled by default, because it is usually not necessary to send notifications. The **Summary** is inserted at the top of infected e-mails, so users never see it when the default **Auto-Clean (Delete)** option is enabled. Users

will see the **Deleted** notification when an attachment is cleaned or deleted.

4. On the **Anti-Virus > Updates** page, change the hourly update time from 12 minutes past the hour if it is not a good time for your site. If direct Internet access is blocked by a firewall, designate the proxy server and port through which updates can be retrieved.

Configuring RAPID Antivirus

RAPID antivirus must be used in conjunction with a signature-based antivirus scanner; used alone it is ineffective in blocking virus attacks.

To configure RAPID Antivirus, follow these steps:

1. On the **Anti-Virus > RAPID > Configuration** page, if the scanner is disabled, click the **Enable It** button.
2. Specify an antivirus quarantine **E-mail Address**. This must be the address for a local administrator account that has been assigned the Quarantine Administrator role. The default address is a subfolder of the **Administrator** account; you can specify any valid user.*username.subfolder* as long as the user is a Quarantine Administrator on this system. See [“How Antivirus Quarantine Works” on page 398](#) for more information.
3. Click **Apply**. Afterwards, all messages that potentially contain viruses are automatically sent to the specified address and quarantined for 8 hours. All other messages are delivered normally. The auto-release time can be modified using the CLI. For more information, see **Help About Antivirus**.

Configuring Spam Protection

To configure Anti-Spam scanning, follow these steps.

1. On the **Anti-Spam > Configuration** page, if the scanner is disabled, click the **Enable It** button.

We recommend that you accept the default spam threshold of 50. Higher values incur more false positives; lower values miss spam.

The **Spam-in-Subject** option is useful for delivery to POP users.

The **Junk Mail Explanation** can be enabled to allow users to view the detailed headers that explain the spam scores. Note: This option only displays for **Mirapoint Antispam** (Principal Edition).

Junk Mail Reporting is on by default, and helps Mirapoint tune the antispam scanning rules.



On RazorGate appliances that function as routers or that pass messages to a local message router (typical in multi-tier deployments), disable local recipient check by selecting **Scan messages for any recipient** near the bottom of page.

Click **Apply** to save your changes.

2. Go to **Anti-Spam > Updates**, select the rulegroup, Principal Edition: **default**, Signature Edition (RAPID): **RPDENGINE** or (in Asia) **RPDASIA**, and click **Update Now**. If you don't see the appropriate rulegroup, enter the **Rule Group Name** and click **Install**. If you clicked **Update Now**, the installed rulegroup is updated; if you clicked **Install**, the named rulegroup is installed. Note: Updating or installing rulegroups can take a few minutes.
3. Select **Update all rule groups every week** and click the **Apply** button. If direct Internet access is blocked by a firewall, designate the proxy server and port through which updates can be retrieved.
4. You do not need to set the **Allowed Senders**, **Blocked Senders**, and **Allowed Mailing Lists** at this point during the configuration process.
5. On the **Anti-Spam > Relay List** page, add any host names for which this server should relay messages. For a typical RazorGate inbound message router, the relay list would only contain your organization's domain name(s).
6. On the **Anti-Spam > RBL Host List** page, add the RBL services you'll be using. Mirapoint recommends subscribing to an RBL service or setting up a local RBL server. If your site lacks access to an RBL service, add the numeric IP address ranges of any known spam sites to the **Anti-Spam > Reject List** page.

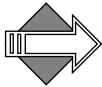
Junk Mail Manager

Use the **Setup Wizard** to configure JMM with the Mirapoint LDAP schema by following these steps.

1. Go to **Home > System > Setup Wizard**. Navigate through the initial Setup Wizard pages by clicking **Next**. The first several pages provide options that you should have already set in the Basic system setup described on the Quick Start Setup card shipped with your appliance or in the procedures outlined in the [“Initial Setup Common to All Deployments”](#) on page 38.

Note: JunkMail Manager and LDAP Routing must be licensed on the appliance to configure JMM. If MailHurdle is licensed, remove its license by using the **License Revoke** command in the CLI. The MailHurdle license is for dedicated MailHurdle appliances.

2. On the **Set Junk Mail Manager** page, click the **Enable it** button. When JMM is enabled, click **Next** to continue.



This step takes a while to complete—you have to wait while the system creates all of the files required for JMM.

3. On the **Choose Routing Method** page, do the following:
 - a. Select **Route via LDAP server with Mirapoint Schema** from the pull-down list.
 - b. The **Confirm Change** page displays. Click **Confirm** to save your changes and return to the **Choose Routing Method** page.
 - c. Add an LDAP server, specified with fully-qualified domain.

Click **Next** to continue.

4. On the **Set Disk Write Cache** page, click **Next** to continue. (You do not need to make any changes.)
5. On the **LDAP User Queries** page, do the following:
 - a. For Base DN, enter **o=miratop** and click the **Set** button.
 - b. Set credentials only if the LDAP server is password protected.
 - c. Test your LDAP queries by entering an e-mail address.

Click **Next** to continue.

6. On the **LDAP Mail Group Queries** page, enter `o=miratop` and click the **Set** button. Test the query with a mailgroup name. When you're done, click **Next** to continue.
7. On the **Junk Mail Manger Domain to Host Mapping** page, if you successfully completed the previous steps, you should see the domains you entered, account defaults, and junk mail summaries. If not, do the following:
 - a. Add each of your site's mail domains as a JMM domain and specify its full JMM host name. For example, for the mail domain *example.com*, the JMM domain is *example.com* and the JMM host name is *jmm.example.com*.
 - b. Specify the JMM host for each JMM mail domain in the **Junk Mail Manager Host** option. If you have multiple JMM-enabled hosts, specify all hosts appropriate for each JMM domain so that mail addressed to that domain can be routed to the correct JMM host. Click **Add** for each entry.

You can also configure your JMM domain names and hostnames on the **Junk Mail Manager Configuration** page.

When you're done, click **Next** to continue.

8. On the **Security** page, enable Antispam and Antivirus, if licensed. Click **Next** to continue.
9. On the **Services** page, enable and start the SMTP service. Click **Next** to continue.
10. On the **Service Reporting** page, verify that your service reporting options are correct. Click **Next** to continue.
11. On the **Configuration Summary** page, review the configuration. Use the **Previous** links to return to pages in the Setup Wizard if you need to make changes. Use the **Next** links to return to the configuration summary. When you're satisfied with the configuration, click **Close** on the Configuration Summary page.

Provisioning Users for JMM

Quarantine users can be autoprovisioned by the JMM host when it connects to an LDAP database that has the necessary attributes set. Autoprovisioning automatically creates a new JMM account

(QTNBOX) from the LDAP database. It also creates the quarantine folder on the JMM client and sends a JMM welcome message to the user.

To enable LDAP autoprovisioning of quarantine folders on the JMM host:

1. Set up your directory service with LDAP records for JMM as described in “Junk Mail Manager LDAP Records” on page 446.
2. On the **Junk Mail Manager > Configuration** page, enable **LDAP Autoprovisioning**.

Trusted Hosts for Multi-Tier Installations

When JMM and security scanning are distributed across separate tiers in a multi-tier deployment, you need to establish trusted host relationships between the tiers. To do this, you use two CLI commands, **Key New** and **Trustedhost Add**.

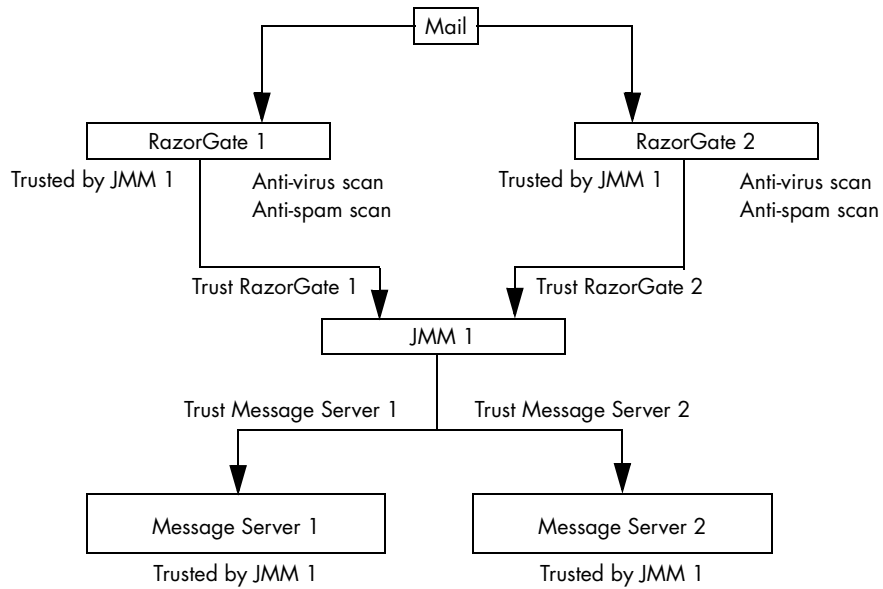


Figure 8 Trusted Host Relationships In A Multi-Tier Environment

To configure trusted host relationships, follow these steps:

1. On each appliance in the trusted group, use the **Key New** command to create a public key for the local mail transfer agent (MTA).

```
Key New Mta "" "" "" ""
```

This command creates a public key to mediate trust relationships.

2. Make sure an “A” record and PTR record exist for each host in the trusted group. On Mirapoint appliances, you can use the **Dns Lookup** command to verify the DNS records. For example, enter these commands:

```
Dns Lookup hostname type=A  
Dns Lookup ipaddress type=Ptr
```

The *hostname* is the name of the appliance, and *ipaddress* is the numeric address returned by the **type=A** lookup.

3. On each connected appliance, use the **Trustedhost Add** command to set up a trusted host relationship. This command needs to be run at both ends of each connection, where *hostname* is the name of the appliance at the other end of the connection:

```
Trustedhost Add mtagroup hostname.example.com "http:"
```

The **http:** argument retrieves the public key from the HTTP server on the specified *hostname*, which must be DNS resolvable. Until you run **Key New** on that host (step 1), this public key does not exist.

Directory Services for User Data (Mirapoint Appliances)

Directory services can be provided by an external LDAP server, such as Active Directory, or by a Mirapoint LDAP Directory Server.

To set up the Mirapoint Directory Server on a tier of Mirapoint appliances, complete the procedure described in “LDAP Lookup” on page 188.

LDAP Lookup

Mirapoint Directory Server can be used for LDAP user authentication and management in a multi-tier deployment. Directory server and

message-store functions can be run on one appliance. Both require high reliability and expandable storage. For higher performance, the Directory Server function can be split off from the message store function onto separate appliances. Two or more Directory Servers are recommended for redundancy.



A Directory Server license is required for other appliances to make LDAP queries, which they must do in a multi-tier environment.

Currently there is no GUI for configuring the LDAP database. One relatively easy approach is to create a file with attribute definitions and user data, then place it on a Web server for import into a Mirapoint Directory Server. You could also cut and paste in the CLI, if the pasted text included both carriage return and linefeed.

Add the following attribute definitions, creating a file named **imported.ldif** on an HTTP server.

```
dn: o=miratop
objectClass: Organization
o: miratop

dn: ou=domains,o=miratop
objectClass: OrganizationalUnit
ou: domains

dn: miDomainname=primary,ou=domains,o=miratop
objectClass: miDomain
miDomainname: primary

dn: miDomainname=subexample.com,ou=domains,o=miratop
objectClass: miDomain
miDomainname: subexample.com
```

The final three lines create LDAP for a delegated domain named **subexample.com**. Add similar definitions for all managed subdomains.

To avoid typing all these lines, and more on the next page, you can download these LDAP definitions from the Mirapoint support site, <http://support.mirapoint.com/secure/docs/imported.ldif> (after customer login) and then modify the file.

To allow COS to control which services are available to users (necessary for JMM, but optional otherwise) add the following lines:

```
dn: ou=cos,o=miratop
objectClass: OrganizationalUnit
ou: cos

dn: miDomainname=primary,ou=cos,o=miratop
objectClass: miDomain
miDomainname: primary

dn: cn=defaultCOS,miDomainname=primary,ou=cos,o=miratop
miService: antispan
miService: antivirus
miService: autoreply
miService: calendar
miService: enterpriseui
miService: filter
miService: forward
miService: getmail
miService: groupcalendar
miService: imap
miService: junkmailmanager
miService: msgexpiration
miService: msgdelete
miService: pop
miService: quota
miService: ssl
miService: webmail
objectclass: miClassOfService
cn: defaultCOS
miMailquota: 0
miMmailexpirepolicy: QTNBOX.* 14 I
miDefaultjunkmailfilter:: IOBNaXJhcG9pbmQtRm1sdGVyLTEuMAOKZm1sdGVyICJTeXNOZW0gSnVuayBNYwIsIFJ1bGUiIFF1YXJhbnRpbmUgI1FUTkJPWC5KdW5rIE1haWwiIGFsbG9mIHN0b3ANCjpvQ0UgaXMgIm5vcmlhbCINCg==
```

The final two attributes are needed only for JMM, but not otherwise for COS. The `miMmailexpirepolicy` says to leave spam messages in the quarantine folder for 14 days after insertion (I) before deleting them. The `miDefaultjunkmailfilter` is actually a base-64 encoding of the following junk mail filtering rule for JMM quarantine.

```
filter "System Junk Mail Rule" quarantine "QTNBOX.Junk Mail" allof stop
:uce is "normal"
```

In LDIF (LDAP data interchange format), double colons indicate binary encoding. You can produce your own binary base-64 encoding with the `base64 -e` command on Linux, or with one of many public websites.

Finally, add a user. This example is for Joe User at **example.com**:

```
dn:mail=juser@example.com,miDomainname=primary,ou=domains,o=miratop
objectClass: mirapointUser
objectClass: mirapointMailUser
cn: Joe User
sn: User
uid: juser
userpassword: secret
mail: juser@example.com
mailhost: doc2.mirapoint.com
miQuarantinehost: doc1.mirapoint.com
miCosDn: cn=defaultCOS,miDomainname=primary,ou=cos,o=miratop
```

It is likely that your organization has a user database somewhere that can be programmatically converted to the above format. You might want to include other LDAP attributes, for instance phone number, but the attributes above are the ones that Mirapoint requires.

The **miQuarantinehost** attribute specifies host name of the JMM. The **miCosDn** attribute calls in the defaultCOS definitions defined on the previous page (the lines with multiple **miService** attributes).

After you have created LDAP user entries for all mail users in your organization, it is time to import the data into the LDAP database. Here are commands to initiate directory service, create a new LDAP tree designated **o=miratop**, and read-in data from the **imported.ldif** file you just created. The web server **ir.example.com** is used for HTTP below. After creating the database, index the important attributes.

```
> telnet ldap 10144
OK ldap.example.com admin 3.8 server ready
User: administrator
Password: adminpass
Service Enable Dir
Service Start Dir
Dir AddDb mira
Dir AddDbsuffix mira o=miratop
Dir ImportLdif o=miratop c http://ir.example.com/imported.ldif
Dir Addindex mira mail eq,pres
Dir Addindex mira cn eq,pres
Dir Addindex mira sn eq,pres
Dir Addindex mira uid eq,pres
Dir Addindex mira objectclass eq,pres
```

You can replace all the LDAP data at any time using the **Dir ImportLdif** command again. No other commands need to be run again.

Routing (RazorGate Appliances)

Configure these functions on tiers of RazorGate appliances:

- ◆ “Inbound Routing” on page 192
- ◆ “Connection Proxy” on page 193
- ◆ “Outbound Routing” on page 194



All routers must have the same locales installed or mail may arrive with unsupported date/time formats.

Inbound Routing

Inbound routing is often done on the same system as message screening. If that’s true at your site, first see “Message Screening” on page 181.

LDAP directory servers are used to assist with inbound routing in a multi-tier configuration. You can use a Mirapoint Directory Server or a third-party LDAP server such as Microsoft Exchange. For information about configuring Directory Server, see “LDAP Lookup” on page 188.



Mirapoint recommends using an LDAP in multi-tier deployments. While you could use a local routing table, it is more difficult to maintain.

To configure inbound routing, follow these steps:

1. On the **System > Routing > Routing Method** page, select either **Route via LDAP Server With Mirapoint Schema**, or possibly with **Non-Mirapoint Schema** if you are sure that’s what you have.
2. The software asks you to **Confirm** your choice.
3. Under the heading **Specify LDAP Servers**, type the name of at least one Directory Server, such as the one you recently configured under “LDAP Lookup” on page 188.
4. On the **System > Routing > User Queries** page, under the heading **Set Base DN**, enter **o=miratop** assuming you closely followed directions under “LDAP Lookup” on page 188, otherwise type the suffix of your LDAP database.

5. Click **Set** to activate. All the user query filter and attribute names appear automatically. **Set Credentials** is not needed for Mirapoint Directory Server, but is likely to be required for third-party servers.
6. Under the **Test Query** heading, type a user e-mail address such as `juser@example.com` or some valid address you added to the LDAP database. The **mail**, **mailhost**, and **cn** (full name) values appear for that e-mail address.
7. The **System > Routing > Mail Group Queries** page does not have to be configured at this time. Further elaboration of the LDAP schema would be necessary to configure mail groups.
8. If this inbound router delivers to multiple domains, for instance to a Mirapoint Message Server with delegated domains, or many servers in different DNS domains, you must set a mail domain for each. There must also be an MX record in DNS for each mail domain.

We recommend that a Message Server manage either multiple delegated domains, or one primary domain, but not both.

On the **System > Services > SMTP > Mail Domains** page, type the name of each mail domain for which this router delivers e-mail. Give the full domain name: everything after the at-sign (@).
9. On the **Home > System Services > SMTP** page, enable and start SMTP service. Make sure LDAP routing is turned on.



Connection Proxy

The outbound message router is often also used to handle proxying. However, the connection proxy requires the same LDAP configuration as the inbound message router. If you use an outbound message router or a dedicated appliance to handle proxying, you must complete the LDAP configuration in steps 1-5 in “Inbound Routing” on page 192.

To configure the connection proxy, follow these steps:

1. If IMAP users connect through this system, set IMAP proxy:
Imap Set Mode Ldaproxy
2. If POP users connect through this system, set POP proxy:
Pop Set Mode Ldaproxy

3. If WebMail users connect through this system, set HTTP proxy:
Http Set Mode Ldapproxy
Or click the **Proxy** button on the **System > Services > HTTP > Mode** page (a GUI interface exists for HTTP proxy only).
4. Require users to authenticate using LDAP:
Auth Set Default Plaintext:Ldap

Outbound Routing

To configure outbound routing, follow these steps:

1. During network configuration, you most likely added a DNS server. For redundancy, outbound routers need at least two DNS servers. If your site has only one DNS server available, try to locate another, or failing that, set up another.

On the **System > Network > Interface** page, under the heading **Set Domain Name Servers**, add another DNS server (or two more).

2. If your site has multiple Message Servers, e-mail should not contain a user's assigned server name in the header. For instance, you probably do not want `ed@mail2.example.com` from one user, and `ann@mail3.example.com` from another user on a different server. To avoid this set the masquerade.

On the **System > Services > SMTP > Main Configuration** page, under the heading **Masquerade Settings**, type the site's primary (standard) domain name in the Masquerade text box, select **Yes** to **Use LDAP for masquerade information**, and click the **Modify** button. You might choose not to masquerade the Sender header, but we recommend masquerading the To and Reply-To headers.

3. If this outbound router accepts (for transmission to the Internet) messages from multiple hosts, or from multiple networks, each host or network must be added to the relay list.

On the **Anti-Spam > Relay List** page, type the name of each host or network for which this router transmits e-mail. Generally it is easier to specify a range of network addresses than many host names. For instance, adding `10.99.99` to the relay list allows transmission for all hosts in the subnet, `10.99.99.0` to `10.99.99.255`.

4. On the **Home > System Services > SMTP** page, enable and start SMTP service.
5. On all on Message Servers that will be transmitting e-mail through this outbound router, set this outbound router as the OMR for SMTP. See “Message Store” on page 195 for instructions.

Message Store and Calendar (Mirapoint Appliances)

Configure these functions on tiers of Mirapoint appliances:

- ◆ “Message Store” on page 195
- ◆ “Group Calendar” on page 197

Message Store

To configure the message store, follow these steps:

1. On the **System > Routing > Routing Method** page, select either **Route via LDAP Server With Mirapoint Schema**, or possibly with **Non-Mirapoint Schema** if you are sure that's what you have. The software might ask you to **Confirm** your choice.

This is not really to configure routing, but autoprovisioning. LDAP routing does not have to be enabled on the message store.
2. Under the heading **Specify LDAP Servers**, type the name of at least one Directory Server, such as the one you recently configured under “LDAP Lookup” on page 188.
3. On the **System > Routing > User Queries** page, under the heading **Set Base DN**, enter **o=miratop** assuming you closely followed directions under “LDAP Lookup” on page 188, otherwise type the suffix of your LDAP database.
4. Click **Set** to activate. All the user query filter and attribute names appear automatically. **Set Credentials** is not needed for Mirapoint Directory Server, but is likely to be required for third-party servers.
5. Switch to the CLI. Enable LDAP autoprovisioning of new users:
Ldap Set Autoprovisioning On

6. Enable LDAP-related features on this server, including autoreply, exceptions, forward, password update, WebMail preferences, and `ldapgui` with this one command:

```
Conf Enable Ldapall
```

7. Require users to authenticate using LDAP:

```
Auth Set Default Plaintext:Ldap
```

8. To allow transmission of e-mail by the outbound router, set OMR. Do this on the **System > Services > SMTP > Main Configuration** page, or do it in the CLI:

```
SmtP Set Omr omr.example.com
```

9. If you want to use the COS facility, enable all the features to be controlled. The `msgexpiration` feature is mandatory for JMM.

Many sites allow antispam, antivirus, autoreply, filter, forward, sender_av, and often sender_as, for all users. If you want to do that, these facilities need not be under COS control, so delete those six or seven lines from the list below:

```
Cos Enable antispam  
Cos Enable antivirus  
Cos Enable autoreply  
Cos Enable calendar  
Cos Enable enterpriseui  
Cos Enable filter  
Cos Enable forward  
Cos Enable getmail  
Cos Enable groupcalendar  
Cos Enable imap  
Cos Enable msgexpiration  
Cos Enable msgundelete  
Cos Enable pop  
Cos Enable quota  
Cos Enable sender_as  
Cos Enable sender_av  
Cos Enable ssl  
Cos Enable webmail
```

10. On the **Home > System Services > SMTP** page, enable and start SMTP service, or do it in the CLI:

```
Service Enable SmtP  
Service Start SmtP
```

11. Also enable and start any of the following services that are licensed and you want to offer: POP, IMAP, and WebMail.

```
Service Enable Pop
Service Start Pop
```

```
Service Enable Imap
Service Start Imap
```

```
Service Enable WebMail
Service Start WebMail
```

Group Calendar

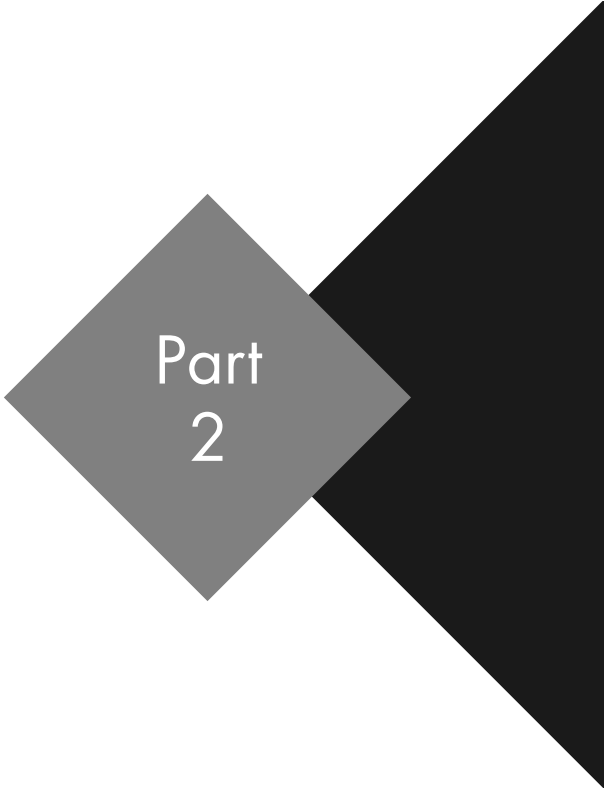
In a multi-tier environment, you must have the LDAP Routing license in order for Group Calendar to work. To configure WebCal group calendar, follow these steps:

1. On the **System > Services > Calendar** page, enable and start calendar service.
2. Ensure that **mailroutingaddress**, **mailhost**, **miUUID**, and **UID** (or some other attribute that you can map to loginID) are included in LDAP user entries. Furthermore, database ACLs might have to be changed so users have write permission on the **miUUID** attribute. (See examples of **Dir AddAclEntry** in the *Mirapoint Administration Protocol Reference*).
3. If current LDAP mail groups are not sufficient for group calendar scheduling, create new LDAP mail groups as needed.
4. To complete Group Calendar configuration, refer to [“Configuring Calendar Options for Domains” on page 274](#) in the Administration Tasks part of this book.

Reset the Administration Timeout

For security, set the administration timeout for a deployed system to 10 minutes. If you increased the timeout during configuration, when you are done configuring the appliance, return to the **Home > System > Services > Administration > Main Configuration** page and set the **Timeout** back to **10 minutes**.

Administration Tasks



Monitoring Tasks

This chapter describes how to monitor system performance, check hardware status, and track down problems. Mirapoint appliances provide several monitoring options, including distribution lists, graphs, and alerts. The following topics are included:

- ◆ [Internal Distribution Lists for Monitoring](#): Default distribution lists for system reports.
- ◆ [Viewing Performance At-a-Glance](#): How to use the performance graphs.
- ◆ [Using the Message Queue](#): Viewing, sorting, and searching messages in the queue.
- ◆ [Viewing Hardware Status](#): How to use the **Storage** page.
- ◆ [Viewing Alerts](#): How to use the **Alerts** page.
- ◆ [Viewing User and/or Administrator Activity](#): How to use the User Audit and Admin Audit features.
- ◆ [Monitoring External Systems via SNMP](#): How to set up SNMP.

Internal Distribution Lists for Monitoring

The default distribution lists shown in Table 11 are created during installation. Mirapoint uses several of these lists to send logs and reports on a scheduled basis. You can add and remove members to these

lists as needed, but can only delete those that aren't used by the system (abuse, mailer-daemon, operator, and nobody).



Mirapoint recommends that each system mailing list be altered to remove Administrator and add the specific system administrators for the system. For a delegated domain's postmaster DL, remove "Administrator" and add the domain administrators individually.

emailNote: DLs beginning with the word *system* are reserved for Mirapoint use. You cannot use "system" as the initial name in a custom DL.

Table 11 Default Mirapoint Distribution Lists

DL Name	Description
system-alerts	Used to notify recipients about conditions that might require human intervention. For more information, see "Viewing Alerts" on page 250 . This list includes Administrator and customer care by default and is reserved for Mirapoint use.
backup-alerts	Used to notify recipients that a backup or restore operation requires changing remote media (such as a tape). For more information, see "Alerts and Completion Status" on page 524 . This list is empty by default and is reserved for Mirapoint use.
backup-status	Used to notify recipients that a backup or restore operation has completed. For more information, see "Alerts and Completion Status" on page 524 . This list is empty by default and is reserved for Mirapoint use.
daily-reports	Used to send detailed information about email traffic and system events at 12:00 a.m. each day. For more information about the included reports see "Receiving Daily and Weekly Reports" on page 475 . This list includes Administrator by default and is reserved for Mirapoint use.
weekly-reports	Used to deliver a summary of the preceding week's email traffic at 12:15 a.m. each Monday. For more information, see "Receiving Daily and Weekly Reports" on page 475 . This list includes Administrator by default and is reserved for Mirapoint use.

Table 11 Default Mirapoint Distribution Lists

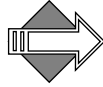
DL Name	Description
postmaster	Required reserved postmaster address (RFCs 2821 and 2822). This list contains Administrator by default. Delegated domain default DL.
abuse	Standard abuse alias. Used to receive information about abuse issues. This list contains Administrator by default and can be deleted.
mailer-daemon	Standard mailer-daemon alias. This list contains “postmaster” by default and can be deleted. (Even if deleted, “mailer-daemon” is used as the From address for bounced mail.) Delegated domain default DL.
operator	Standard operator alias. This list contains “Administrator” by default and can be deleted.
schedule-output	This list includes “administrator” by default.
virus-alerts	This list includes “administrator” by default.
nobody	Standard nobody alias. This list is empty by default and can be deleted.

Viewing Performance At-a-Glance

The **Performance Graphs** show activity on your Mirapoint system. Only applicable graphs display. Monitor the graphs regularly to get a baseline understanding of your system. These graphs, discussed in detail in the following sections, are available:

- ◆ **Performance Gauges:** Show the current CPU usage, system load, and mail queue size.
- ◆ **Mail Graphs:** Show information about SMTP traffic.
- ◆ **POP/IMAP Graphs:** Show information about POP/IMAP traffic.
- ◆ **WebMail Graphs:** Show information about WebMail traffic.
- ◆ **Junk Mail Graphs:** Show junk-mail statistics.
- ◆ **Directory Graphs:** Show LDAP directory usage statistics.
- ◆ **Misc Graphs:** Show information about administration connections.

- ◆ **External Graphs:** Shows external server information.
- ◆ **Disk Graphs:** Show disk usage and performance information.
- ◆ **Network Graphs:** Show network traffic statistics.
- ◆ **CPU Graphs:** Show CPU and load statistics.



The vertical axis of each graph is scaled to show the range of actual values to be presented. The graphs all start at zero.

On most **Performance** pages, the graphs for the current week display by default. The graphs show a one-hour average sampling in the **Week** view, a 10 minute sampling in the **Day** view, and a 20 second sampling in the **Hour** view. The graph plots can contain gaps that correspond to reboots or changes in the system clock setting. These gaps are represented by a red line.

Click **Day** to view today's statistics, **Hour** to view statistics for the last hour. When in the **Day** or **Hour** view, a **Refresh** option displays; this option, when **On** (default), causes the system to update the graph data every fifteen seconds. Click **Off** to stop the automatic updates. Each tick mark along the horizontal axis represents:

- ◆ **Week view:** Each tick is one day
- ◆ **Day view:** Each tick is one hour
- ◆ **Hour view:** Each tick is 10 minutes.

Pie-Chart Categories

Several graphs are pie charts that show percentages of a total by software subsystem (category); the possible categories are:

- ◆ **Administration:** Administration service
- ◆ **Antispam:** Antispam scanning (RAPID Antispam)
- ◆ **Antivirus:** Antivirus scanning (Signature)
- ◆ **Backup:** Backup and restore operations
- ◆ **Basic Services:** Services, such as DNS and the HTTP server, that are always running and are not controlled by the **Service** command
- ◆ **Directory:** Directory Server
- ◆ **Filtering:** Message filtering

- ◆ **Idle:** Unused capacity (CPU Usage chart only)
- ◆ **IMAP:** IMAP information
- ◆ **LDAP Client:** LDAP client operations
- ◆ **Logging:** Log and MUL event generation
- ◆ **Mail Delivery:** Inbound SMTP (local message delivery)
- ◆ **Mail Transfer:** Outbound SMTP (except for local message delivery)
- ◆ **Message Store:** Internal message store management
- ◆ **Monitoring:** System health monitoring activity
- ◆ **Other:** Combination of categories too small to be displayed individually and activity not classified in any other category; on lightly loaded systems, this category can constitute a large percentage of total activity
- ◆ **POP:** POP service
- ◆ **Periodic:** Periodic automatic system self-maintenance activity, including tasks run by the **Schedule** command
- ◆ **Proxies:** IMAP, POP, and HTTP proxy operations
- ◆ **Security:** SSL and SSH operations. **Note:** Secure connections such as HTTPS, IMAPS, and SMTP/TLS show usage under both Security and the corresponding non-secure protocol.
- ◆ **Upgrade:** System software upgrades and patch installation

Using the Performance Gauges

The performance gauges shown in Figure 9 are displayed on the main **Performance Graphs** page. These three dial-type gauges show:

- ❖ **CPU Usage:** Percentage of the system CPU is use.
- ❖ **System Load:** One-minute system load average.
- ❖ **Mailq Size:** Number of messages in the SMTP queue.

You can view the averages over the last day or hour, or select the **Now** view to display an instant update.

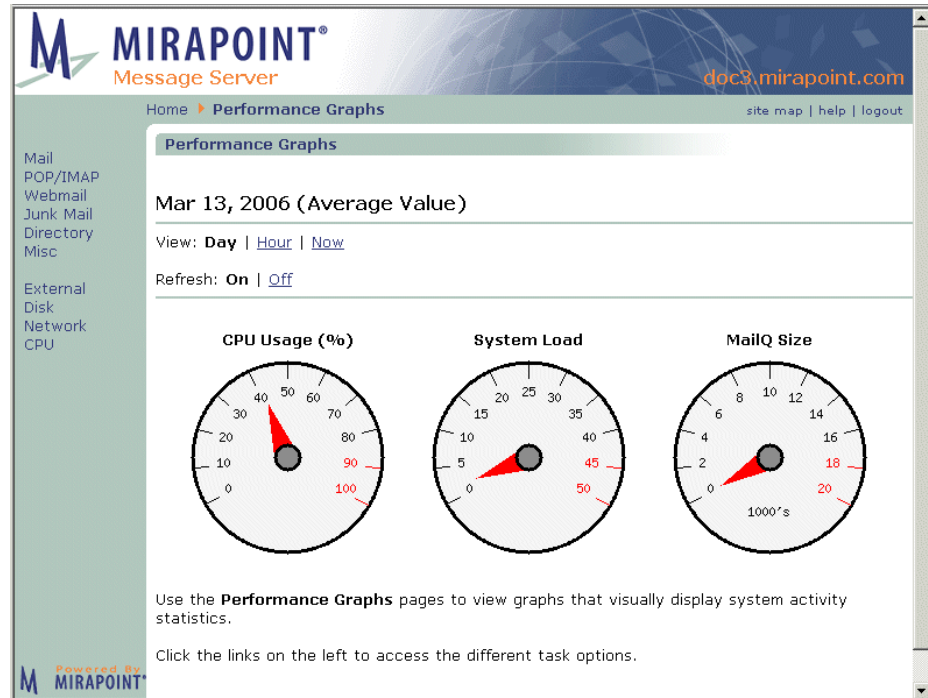
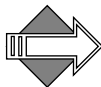


Figure 9 Performance Graphs: Gauges

The top level dashboard shows if the CPU seems to be pegged, or problematic; if so, click the CPU detailed graph at the bottom where the pie chart is to see what is using up the CPU.



CPU at 100% is not necessarily a cause for concern; CPU is not a prime indicator of performance. Certain times of day are notorious for CPU spikes, for example, in the morning when everyone logs on at once.



You might have a problem if your **System Load** stays in the 4.0 to 8.0 range for more than five minutes. If the load exceeds 8.0 for five minutes or more, start looking at other graphs for the cause. A sustained **System Load** spike could indicate a spam attack.

The load trend typically increases over time because more users are using the system, more messages are being processed, or the typical usage profile is changing (for example, users are sending larger attachments). Consider increasing the capacity of the tier that the

system resides in when the load trend moves above an average load of 4.0.

Mail Graphs

The **Mail Traffic** graphs show tick marks along the horizontal axis representing one day of elapsed time in the **Week** view, one hour in the **Day** view, and ten minutes in the **Hour** view.

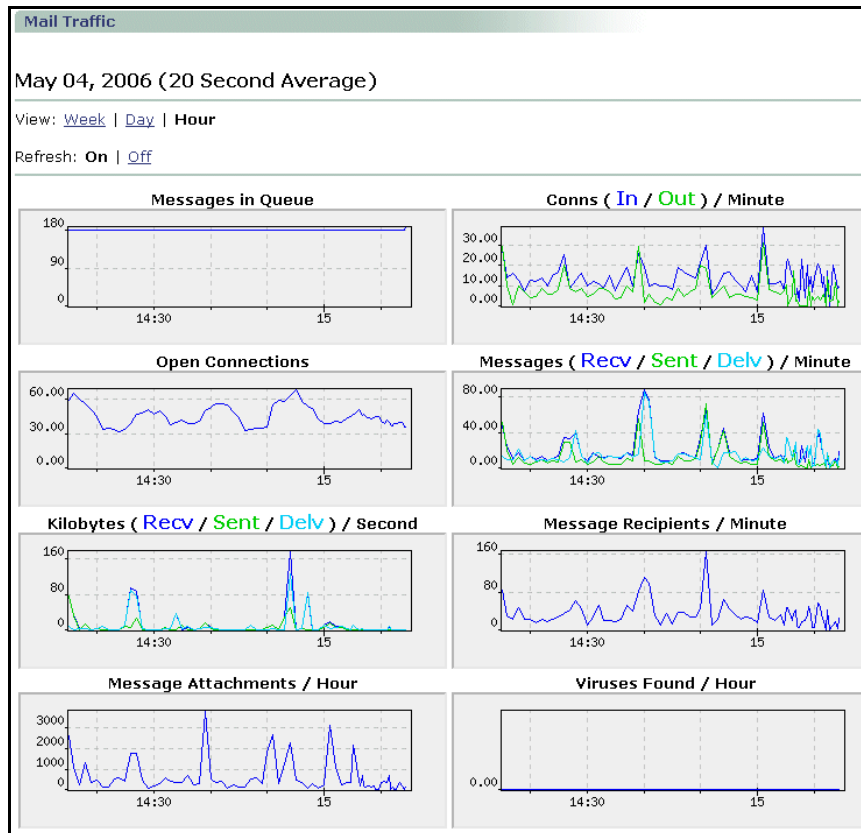


Figure 10 Mail Performance Graphs

Table 12 Mail Traffic Graphs (see Figure 10)

Graph	Description
Messages in Queue	Number of messages currently in the SMTP delivery queue.
Conns (In/Out) / Minute	Number of incoming (In) and outgoing (Out) SMTP connections per minute, shown in different colors.
Open Connections	Number of currently open SMTP connections.
Messages (Recv / Sent / Delv) / Minute	Number of messages incoming (Recv), outgoing (Sent), and delivered locally on the reporting system (Delv) per minute, shown in different colors.
Kilobytes (Recv / Sent / Delv) / Second	Number of kilobytes of message data incoming (Recv), outgoing (Sent), and delivered locally on the reporting system (Delv) per second, shown in different colors.
Message Recipients / Minute	Number of message recipients per minute.
Message Attachments / Hour	Number of received messages attachments per hour.
Viruses Found / Hour	Number of viruses found per hour.

What to Look for in Mail Graphs

Sharp changes in the queue size generally indicate that there's a problem. A growing queue might indicate a problem; however, it can also represent a temporary imbalance between input traffic and deliveries or outbound traffic. If you already know you have a problem, this can tell you about when it started, which is often a vital clue.

POP/IMAP Graphs

The POP/IMAP Activity graphs show a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view.

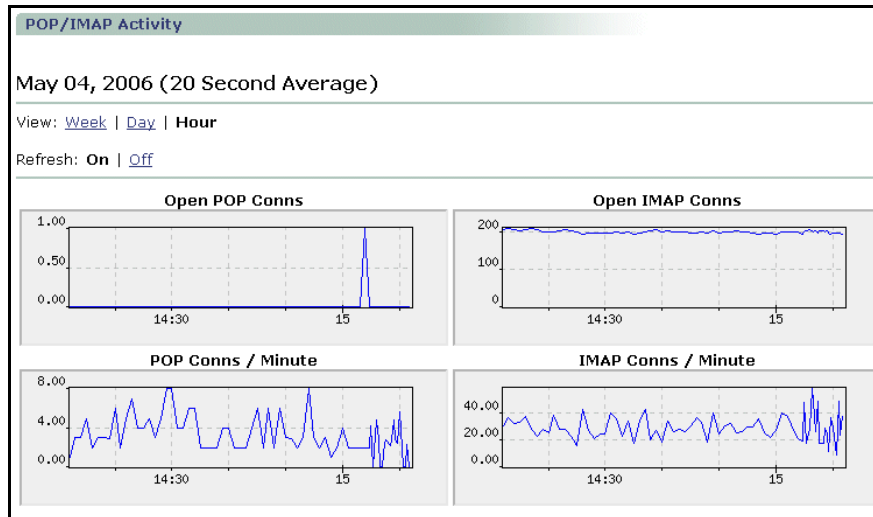


Figure 11 POP/IMAP Performance Graphs

Table 13 POP/IMAP Activity Graphs (see Figure 11)

Graph	Description
Open POP Conns	Number of open POP connections
Open IMAP Conns	Number of open IMAP connections
POP Conns / Minute	Number of POP connections per minute
IMAP Conns / Minute	Number of IMAP connections per minute

What to Look for in POP/IMAP Graphs

The POP connections per minute graph provides an indication of how many users are using POP3. The IMAP connections per minute graph indicates the level of IMAP usage. Expect these graphs to follow standard usage patterns—for example, a substantial increase during the work day.

If the load average indicates a problem, and the CPU utilization indicates IMAP/POP3 as a problem area, then these graphs might show a temporary spike indicating the cause. More investigation in the detailed logs is needed to narrow down the ultimate source of the problem.

WebMail Graphs

The first **WebMail Activity** graph displays the average number of sessions for the previous week, day, or hour that were:

- ◆ Idle for more than 60 minutes (**Dormant**)
- ◆ Active within the last 5 minutes (**Active 5**)
- ◆ Active within the last 60 minutes (**Active 60**)

The second **WebMail Activity** graph displays the average **Logins** and **Logouts** per minute. It shows a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view.

Note: When the idle timeout period elapses, user sessions are automatically terminated. (Users typically don't log out of webmail, they just close the browser window.)

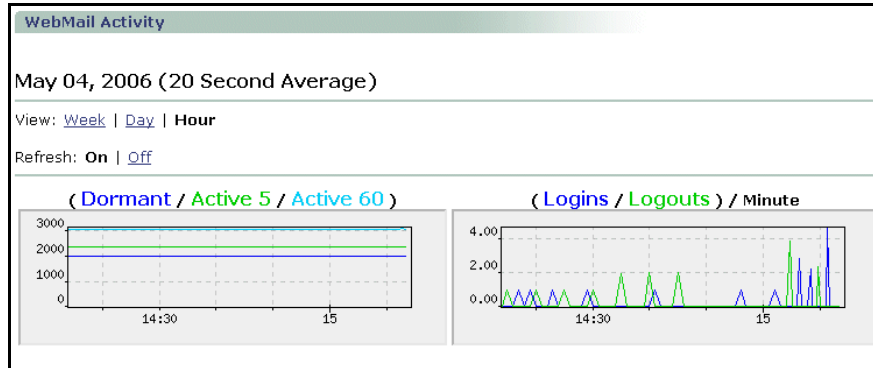


Figure 12 WebMail Performance Graphs



WebMail graphs are a good way to get a baseline understanding of how users on your system are using WebMail.

Table 14 WebMail Activity Graphs (see Figure 12)

Graph	Description
(Dormant / Active 5 / Active 60)	<p>Dormant: The number of sessions that have been idle for more than 60 minutes and less than the WebMail timeout setting, usually 360 minutes.</p> <p>Active 5: The number of sessions that were active within the last 5 minutes.</p> <p>Active 60: The number of sessions that were active more than 5 minutes ago and less than 60 minutes. The performance graph samples this number every 10 minutes and displays that sample on the Today graph, or it displays the average of 6 of these samples on the Week graph.</p>
(Logins / Logouts) / Minute	Number of logins or logouts per minute.

Junk Mail Graphs

The **Junk Mail Statistics** graphs show a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view.

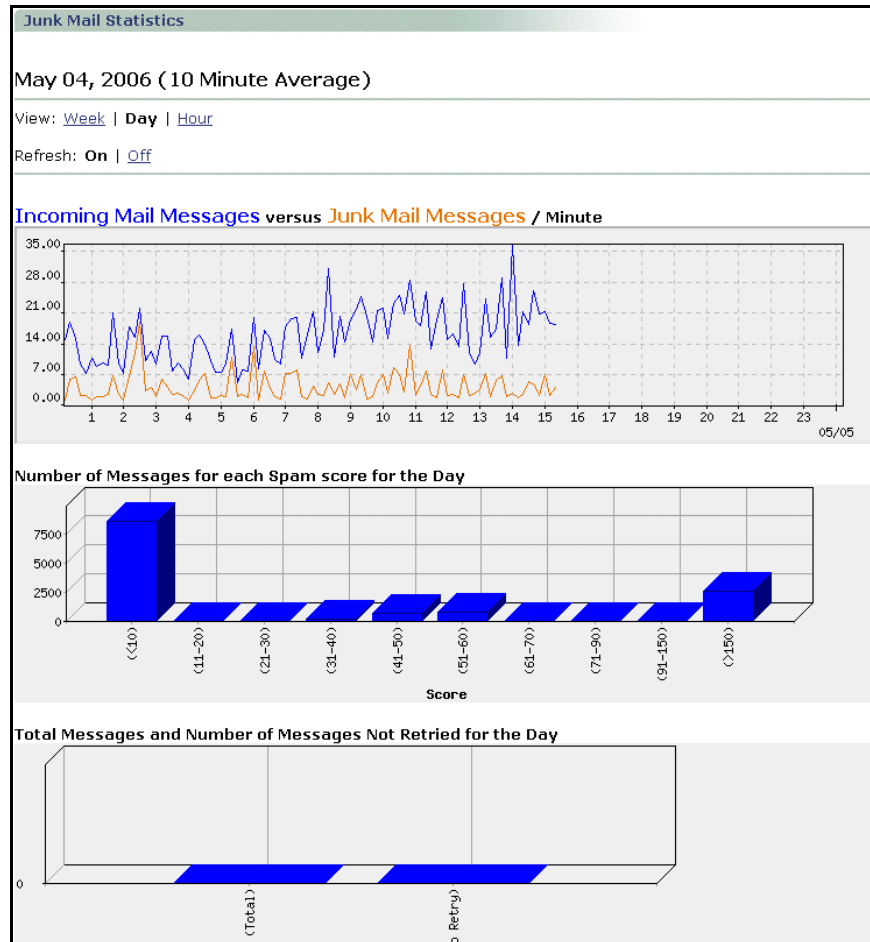
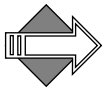


Figure 13 Junkmail Performance Graphs, Detail

Table 15 Junkmail Statistics Graphs (see Figure 13)

Graph	Description
Incoming Mail Messages versus Junk Mail Messages	This graph shows: <ul style="list-style-type: none"> ❖ Incoming messages per minute (blue) ❖ Incoming Junk Mail messages per minute (orange)
Number of Messages for each Spam score for the Day	This bar graph shows the number of messages that fell within each of several ranges of junk-mail scores for the current week, day, or hour. This information can help you use the Anti-Spam > scanner > Configuration page to tune the junk-mail threshold for your email traffic. The Week view shows totals for the current week (starting Monday), the Day view shows totals for today, and the Hour view shows the totals for the current hour. For more information on the Spam score, see “About the Antispam Scanning Rules and Threshold” on page 336.
Total Messages and Number of Messages Not Retrieved for the Day	This bar graph shows two buckets: one depicts the total number of messages received that day; the other, the number of those messages that were not retried against MailHurdle; see below for details. For more information on MailHurdle, see “Working with MailHurdle” on page 388.



In the **Total Messages and Number of Messages Not Retrieved for the Day** graph, the **Total Messages** value represents the total number of messages received in a day (for the selected day). The **No Retry** value represents that no retry was accepted before the Initial-Active timeout (twelve hours by default). It's possible that users send emails during the twelve hour period before midnight, so the present day graph increases the Total count and the next day graph doesn't show those messages in the Total count. The Initial-Active timeout for such messages ends the next day and, if no retry is accepted for any of those messages, then the No Retry value shows those messages in the next day's graph. In that manner, it is possible that the No Retry value is higher than the Total messages value.

What to Look for in Junkmail Graphs

Check the pattern for incoming mails vs. incoming junk mail. This also helps you determine what the UCE threshold should be. If a high volume of spam is getting through, you can raise the UCE threshold using the Content Filtering > Advanced page. For details, see [“Managing Content Policies \(Domain Filters\)” on page 332](#).

You can also look for spam attacks in the junkmail graphs and check the logs to see if you can block IP addresses that are the source of the attacks.

Directory Graphs

The LDAP Directory Statistics graphs show a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view.

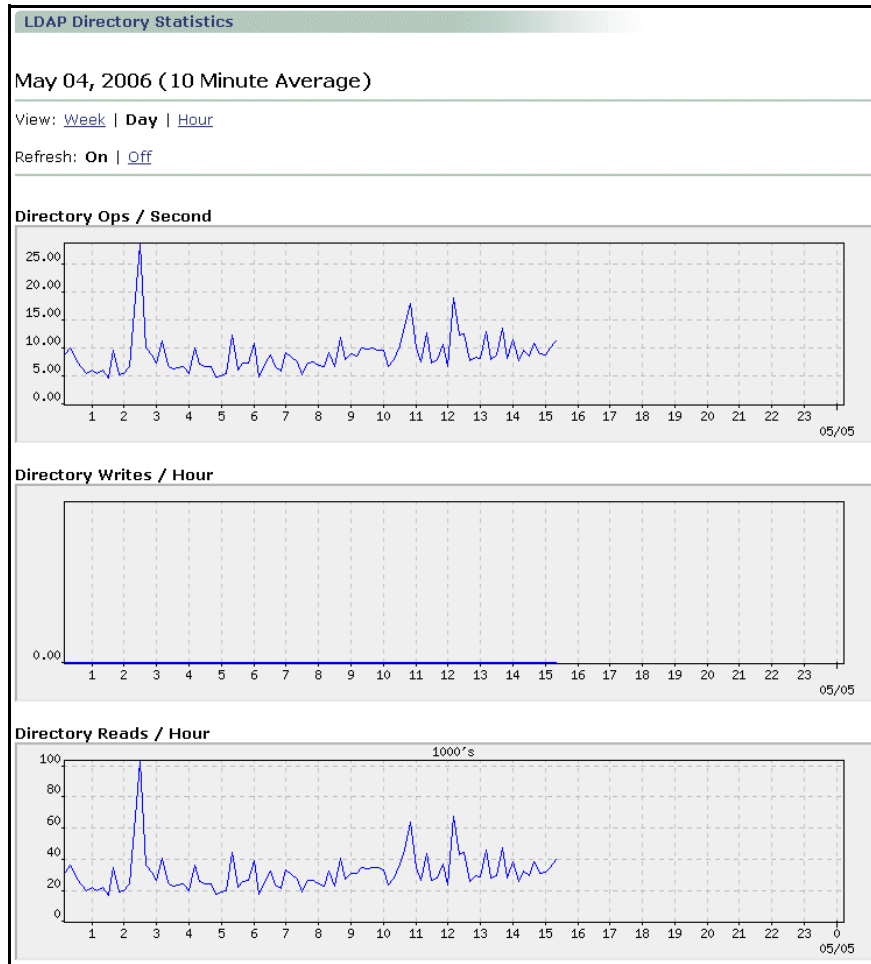


Figure 14 Directory Performance Graphs

Table 16 LDAP Directory Statistics Graphs (see Figure 14)

Graph	Description
Directory Ops / Second	Number of Directory Server operations (reads, writes, binds, etc.) per second
Directory Writes / Hour	Number of Directory Server writes per hour; includes adds, removes, and changes

Table 16 LDAP Directory Statistics Graphs (see Figure 14) (Continued)

Graph	Description
Directory Reads / Hour	Number of Directory Server reads per hour
Entries Added / Hour	Number of Directory Server entries added per hour
Entries Removed / Hour	Number of Directory Server entries removed per hour
Connections / Minute	Number of Directory Server connections per minute
Completed Replications / Hour	Number of replication operations completed per hour

What to Look for in Directory Graphs

The **Directory Operations** graph shows the load on the DS—the number of logins and transfers minus the effect of the cache.

An overloaded directory server can result in user authentication timeouts and message bounces, so it is critical to ensure that your configuration can support the expected load.

For a dedicated DS, the overload point is 3,000 per second. In a mixed environment (Message Server plus directory server), the overload point is 500.

The **Entries Added**, **Entries Removed**, and **Completed Replications** indicate true activity; if any of these graphs indicates activity that has not officially happened, you might have been hacked. Please note: creating or deleting a user results in several operations.

In viewing the **Connections per Minute** graph, a peak could indicate a spam attack.



High disk usage on a directory server-only machine, could indicate that the cache is full. If the number of **Disk Operations** reaches double the amount of **Directory Operations**, your directory server is overloaded. Increase DS capacity before you reach this point and load balance the directory servers with a Layer 4 load balancer.

Misc Graphs

The Miscellaneous Services **Open Admin Connections** graph shows a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view.

Table 17 Miscellaneous Services Graphs

Graph	Description
Open Admin Conns	Number of open administration service connections

What to Look for in the Misc Graph

You should be able to account for every single admin connection listed; that is, if you have 3 connections listed, you should be able to point to 3 connections (which can be Administration Suite or CLI). The maximum number of concurrent administration connections is 100 (this is a hard coded limit).

Problems to look for are when an unexpected increase in connections appear, either in number or in intensity. This might indicate that someone is trying to breach the security of the system, or that some external process that relies on this interface might have gone awry.

Action is required if over time any application that relies on this interface steadily approaches the connection limit and is in jeopardy of going over the limit.

If a site has their own provisioning system, then the numbers can be high. If a site does not have their own provisioning system, then the numbers should never be greater than the number of administrators.

A high number (> 50) indicates a load system on the provisioning system. Actions include: (a) determining if the load is normal, and (b) re-designing the provisioning system to pool administration connections. A system that pools connections can support hundreds of thousands of users with no more than 30-40 connections.

External Graphs

Use the **External Server Monitoring** graph to check the status of systems the Mirapoint depends on. The **External Server Monitoring** graphs show a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view. When multiple external servers are shown on a graph,

each server is assigned a unique color. Statistics display only for configured servers.

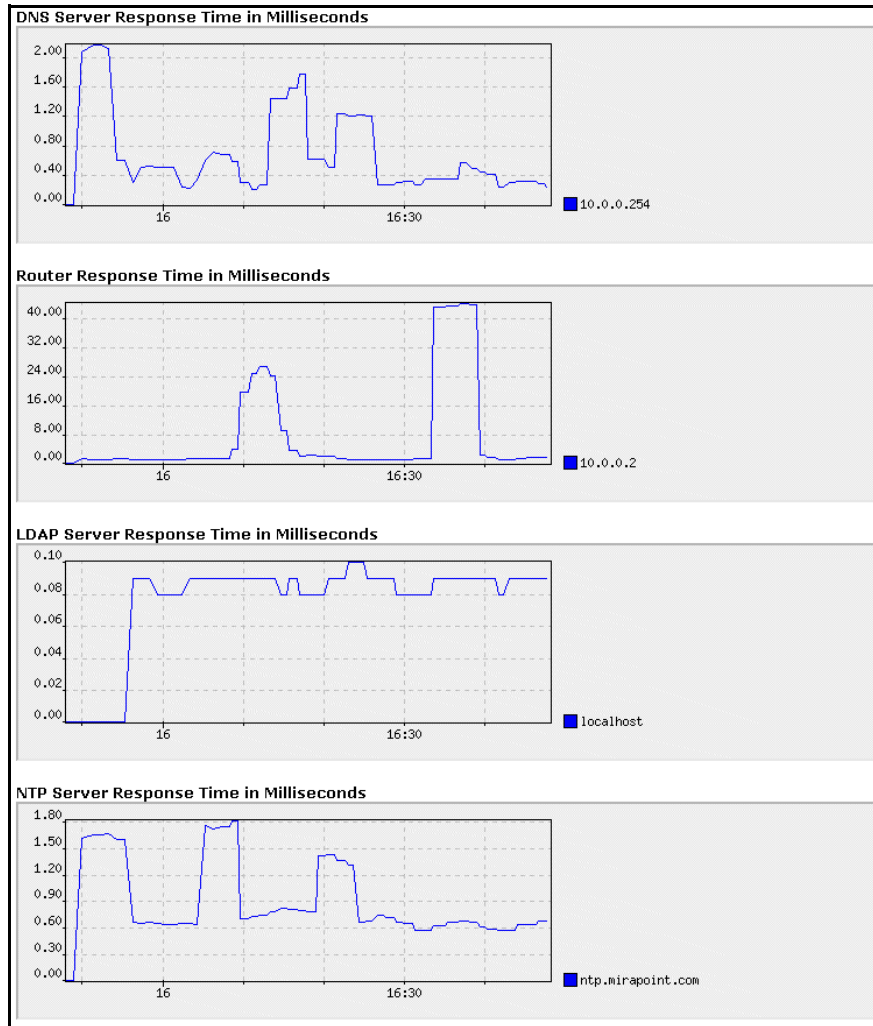


Figure 15 External Performance Graphs (Detail)

Table 18 External Server Monitoring Graphs (see Figure 15)

Graph	Description
DNS Server Response Time in Milliseconds	Response time (of user datagram packets) of each Domain Name Service (DNS) server.
Router Response Time in Milliseconds	Response time (a packet traveling from the Message Server to the hub/switch and then to the router) of each network router.
LDAP Server Response Time in Milliseconds	Response time (the time to retrieve LDAP data) of each Lightweight Directory Access Protocol (LDAP) server.
NTP Server Response Time in Milliseconds	Response time of each Network Time Protocol (NTP) server.
RBL Server Response Time in Milliseconds	Response time of each Realtime Blackhole List (RBL) server.
OMR Response Time in Milliseconds	Response time of each outbound message router (OMR).

What to Look for in External Graphs

All the graphs should show peaks at the same time; if not, you probably have a network problem, not a server problem. For all External Server graphs, check your hardware: network cables, wires, etc.

DNS Server Response Time is of concern if it slows to 1 second for five minutes. Less than 100 milliseconds is normal and anything over 500 milliseconds is bad. If response time is 0, then no queries are happening. This is normal during configuration, but after deployment DNS queries are happening most of the time on systems that are operating normally.

Router Response Time is bad if it exceeds 150 milliseconds and really bad if it exceeds 500 milliseconds. This graph should show a consistent response time, any sustained peak is cause for concern.

LDAP Server Response Time is bad if it exceeds 100 milliseconds and really bad if it exceeds 500 milliseconds. A response time over 100 milliseconds means that messages and user logins are delayed. A response time over 500 milliseconds means that some user logins might time out and some messages might be bounced because information cannot be retrieved from the LDAP server fast enough.

The NTP Server Response Time is not relevant to troubleshooting. The NTP protocol takes the server response time into account when determining the current time.

If you disable ping (**Mon Disable Netmonping**), then all response times in the external servers area will be flat-lined. For details, see **Help About Mon** in the CLI.

Disk Graphs

The **Disk Usage Information** graphs show a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view.

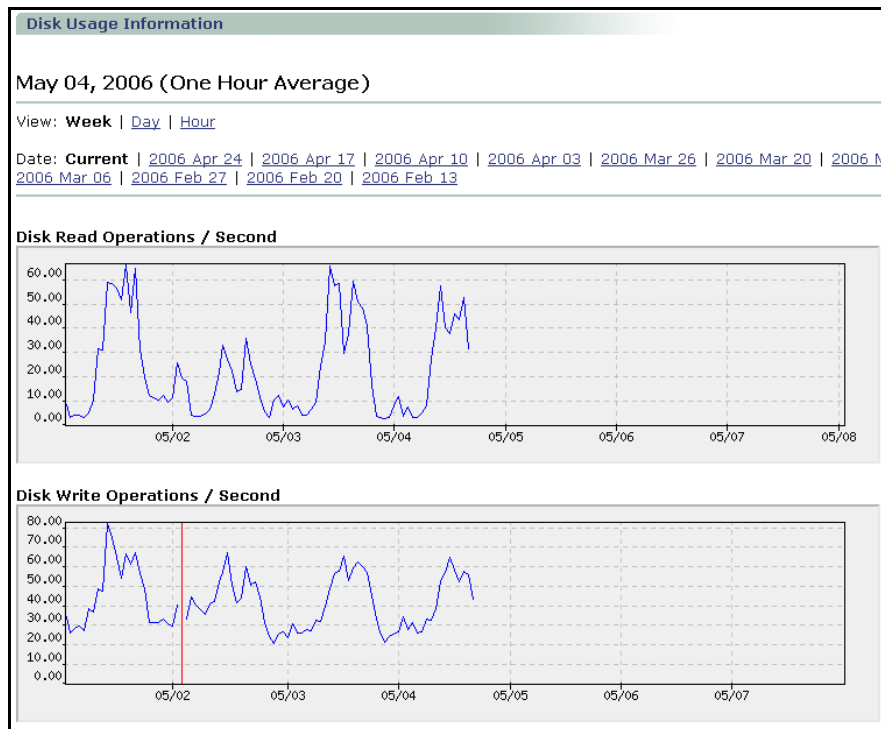


Figure 16 Disk Performance Graphs

Table 19 Disk Usage Information Graphs (see Figure 16)

Graph	Description
Disk Read Operations/ Second	Number of disk read operations per second for one day. Measures block transfers.
Disk Write Operations/ Second	Number of disk write operations per second one day. Measures block transfers.
Disk read activity by category and Disk write activity by category	Show the percentage of total disk reads/writes performed by each subsystem. For a list of possible subsystems, see “Pie-Chart Categories,” below.
(Mail Store / System) % disk used	The percentage of total disk space being used in the mail store and system disk partitions.
(Mail Store / System) % files used	The percentage of the maximum allowed number of files being used in the mail store and system disk partitions.

The Disk pie charts shown on the Disk Usage Information page only count the actual disk reads/writes not reads and writes in and out of the buffer cache. These pie charts are shown in Figure 17. For explanations of the possible pie chart categories, see [“Pie-Chart Categories” on page 204.](#)

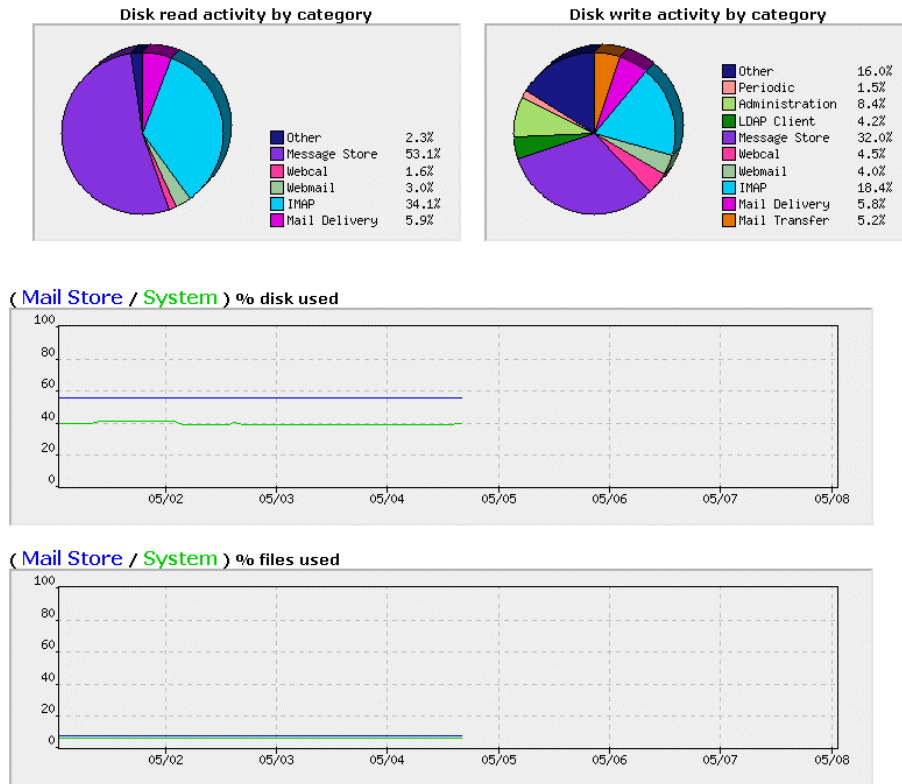


Figure 17 Disk Pie Charts

What to Look for in Disk Graphs

High disk traffic is bad; check your IMAP, POP, and Directory graphs to find the causes.

The **Mail Store/System % files used** should be about half the **Mail Store/System % disk used**.

If the Disk Usage graphs are showing consistent growth over time, consider expiring unimportant mail (for example, Trash or Junk Mail folders).

A sustained reading of 60% to 75% is an indicator that you need to start reducing usage or increasing capacity.

Sluggish performance could come from any number of sub-systems; check the “activity by category” pie charts to find causes.

Network Graphs

The **Network Traffic** graphs show a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view.

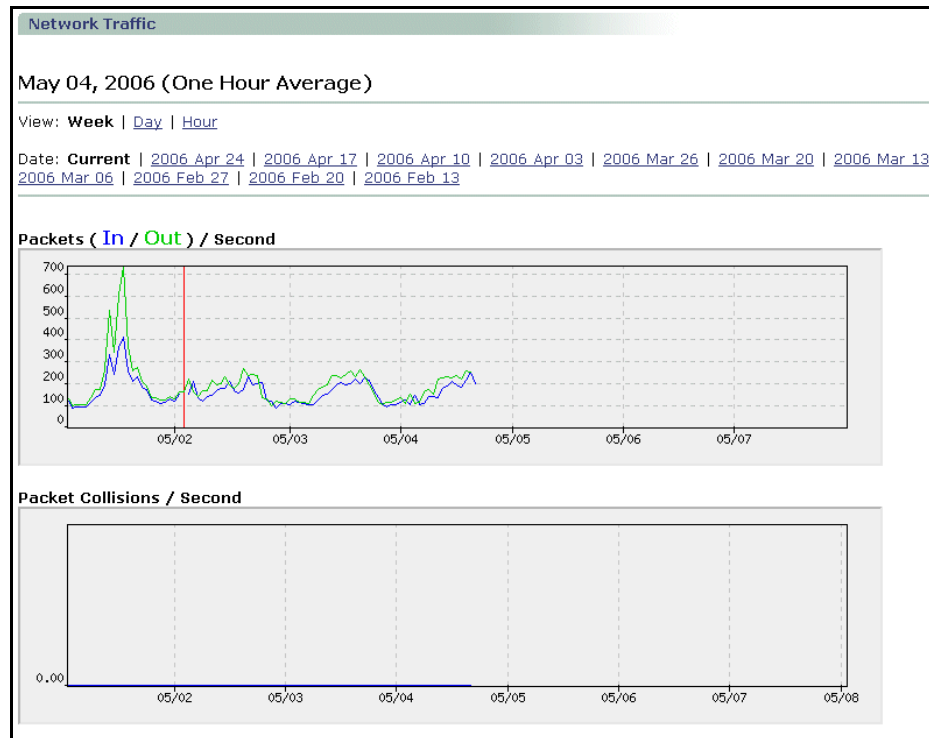


Figure 18 Network Performance Graphs Detail

Table 20 Network Traffic Graphs (see Figure 18)

Graph	Description
Packets (In / Out) / Second	Number of incoming and outgoing network packets per second.
Packet Collisions / Second	Number of network packet collisions per second.
Packets Input by Category and Packets Output by Category	Shows the percentage of total network packets received/sent by each subsystem. For a list of possible subsystems, see “Pie-Chart Categories” on page 204 .

The **Network Traffic** pie charts give you information about what's using up network traffic. These charts are shown in Figure 19. For explanations of the possible pie chart categories, see [“Pie-Chart Categories” on page 204](#).

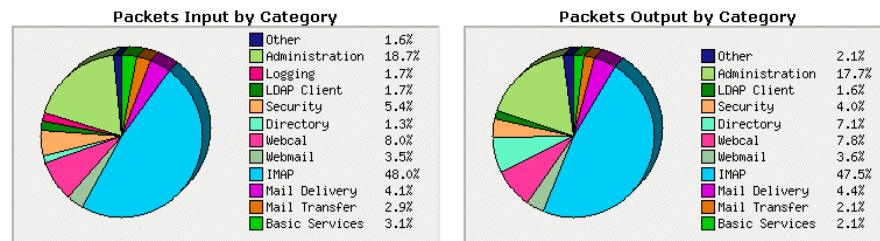


Figure 19 Network Traffic Pie Charts

What to Look for in Network Graphs

If the **Network Traffic** pie charts are flat-lined, your network is down.

If you see anything in the **Packet Collisions / Second** graph, the network is having problems or the NIC is having auto-detection difficulties with your Ethernet switch. To solve the auto-detection problems, you can force the NIC speed. If this graph shows network saturation—a sustained peak—your I.T. crew needs to check the network. A few spikes are normal; lots of spikes or sustained spikes is cause for concern.

A sudden increase in the Packets (In / Out) / Second graph might indicate a Denial of Service attack if it does not correspond with normal usage patterns.

The Packets Input and Packets Output by Category pie charts show what sub-systems are getting and sending packets.

For explanations of the possible pie chart categories, see [“Pie-Chart Categories” on page 204](#).

CPU Graphs

The CPU Activity graphs show a one-hour average sampling in the **Week** view, a 10 minute average sampling in the **Day** view, and a 20 second average sampling in the **Hour** view.

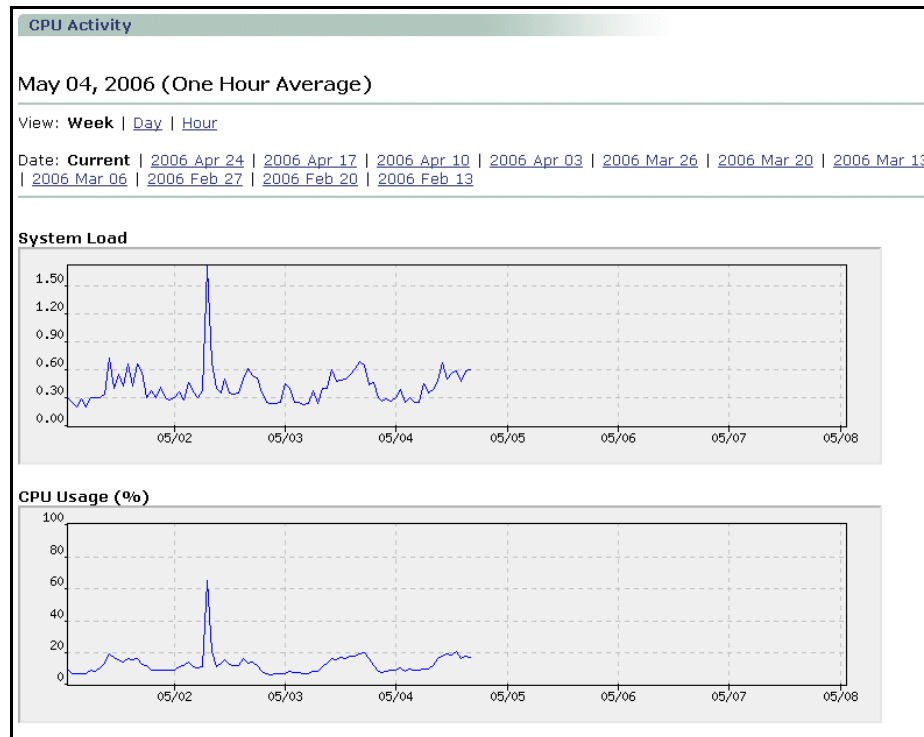


Figure 20 CPU Performance Graphs Detail

Table 21 CPU Activity Graphs

Graph	Description
System Load	The one-minute load average as calculated by the operating system. This number gives the average number of processes in the run queue over 60 seconds.
CPU Usage (%)	The percentage of CPU capacity in use. A transient CPU usage of 100% is normal and is not a cause for concern; sustained CPU usage of 100% coupled with a high System Load, however, probably indicates a real problem.
CPU Usage by Category (%)	Pie chart shows the percentage of total CPU usage by each subsystem. For a list of possible subsystems, see “Pie-Chart Categories” on page 204

What to Look for in CPU Graphs

If the top level **CPU Activity** dashboard gauge shows that the CPU is pegged, look at the CPU pie chart to see what's consuming CPU cycles.

Spikes in CPU Usage are normal, but sustained spikes could indicate a spam attack. If the load average is consistently running high, it could indicate a system capacity problem.

For explanations of the possible pie chart categories, see [“Pie-Chart Categories” on page 204](#).

Using the Message Queue

The **Queue** pages provide information on and control of the message queue. The queue utility provides these functions:

- ◆ Viewing details on any message in the queue; see [“Viewing the Queue Summary” on page 230](#).
- ◆ Sorting messages in the queue; see [“Sorting Messages in the Queue” on page 232](#).

- ◆ Searching for messages in the queue; see [“Searching the Queue” on page 239](#).



The message queue can be a valuable tool for tracking down a pegged system problem. However, only by observing your queue over time can you determine what a “large” queue for your systems is. To determine why a large number of messages are being queued, use the **Sort by Reason** page to look for frequently-occurring reasons. For more information, see [“Common Reasons Found in the Queue” on page 229](#).

About the Queue

Mail systems route mail through a Message Transfer Agent (MTA). MTAs accept messages from mail clients, mail enabled applications, and other MTAs. The MTA processes the message (optionally cleans or removes viruses, tags with headers, removes or redirects spam, or applies other filters and actions). Finally the MTA, forwards the message on to the next stop in its path - either locally delivering it to a message Inbox/Qtinbox or forwarding it on to another MTA. During all this processing and routing of mail, the MTA takes ownership of the message and places it in a working queue. A working mail queue for an MTA is extremely dynamic. Many messages enter the queue, are processed, and leave the queue every second. When you look at a queue, you are seeing a snapshot of the queue at an instance in time.

This section describes what the Mirapoint appliance allows you to see and manipulate in the message queue. In most cases, you use the **Queue** pages to drill down into a queue and act on messages that have been deferred (stalled) for an external reason, or to sort and understand the traffic passing through the queue. It is Ok to perform these tasks on a running, working queue. Sometimes, after drilling down into a queue, you might want to suspend the delivery process and clean up the queue; for example, if you are the victim of a spammer and there are thousands of messages backing up your resources. See [“Temporarily Stopping Mail Service” on page 241](#) and [“Deleting the Queue for a Domain” on page 242](#) for details.

Common Reasons Found in the Queue

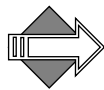
When viewing a queue, especially a large queue, you'll want to try and find common reasons. Some of the more typical reasons are these:

- ◆ **Connection Refused:** Usually this is the response when the target server is reachable on the network but is not allowing your server to connect to the SMTP port. This is usually because the SMTP subsystem is not running, but it can also mean that the sending server is being blocked, possibly by a firewall, blocklist, or some other configuration setting.
- ◆ **Operation Timed Out:** Usually indicates that a target server is unreachable on the network. Either the machine is down, the network is down, the machine doesn't exist, or the machine is overloaded to the point where it can't respond within the timeout period.
- ◆ **Over Quota:** Means that the recipient's folder is over their set quota, and the SMTP server is rejecting messages for that user because of the over quota policy.
- ◆ **Read Error:** Usually indicates a system error in the SMTP program, an unexpected response, or lack of response from the target SMTP system. It could mean that the initial handshake failed due to SMTP version incompatibilities, or it could be an indication of some problem on the network between the two machines.
- ◆ **Unknown User:** If a large number of messages are queued due to the reason "Unknown user" you are most likely subject to a directory harvesting attack. (This can happen if you don't have SMTP recipient check turned on.) To reduce the queue size, you can delete all of the "Unknown user" messages in the queue. (For information about removing messages from the queue, see ["Acting on Sorted Messages" on page 234.](#))
- ◆ **Deferred Time Out:** If connections to your own system are timing out, try to free cycles on your internal mail system so it can process more mail.

What to Look for in the Queue

The message queue can provide valuable information when troubleshooting system performance. Mainly, there are three values to monitor:

- ◆ **Large queues:** When the **Entries not yet processed** is consistently more than 5000 messages at a time, that is a large queue. A large queue can indicate a spam attack, CPU overloading, or other system problems. When this happens, you'll want to look at the other graphs, logs and reports, and isolate the bottleneck.
- ◆ **Maximum queue size:** When the **Total queue entries** consistently exceeds 20,000, your queue is overloaded and it is time to consider off-loading the outbound message router function to a separate server. If the entries not processed remains relatively low (below 50), then it might be time to consider off-loading some users.
- ◆ **Slow queues:** If the **Longest time in queue** value consistently exceeds 15 minutes for entries that haven't been processed, your system's performance is suffering and you are likely to start hearing complaints. Looking through the graphs, logs, and reports can help you isolate the problem.

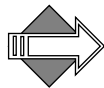


In an OMR (outbound message router), it is not unusual to see large queues because a large number of hosts are down, and the messages are marked for re-try. In the case of spam/viruses, the hosts might not exist any more. On a message store with a separate OMR, the queue size should be very low.

Viewing the Queue Summary

Use the **Queue > Get Queue Summary** page (see Figure 21) to get information on the current state of the queue. Use these buttons:

- ◆ **Refresh** button: Gives an immediate update on the queue.
- ◆ **Remove All** button: Clears the entire queue.



The queue pages work on a point-in-time basis; all data references the information available as of the last time the page was generated.



Figure 21 Queue Summary Page

The top three lines on the **Get Queue Summary** page give statistics on the over-all state of the queue:

- ◆ **Total queue entries:** The total number of entries in the queue. Over time, you develop an understanding of what is a normal queue size at any given point in time. Then, you'll be able to tell from the total queue entries if your queue is indicating a problem or not.
- ◆ **Entries not yet processed:** The number of entries in the queue waiting for processing. By subtracting this number from the Total queue entries, you can quickly determine how many entries have been processed and yet are still in the queue. If this is a large number, you'll want to look for a common reason.

- ◆ **Avg number of recipients:** The average number of recipients for the messages passed through the queue.
- ◆ **Max number of recipients:** The maximum number of recipients for a message that has passed through the queue.
- ◆ **Average message size:** The average size of the messages, in bytes, passing through the queue.
- ◆ **Max message size:** The maximum message size, in bytes.

Note: The recipients and message size values are useful for determining the typical usage profile of your users.

The bottom six lines give current statistics for each of the factors available through the **Sort** pages:

- ◆ **Longest time in queue:** The date and exact time length of the longest time a message spent in the queue.
- ◆ **Maximum entries from a host:** The domain name, everything on the left side of the at sign (@), and number of messages in the queue.
- ◆ **Maximum entries from an address:** The address, and number of messages in the queue.
- ◆ **Maximum entries to a host:** The domain name—everything on the left side of the at sign (@), and number of received messages.
- ◆ **Maximum entries to an address:** The address, and number of received messages.
- ◆ **Most common reason for being queued:** The reason, and the number of matching messages.

Use the links at the left of the **Get Queue Summary** page to **Sort** or **Search** the queue. For details, see [“Sorting Messages in the Queue” on page 232](#) and [“Searching the Queue” on page 239](#).

Sorting Messages in the Queue

Use the **Queue > Sort** pages to view selected messages. At the top of each sort page is a status table summarizing the results of the search. If

there are more than one set of results, each set displays as a link under the *sort factor* heading; click the link to display those messages.

The screenshot shows the Mirapoint Message Server interface. The main content area is titled 'Sort Message Queue (Time)'. It displays a summary table for the 'Reason' category:

Reason	Instances
Unprocessed	179

Below this, the 'Reason: Unprocessed' section contains a list of 10 messages. The table below shows the details for these messages:

Time in Queue	Size	Reason	Recipient	Subject
<input type="checkbox"/> 0d 00:00:13	78	Unprocessed	joesmith	[Message header is not available]
<input type="checkbox"/> 0d 00:00:13	78	Unprocessed	joesmith	[Message header is not available]
<input type="checkbox"/> 0d 00:00:13	78	Unprocessed	joesmith	Regular mail message
<input type="checkbox"/> 0d 00:00:13	78	Unprocessed	joesmith	Regular mail message
<input type="checkbox"/> 0d 00:00:13	78	Unprocessed	joesmith	Regular mail message
<input type="checkbox"/> 0d 00:00:13	78	Unprocessed	joesmith	Regular mail message
<input type="checkbox"/> 0d 00:00:13	78	Unprocessed	joesmith	Regular mail message
<input type="checkbox"/> 0d 00:00:13	78	Unprocessed	joesmith	Regular mail message
<input type="checkbox"/> 0d 00:00:14	78	Unprocessed	joesmith	Regular mail message
<input type="checkbox"/> 0d 00:00:14	78	Unprocessed	joesmith	Regular mail message

Figure 22 Queue Sort Page

To display a set of sorted messages, follow these steps.

1. On the **Get Queue Summary** page, click any of the sort links at left:
 - ❖ **Reason:** Messages are sorted by reason queued. The most common reason is listed first with the number of messages queued for that reason given.
 - ❖ **From Host:** Messages are sorted by sending host. The most common host is listed first with the number of messages queued for that host given.
 - ❖ **From Address:** Messages are sorted by sending address. The most common address is listed first with the number of messages queued for that address given.

- ❖ **To Host:** Messages are sorted by recipient host. The most common host is listed first with the number of messages queued for that host given.
- ❖ **To Address:** Messages are sorted by recipient address. The most common address is listed first with the number of messages queued for that address given.
- ❖ **Time:** Messages are sorted by time queued. The longest time length is listed first with the number of messages queued for that time given.

Result: A status table displays sets of messages that match the sort criteria in order of frequency, as well as the number of **Instances** (queued messages) for each set.

2. Click an underlined *sort factor* link in the status table.

Result: A list of messages queued for that factor displays. The queue is sorted by frequency based on the message property: **Time in Queue, Size, Reason, Recipient, and Subject**, that pertains to the current page you are on

Acting on Sorted Messages

Once you have sorted the queue, you can act on the messages as follows.

1. Use these command buttons to operate on displayed messages:
 - ❖ **Refresh:** Redraws the page with latest queue data.
 - ❖ **Retry:** Directs the system to try sending again the entire message queue.
 - ❖ **Remove:** Directs the system to delete selected messages from the queue.
 - ❖ **Remove All:** Removes all queue entries matching the selected reason. For example, if you sort by time, select the “1h” set in the status table, and push **Remove All**; all the matching entries are permanently deleted. This is different from the **Remove All** button on the **Summary** page that wipes out the entire queue.

Result: Depending on your command, the queue is refreshed, all of the messages are retried or removed, or the selected messages are removed.

2. Click the **Subject** link for a displayed message.
Result: The **Envelope and Header** page for that message opens; see [“Reading Message Envelopes and Headers” on page 235](#) for details.

Reading Message Envelopes and Headers

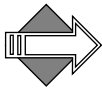
To view the envelope and headers of a message in the queue, click a **Subject** link in the message queue search results table.

Result: The **Envelope and Header** page for that message displays showing some or all of the following information. This information is also available by clicking the **Open** link for a message.

- ◆ **Queue ID:** The identification number system-assigned when the message arrives. The queue ID is system dependent and the same queue ID can be used by multiple systems in the same messaging deployment. However, the Message ID in the message header is generally unique among all messages.
- ◆ **Message Envelope:** Message information that the system uses to route email.
 - ❖ **Mail From:** Message information that the system uses to distinguish and selectively receive email. The fields are message envelope source, destination, tag, and communicator. The message source is implicitly determined by the identity of the message source message sender. The other fields are specified by arguments in the send operation.
 - ❖ **RCPT To:** The requested receipt address on the message.
- ◆ **Message Header:** Message information that the message senders and receivers use. Typically, header fields are the following:
 - ❖ **Received:** When the system received the message.
 - ❖ **From:** The name and/or email address of the sender.
 - ❖ **To:** The identity of the primary recipients of the message; not Cc or Bcc recipients.
 - ❖ **Date:** The day and time at which the message was sent.
 - ❖ **Subject:** The sender-entered subject of the message
 - ❖ **Return-Path:** The coded return address on the message; can include more than one mail server.

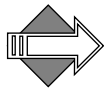
- ❖ **X-Mailer:** The mail client in which the email was composed.
- ❖ **Message Id:** A unique identifier usually assigned by the first MTA (message transfer agent) that handled the message.
- ❖ **Content-Type:** The MIME Content-Type used in a message such as text/plain, text/html, multipart/related, multipart/alternative, image/gif, and so on.
- ❖ **MIME-Version:** Indicates that the message is MIME-formatted. The value is typically “1.0.”
- ◆ **X headers:** X headers are added by the mail processing function for various reasons; in general, they provide additional information about the message. Mirapoint uses the following X headers as indicated:
 - ❖ During antispam and antivirus scanning,:
 - **X-Junkmail:** The UCE score that the message was given by the anti-spam scanner that categorized it as junkmail. Example:
X-Junkmail: UCE(190)
 - **X-Junkmail-Status:** The UCE score shown over the configured default UCE threshold (see [“About the Antispam Scanning Rules and Threshold”](#) on page 336 for information on adjusting the default threshold) and what host performed the scanning. Example:
X-Junkmail-Status: score=0/50, host=mirapoint.com
 - **X-Junkmail-SD-Raw:** Indicates that the **Signature** edition anti-spam scanner using RAPID® technology was used.
 - **X-Junkmail-Info:** Provides coded explanations of why the message was categorized as spam (junkmail). This header can be disabled by your system administrator. This header only applies to the **Principal Edition** anti-spam scanner; to understand the codes, see [The Apache SpamAssasin Project](#). Example:
X-Junkmail-Info: FORGED_RCVD_HELO,HTML_80_90,CLICK_BELOW
 - **X-Mirapoint-Virus:** Tracks the state of the virus cleaning done on a message.
 - **X-Mirapoint-RAPID-Raw:** Indicates that the **RAPID** antivirus scanner was used. Example:
X-Mirapoint-RAPID-Raw: score=unknown (0)

- **X-Mirapoint-State:** Tracks the filtering already done and remaining to be done.
 - **X-Mirapoint-Old-Envelope-From:** Keeps the original MAIL FROM and RCPT TO header information (when using wiretap the FROM and TO are re-written).
 - **X-Mirapoint-Old-Envelope-To:** Keeps the original MAIL FROM and RCPT TO header information (when using wiretap the FROM and TO are re-written) .
 - **X-old-subject:** Keeps the original subject (when the subject line has been modified).
 - **X-DSN-Junkmail:** Keeps track of the original messages UCE status for a DSN (delivery status notification).
 - **X-DSN-Junkmail-Status:** Keeps track of the DSN messages original Junkmail Score.
 - **X-DSN-Mirapoint-Virus:** Keeps track of the DSN messages original Virus Information.
- ❖ During domain content filtering,
- **X-Junkmail-Whitelist:** The message sender was on the Allowed Senders list for that domain. Example:
X-Junkmail-Whitelist: YES (by domain whitelist at mirapoint.com)
 - **X-Junkmail-Recipient-Whitelist:** The message recipient was on the Allowed Mailing Lists for that domain. Example:
X-Junkmail-Whitelistto: YES (by domain whitelitto at mirapoint.com)
 - **X-Junkmail-Blacklist:** The message sender was on the Blocked Senders list for that domain. Example:
X-Junkmail-Blacklist: YES (by domain blacklist at mirapoint.com)



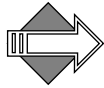
If a message has received an **X-Junkmail** header and, during domain content filtering, qualifies for one of these headers, the anti-spam scanning **X-Junkmail** header is removed.

- ❖ During end-user content filtering,
 - **X-Junkmail-Whitelist:** The message sender was on the Allowed Senders list for that end-user. Example:
X-Junkmail-Whitelist: YES (by user whitelist at mirapoint.com)
 - **X-Junkmail-Recipient-Whitelist:** The message recipient was on the Allowed Mailing Lists for that end-user. Example:
X-Junkmail-Whitelistto: YES (by user whitelitto at mirapoint.com)
 - **X-Junkmail-Blacklist:** The message sender was on the Blocked Senders list for that end-user. Example:
X-Junkmail-Blacklist: YES (by user blacklist at mirapoint.com)



If a message has received an **X-Junkmail** header and, during end-user content filtering, qualifies for one of these headers, the anti-spam scanning **X-Junkmail** header is removed.

Any mail agent (such as another server or a client application that is sending the message) can add X- headers. The ones listed above are added by the Mirapoint MTA.



Only the envelopes and headers of messages are available for viewing on these **Queue** pages. The content, or body, of a message can only be viewed by the addressed recipients unless the message is quarantined. (If the message is quarantined, it can also be viewed by the Quarantine Administrator.)

Searching the Queue

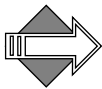
Use the **Queue > Search** page to search for messages. Once messages are found, you can retry, remove, and view data on any or all of the messages in the queue.

Override the default boolean operator (\Rightarrow) by entering another here

Figure 23 Queue Search Page

The **Queue** search engine allows you to use Boolean operators to find messages within certain specified parameters. You can also specify suffixes for the search parameters as another method of refining a search. The default Boolean operator for the **Minimum Time** and **Minimum Size** search parameters is the greater than/equals (\geq) operator. Default Boolean operators can be overridden by prefixing the field entry with one of the other operators, such as the less than/equals (\leq) or equals ($=$) operator. For example, to search for messages that have been in the queue for less than two days, enter ≤ 2 in the **Minimum Time** option.

See the table below, [“Operators for Search Parameters” on page 241](#), for a list of default Boolean operators used by the search engine.



Only the envelopes and headers of messages are available for viewing. The content, or body, of a message can only be viewed by the addressed recipients unless the message is quarantined. (If the message is quarantined, it can also be viewed by the Quarantine Administrator.)

To search for a message in the queue, follow these steps on the **Queue > Search Message Queue** page.

1. Enter some data in any or all of the following option boxes:
 - ❖ **Queue ID:** The identification number system-assigned when the message arrives. Enter an alphanumeric string to search for a message whose queue ID you know.
 - ❖ **Minimum Time:** The minimum length of time the message could be in the queue. Enter an integer and select a time unit from the drop-down list to restrict your search to messages that are not older than a given time. You can use the operators described below in the table [“Operators for Search Parameters” on page 241](#).
 - ❖ **Minimum Size:** The minimum size of the message. Enter an integer and select a size unit from the drop-down list to restrict your search to messages that are not smaller than a given size. You can use the operators described below in the table [“Operators for Search Parameters” on page 241](#).
 - ❖ **Reason:** An explanation for why the message was not delivered. Enter a text string to search for a message that might be in the queue. Suggested **Reason** searches, using the asterisk (*) wildcard: ***Deferred: Connection refused***, ***Deferred: Operation timed out***, ***Deferred: Over quota***, and ***read error***.
 - ❖ **Recipients:** The specified recipients of the message. Enter names or email addresses to search for a message sent to certain parties.
 - ❖ **Display Count:** The number of messages you want displayed on one page.
2. Click **Search** or **Clear**.

Result: If you click **Search**, the system searches for the message(s) using the parameters you entered. Results displays in a table below or a message displays indicating that the message is not in the queue. If you click **Clear**, the search text boxes are emptied; you can reenter data to begin a new search. See [“Sorting Messages in the Queue” on page 232](#) for more information.

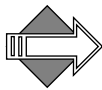
Operators for Search Parameters

Definitions:

= (equals), >= (greater than or equals), <= (lesser than or equals)

Table 22 Boolean Operators

Edit Field	Default Boolean Operator	Allowable Boolean Operators
Queue ID	=	Cannot override
Minimum Time	>=	>= <= =
Minimum Size	>=	>= <= =
Reason	=	Cannot override
Recipients	=	Cannot override



You can use an empty string (""), which is equivalent to the wildcard character asterisk (*), meaning all message queue IDs.

Temporarily Stopping Mail Service

If your queue is excessively large, you might want to temporarily stop all SMTP traffic. To do this, go to **System > Services > SMTP > Main Configuration** and click **Stop it**. All inbound and outbound mail is halted and will be retried when the SMTP service is restarted. Wait a few minutes before restarting the service by clicking the **Start it** link.

Note: You can also stop inbound mail without stopping the processing of the queue by altering the **SMTP Listen Port** in the SMTP Configuration. The SMTP service stops and immediately restarts, but no-one will be able to establish an inbound connection unless they know the new port number.

Deleting the Queue for a Domain

To remove all messages in the queue for a particular domain, use the **Queue > Sort Message Queue** page in the **Sort by To Address** view; see Figure 22) to isolate all of the messages in a particular domain. Once you have all of those messages displayed, you can use the **Remove All** button to flush the queue. **Note:** The **Remove All** button does not display unless there are messages in the queue.

Viewing Hardware Status

You can view the hardware status to monitor the condition of the appliance hardware, including storage, CPU, health monitoring, and alerts.

Note: The contents of the **Monitoring** pages differ depending on your hardware and licensing.

Monitoring Storage

Mirapoint appliances can inform you about disk storage status, health of computer components, and alert you to emergency conditions.

Use the **Monitoring > Storage** page to view and manage your storage. The information and options displayed depend on your system configuration, enabling you to:

- ◆ View the status of and manage a RAID (redundant array of independent disks) system.
- ◆ View the properties of IDE storage and manage the disk cache.

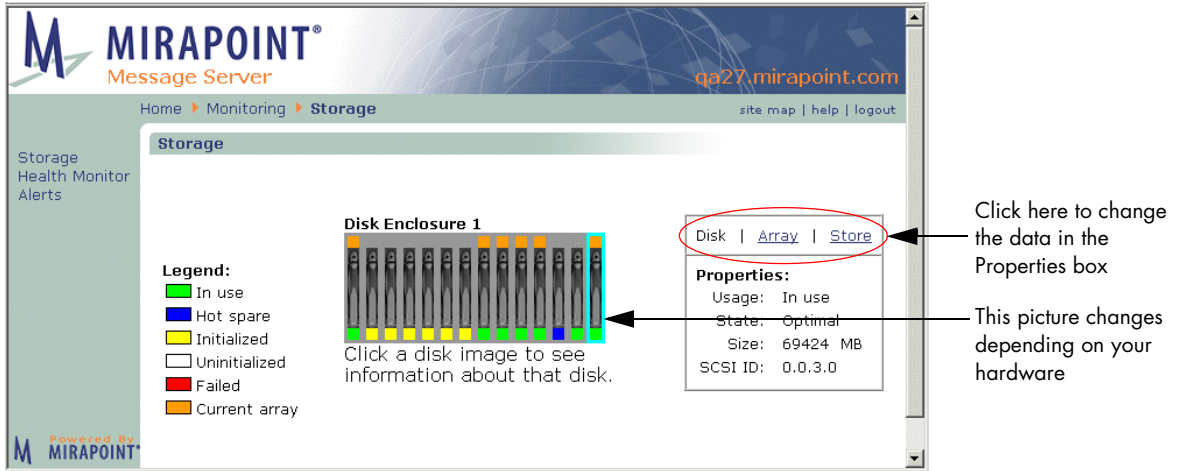


Figure 24 Monitoring > Storage Page Disk View

If your system has IDE (integrated drive electronics) storage, then the **Storage** page displays only the **Properties** data box, as shown in Figure 25.

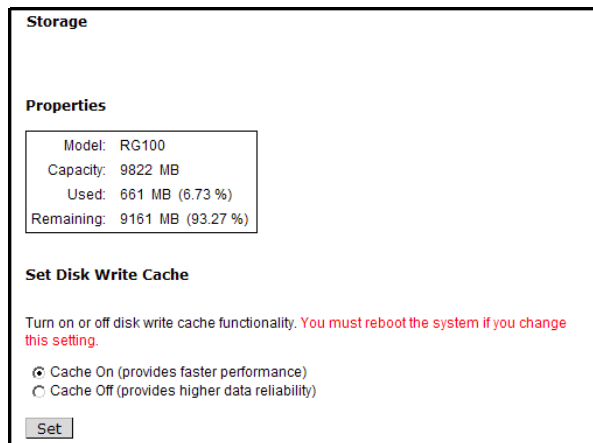


Figure 25 Monitoring IDE Storage

For configurations that have advanced storage devices, you can view the overall capacity of the message store, including information about the amount of space that has been used and the amount of available

space. You can also add or delete spares and arrays, and configure arrays.

- ◆ The **Legend** provides an explanation for the colors used in the Disk Enclosure/Shelf graphics.
- ◆ The **Disk Enclosure/Disk Shelf** graphics display identification when you put your cursor over an image and information on the selected disk in the **Properties** box when you click an image.
- ◆ The **Properties** data box shows storage information; you can choose between three views:
 - ❖ **Disk:** View data on installed RAID disks. Add a spare, if available; see [“Storage Disk Data View” on page 244](#) for details.
 - ❖ **Array:** View data on system storage arrays. Add an array to expand the available disk space. Delete an array or spare. See [“Storage Array Data View” on page 246](#) for details.
 - ❖ **Store:** View data on system storage space. For RG100s, the **Properties** box only displays the **Store** view. See [“Storage Store \(Space\) Data View” on page 248](#) for details.

Storage Disk Data View

Each Disk Enclosure or Disk Shelf image shows the general status of each disk the enclosure/shelf contains. A data box at right provides information on the disks shown; by default the properties of the last initialized disk is displayed. Click any displayed disk to view its properties.

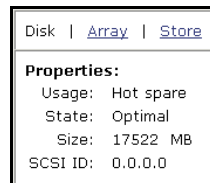


Figure 26 Monitoring > Storage Page Disk View Properties Box Detail

The following table explains the terms in the **Properties** data box for **Disk** view; see Figure 24. **Note:** A message displays if a disk has failed, or is in a missing state.

Table 23 Disk View Properties Data Box Items (see Figure 24)

Item	Description
Usage	In use, Hot spare, Not in use, or No disk.
State	Optimal—operating normally. Initializing—the array is being added to the system. Rebuilding—rebuilding the disk after a failure. Failed—the disk is not operating.
Size	Size in megabytes.
SCSI ID	Information on the location of the disk (in relation to the other disks in the enclosure).

Adding a Spare

Add a spare to your RAID system if it is currently running without one. This procedure initializes the first unused disk found in any spare disk bay. See the hardware manual for your system to find the location of the hot-spare disk bay or bays on your system. If there is no unused disk in any hot-spare disk bay, the **Add Spare** button does not appear. To add a spare follow these steps.

1. Install your new hot spare disk as described in the hardware manual for your system.
Result: The new disk is available or an error message displays.
2. On the **Storage** page in **Disk** view, click **Add Spare**.
Result: A message displays indicating success or failure at adding the spare.

Deleting a Spare

Delete a spare only when you want to replace it with higher-capacity disk. To delete a spare, on the **Storage** page in Array view, select the spare you want to delete and click **Delete**.

Result: A confirmation message appears. Click **Delete** to continue; click **Cancel** to terminate the deletion operation.

Storage Array Data View

To view the disk array status, on the **Storage** page in **Array** view, click on a disk.

Result: The disk becomes outlined in **aqua**. The data box at right changes to display array properties.

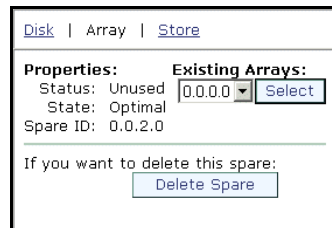


Figure 27 Monitoring > Storage Page Array View Properties Box Detail

The following table explains the terms in the **Properties** data box for the **Array** view; see Figure 24.

Table 24 Array View Properties Data Box Items (see Figure 24)

Item	Description
Status	In use, Hot spare, Not in use, or No disk.
State	Optimal, Initializing, Rebuilding, or Failed.
Array ID	Identifying number of the array.

Adding and Configuring an Array

You can add an array to your system only if a sufficient number of unused disks are available (independent of configuration); otherwise, the **Add Array** button does not appear. This procedure initializes the first array of unused RAID disks detected by the storage scan function. These disks must be installed as described in the hardware manual for your system. If the disks are installed incorrectly the **Add Array** button does not appear.

Once the array is added, it must be configured to become part of the active mail store. You can do both, add and configure an array, using this page.

To add and configure an array, follow these steps.

1. Install your new unused disks as described in the hardware manual for your system. **Note:** You might need to click the **Scan** button in the **Store** view for the system to recognize the new disk(s).
Result: The **Add Array** button displays on the **System > Storage** page **Disk** view.
2. On the **Storage** page in **Disk** view, click **Add Array**.
Result: A progress bar displays and a message indicating success or failure at adding the array, although the add process continues and typically lasts several hours; you can do other administration tasks or quit the browser while this is going on. When initialization is complete, you must click **Configure** to begin using the new array.
3. On the **Storage** page in **Array** view, select the new array and click **Configure**.
Result: A progress bar and confirmation message appear; configuring the array causes the system to stop all e-mail services for five to fifteen minutes or more.
4. To proceed click **Configure**, to cancel, click **Cancel**.
Result: If you click **Configure**, the page re-displays with the **Properties** box showing the status of the configuration; the system adds the array to the mail store; this can take a minute or two. When configuration is complete, the status reads 100% and the array is displays in the list of **Existing Arrays**. If you click **Cancel**, the previous page re-displays.

Deleting an Array

Delete an array only when you want to remove an array that failed to initialize properly. Only an unused array (one that has not been added to the mail store) can be deleted. On the **Storage** page in **Array** view, select the array you want to delete and click **Delete**.

Result: A confirmation message appears; click **Delete** to continue, click **Cancel** to terminate the deletion operation.

Storage Store (Space) Data View

To view the overall capacity of the message store, with information on the amount of space that has been used and the space that remains available, open the **Storage** page to **Store** view.

Result: The data changes to display system storage information.

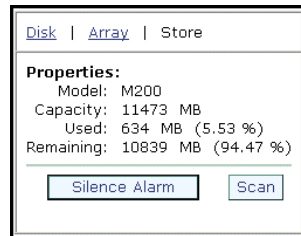


Figure 28 Monitoring > Storage Page Store View Properties Box Detail

The following table explains the terms in the **Properties** data box for the **Store** view; see Figure 24.

Table 25 Store View Properties Data Box Items (see Figure 24)

Item	Description
Model	The hardware model type.
Capacity	How many MBs (megabytes) of space the disk enclosure supplies.
Used	How many MBs of space the disk enclosure is currently using.
Remaining	How many MBs of space the disk enclosure has available.

Silencing Alarm and Scan Buttons

On the **Storage** page in **Store** view, use the **Silence Alarm** button to turn off the audible alarm triggered by a failure in the RAID system (such as a disk failure).

On the **Storage** page in **Store** view, click **Scan** to scan the RAID system for changes in the hardware configuration, such as the insertion of new

disks. Using this button frequently can degrade performance; it is best to use the **Scan** button only after installing new disks.

Monitoring Hardware Health

It is advisable to monitor the health of appliance hardware, especially if you receive email notifications or anecdotal reports of problems in the machine room. You can separately check hardware status of the main computer chassis, RAID controller, and separate disk enclosures.

MIRAPPOINT®
Message Server qa27.mirapoint.com

Home ▶ Monitoring ▶ **Health Monitor** site map | help | logout

Health Monitor

[Refresh](#)
[Stop](#)

You have outstanding system alerts. For details and suggestions, see the Alerts page.
[View Alerts.](#)

System Status	
Temperature	OK
CPU 1	OK
CPU 2	OK
CPU 1 Temperature	OK
CPU 2 Temperature	OK
CPU 1 Fan	OK
CPU 2 Fan	OK
Fan 1	OK
Fan 2	OK
Fan 3	OK
Fan 4	OK
ECC Errors	OK
Power Supplies	OK
Voltage	OK

Disk Enclosure Status		
	1	2
Fan/PS	OK	n/a
Voltage	OK	n/a
Temperature	OK	n/a

RAID Controller Status		
Controller:	1	2
Battery Status	Charged	n/a
Battery Time	6d 02:09:00	n/a
Caching	ON	n/a

Some servers contain dual-fan modules that require replacement of the complete module when only one fan reports a failure. Consult your Hardware Installation and Maintenance manual for cooling fan information.

Time Running: 0d 02:59:16
MOS Version: 3.8.0

Figure 29 Monitoring > Health Monitor Page

To verify the health of computer components using the Administration Suite, go to the **Monitoring > Health Monitor** page (see Figure 24).

The table on the left represents the computer chassis, while the table on the right represents the disk enclosure. Reported statistics might not be the same on all appliances.

Problem conditions appear in red. If temperatures are too high, check environmental conditions in the machine room. If any fans have failed, replace them. ECC errors could indicate bad memory segments. If a power supply has failed, replace it. Low voltage could indicate a problem with AC power.

A value other than OK in the first status column in the Disk Enclosure Status table could indicate either a failed fan or a bad power supply.

The third table shows battery status and cache status for the RAID controller.

The system software release number and time since the system was last restarted appear at lower left.

Information is available on far more system statistics than those shown above. To see all publicly available values, run this CLI command:

```
Stat Get *
```

For documentation about system statistics, run this CLI command:

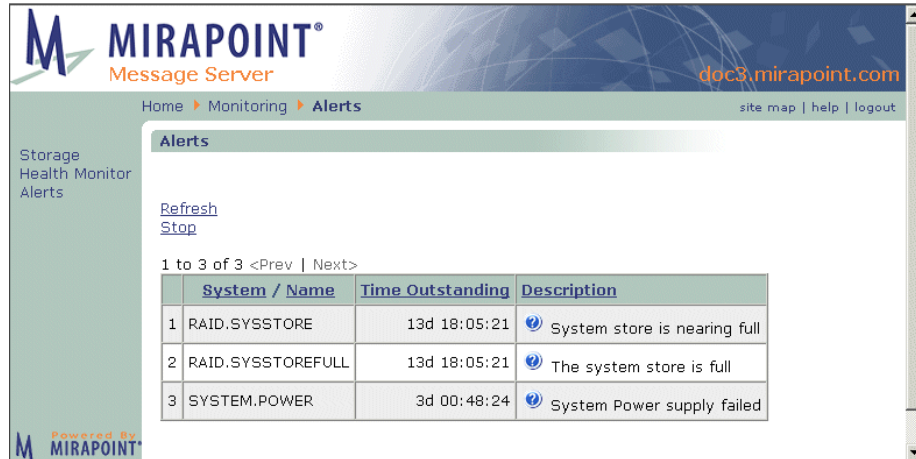
```
Help Stat Get *
```

Viewing Alerts

Alerts are important messages from a messaging appliance indicating conditions that might require human intervention. Alerts appear in the

periodic email summary **system-alerts**, but you can view them anytime using the **Monitoring > Alerts** page.

To check recent (uncleared) system alerts using Administration Suite, go to the **Monitoring > Alerts** page (see Figure 30).



The screenshot shows the Mirapoint Message Server interface. The top navigation bar includes 'Home > Monitoring > Alerts'. The main content area is titled 'Alerts' and contains a table of alerts. The table has three columns: 'System / Name', 'Time Outstanding', and 'Description'. There are three rows of alerts, each with a blue question mark icon in the description column.

	System / Name	Time Outstanding	Description
1	RAID.SYSSTORE	13d 18:05:21	System store is nearing full
2	RAID.SYSSTOREFULL	13d 18:05:21	The system store is full
3	SYSTEM.POWER	3d 00:48:24	System Power supply failed

Figure 30 Monitoring > Alerts Page

In this case, these alerts probably occurred at the same time due to power failure on the utility grid. Alerts also appear in the system log.

To see documentation and a suggested fix for each alert, click the icon shaped like a blue question mark (?).

Viewing User and/or Administrator Activity

You can view the activity of any user or administrator on the system with the User Audit and Admin Audit reports, respectively.

Using the User Audit Trail

The **User Audit Trail** report searches for and lists all events for the selected user, day, and event type. You can choose from these event types:

- ◆ **Mail:** Events related to mail traffic
- ◆ **Security:** Events related to security, such as virus and junk-mail filtering
- ◆ **Logins:** Logins to system services, such as POP, IMAP, WebMail, and the administration service
- ◆ **Commands:** Administration protocol commands

To view or download the reports for a user:

1. Select a day
2. Enter the user name in the **User** field
3. Click one or more **Event** type options
4. Click **Search** to view the reports or **Download** to download them to your local computer. Click **Clear** to empty the search fields.

Each line in each report has the format:

hh:mm:ss GMT-offset: event

Using the Admin Audit Trail

The **Admin Audit Trail** report lists all administrative actions chronologically for the selected day. Click **View** to view this report on screen or **Download** to save it to a file on your local computer.

Each line in the report has the following fields:

hh:mm:ss GMT-offset: user (id): action

Each line in each report has the format:

hh:mm:ss GMT-offset: event

The remaining fields are as follows:

Table 26 Admin Audit Trail Report

Field	Description
<i>user</i>	The login name of the user performing the action; for delegated domain users, this includes the domain name
<i>id</i>	The unique identifier for the administration service connection (session) in which the event occurred
<i>action</i>	A short text string describing the action, such as “Login by administrator.”

Monitoring External Systems via SNMP

Use the **Services > SNMP** pages to configure, enable, disable, start, or stop this monitoring service. The opening page allows you to **disable/enable** or **start/stop** the service.

Configuring SNMP Monitoring

On the **SNMP > Main Configuration** page, follow these steps.

1. Access MIB definition files by clicking one of the **MIB Definition Modules** links:
 - ❖ **Master MIB:** The MIB definition file for every MIB object supported by the system.
 - ❖ **Enterprise MIB:** The MIB definition file for proprietary MIB objects supported by the system, a subset of the Master MIB.
 - ❖ **Traps MIB:** The MIB definition file for trap MIB objects supported by the system, a subset of the Master MIB.

Result: A text file opens that you can load on to your system and use. These are standard MIB definition files that can be imported into an SNMP monitoring solution, such as HP Openview or Sun Net Manager.

2. Specify the following:

- ❖ **System Location:** A text string describing to users of SNMP clients where your system is physically located.
 - ❖ **System Contact.** Your name, email address, or phone number so users of SNMP clients can contact you.
3. Click **Modify** or **Reset**.
Result: If you click **Modify**, your changes are saved and the page displays the new settings. If you click **Reset**, your changes are discarded and the page displays the last-saved settings.



Adding SNMP Hosts

The SNMP Read-only community string enables a remote device to retrieve “read-only” information from a device. You configure this using the **Hosts** configuration options. If you don't explicitly define any access profiles using the **Hosts** configuration options, the SNMP service allows the “public” SNMP community read access to the entire MIB-II tree. To add, edit, or delete hosts; follow these steps.

1. To add a Host, click the **Hosts** link and then **Add Host**.
Result: The **Hosts** page displays with the following options:
 - ❖ **Access Host:** The fully qualified domain name (FQDN) of the host to which you want to grant access to query SNMP on the system.
 - ❖ **Read Community:** The community string that SNMP clients must specify to be allowed to query the system; space characters are not allowed.

Click **Ok**, or **Cancel**.

Result: If you click **Ok**, the names you enter display in a list box. If you click **Cancel**, you are returned to the main **Hosts** page, no changes are made.

2. To edit a host, click its **Edit** icon .
- Result: The add hosts page opens, see step 1 for options.
3. To delete a host, click its **Delete** icon .
- Result: The main **Hosts** page displays, the host is deleted and goes away from the list box.



Adding SNMP Traps

The SNMP Trap community string is used when sending SNMP Traps to another device. An **SNMP Trap** is an asynchronous notification of an event that is sent to specified hosts. The system sends all SNMP Traps to all hosts in the Trap list. The same events that generate email alerts also generate Traps. To add, edit, or delete traps; follow these steps.

1. To add a trap, click the **Traps** link and then **Add Trap**.
Result: The **Traps** page displays with the following options:
 - ❖ **Destination Host:** The fully qualified domain name (FQDN) of the host to which SNMP traps should be sent.
 - ❖ **Traps Community:** The community string for the Traps hosts list; space characters are not allowed.

Click **Ok**, or **Cancel**.

Result: If you click **Ok**, the names you enter display in a list box. If you click **Cancel**, you are returned to the main **Traps** page, no changes are made.

2. To edit a trap, click its **Edit** icon .
 3. To delete a trap, click its **Delete** icon .
- Result: The main **Traps** page displays, the trap is deleted and goes away from the list box.



Provisioning Tasks

This chapter describes how to provision and manage a Message Server's domains, user accounts and folders, queue, and distribution lists. The following topics are included:

- ◆ [Managing Delegated Domains](#): How to add, find, edit, and delete delegated domains including how to add an administrator, add the delegated domain administrator to the postmaster DL for that domain, and add WebCal resources (meeting rooms, equipment, and so forth) for that domain.
- ◆ [Managing User Accounts](#): How to add, find, edit, and delete user accounts and set account defaults; also how to assign roles, such as administrator, to user accounts.
- ◆ [Managing Folders](#): How to add, find, edit, and delete folders for user accounts. Also describes how to create a shared folder.
- ◆ [Managing Messages](#): Mail management tasks such as setting up message aging, and flushing the mail queue.
- ◆ [Managing Distribution Lists](#): How to add, find, edit, and delete distribution lists.

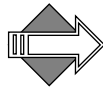
Managing Delegated Domains

An electronic mail solution built with one or more Mirapoint appliances can support multiple domains. To do this, the appliances support two different types of domains: the primary (default) domain and delegated domains.

A **domain** is an organization or entity on a host whose name (the **domain name**) is part of its Internet address. A **fully qualified domain name** is the host name plus the domain name. The last component of the domain name is the **top-level domain**: the part after the last period.

The **primary domain** is the top-level, default domain. For example, if your machine's hostname is set to "example.com", then your primary domain is "example.com".

Delegated domains provide a separate namespace for accounts, folders, and distribution lists for a segment of your user population, see Figure 31 for an illustration. For example, if your primary domain is "example.com" you might want to delegate space for domains named "sales.example.com" and "support.example.com." That way, the managers of the sales and support organizations could handle their own provisioning and each domain would receive mail addressed to them separately.



Once delegated domains are set up, you log into a delegated domain by specifying your login and the domain name separated by an at sign (@) as your username. For example, me@sales.example.com.

You can control many facilities on a delegated domain-specific basis including distribution lists, message forward and auto-reply availability, disk quota, user limits, and notification messages. Undeliverable messages can be bounced to the administrator of the delegated domain rather than the primary domain. Common tasks, such as adding or deleting users and setting passwords, can be done by a **Delegated Domain administrator**; this allows service providers to give control back to a client organization.



Even if you currently only expect to use a single domain, Mirapoint recommends that you create your domain as a delegated domain rather than using the primary domain. This provides you with the flexibility of

adding additional namespaces later. When you have delegated domains, only use the primary domain for global administration. Do all mail handling through the delegated domains.

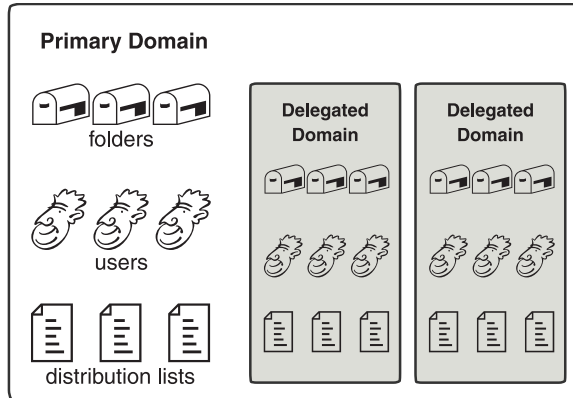
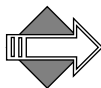
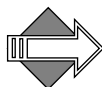


Figure 31 Primary Domain and Delegated Domains



To route messages addressed to a delegated domain on a Mirapoint system, use the “MX” record for the delegated domain referring to that Mirapoint system. As of release 2.9.3, you are allowed to configure an “A” or “CNAME” record as well. This enables users to directly log in to a delegated domain.

To enable inbound routers to deliver mail correctly for delegated domains, use LDAP routing for all messages (SMTP service setting, **Use LDAP Routing: For All Messages**). If you’re not using LDAP, you need to configure SMTP mail domains on the inbound router(s) for the delegated domain(s) to which they are delivering. Otherwise, user@toplevel and user@delegated will be sent to the same place. For information about configuring mail domains, see [“Setting SMTP Security Checks and Mail Domains” on page 130.](#)”



If the Administration Suite LDAP provisioning pages have been enabled through the CLI and you can use them to update the LDAP database for the domain, the domain is labelled as an **LDAP Domain**; otherwise it is simply labelled **Domain**.

When the LDAP provisioning pages are enabled, the **Domains > Administration, Domains > Add User and Class of Service** pages can be

used to modify your LDAP database and the label **LDAP Enabled** appears at the bottom of each page.



The delegated domains Administration Suite pages are a licensed feature used by message store appliances. (This license is not required to manage delegated domains through the CLI.)

Note: The **Domains > Administration** and **Class of Service** pages require special licenses to display. See [“Setting Up a User Directory Service” on page 80](#) for details on configuring your system to enable this LDAP feature.

Domain Sensitivity

Some commands behave differently if a delegated domain is selected see [“Selecting a Domain” on page 265](#) for details about selecting and working with domains. In particular, tasks that affect user accounts, folders, and distribution lists are all domain-sensitive. Some tasks are not allowed at all when a delegated domain is selected. Other tasks are only allowed when a delegated domain is selected or you log in to a delegated domain as the domain administrator.

Adding Delegated Domains

To add a delegated domain, you need to:

1. Name the domain and set the basic configuration. This is discussed in this section.
2. Create an administrator for the domain. This is discussed in [“Creating an Administrator for a Delegated Domain” on page 263](#).
3. Assign the domain administrator to the postmaster distribution list. This is discussed in [“Adding Delegated Domain Administrators to the Postmaster DL” on page 264](#).
4. Configure settings for policy management, calendar defaults, and customization as needed. These options are discussed in [“Editing Delegated Domains” on page 267](#) and [“Configuring Calendar Options for Domains” on page 274](#).

Use the **Domains > Administer Domains** page shown in Figure 32 to add, view, edit, or delete domains.

The domain table shown on the **Administer Domains** page lists all of the configured domains. This table displays ten domains at a time; click **Prev** and **Next** to page through the list.



Even if you currently only expect to use a single domain, Mirapoint recommends that you create your domain as a delegated domain rather than using the primary domain. This provides you with the flexibility of adding additional namespaces later. When you have delegated domains, only use the primary domain for administration. Do all mail handling through the delegated domains.

The screenshot shows the 'Administer Domains' page in the Mirapoint Message Server interface. The page title is 'Administer Domains' and the breadcrumb is 'Home > Domains > Administration'. The page contains a form for adding a new domain with the following fields:

- Domain Name: testDom.com
- Domain Disk Quota: 1000000 KB
- Maximum Users: 100
- Junkmail Manager Host: doc2.mirapoint.com

There are three checkboxes on the right side of the form:

- Enable Distribution Lists
- Enable Mail Forwarding
- Enable Automatic Reply

Below the form is a table of existing domains:

Domain	Used / Quota (KB)	Max Users	JMM Host	Edit	Delete
<primary>					
example.com	no quota	20			

At the bottom of the page, the domain 'example.com' is listed with the user 'administrator' and the status 'LDAP enabled'. Annotations with arrows point to the 'Add Domain' button, the 'Junkmail Manager Host' field, and the 'LDAP enabled' status.

Figure 32 Domains > Administer Domains Page, Add a Domain

To add a new domain, make these specifications and then click **Add Domain**:

- ◆ **Domain Name:** The domain name must include the top-level domain; for example “.com,” “.net,” “.org,” and so forth. When

users log in to that domain, they enter *username@domainname* in the User login field—for example, “jSmith@example.com.”

- ◆ **Domain Disk Quota:** The maximum disk space in kilobytes that the domain can use (includes all data), ranging from 0 (zero space allowed) on up. The default is no quota, implying unlimited disk space. To restore the default, set the disk quota to -1 (minus one).
- ◆ **Maximum Users:** The maximum number of users allowed in the domain. The value must be a non-negative integer. Specifying a value of 0 allows the domain to contain an unlimited number of users. If you do not set this parameter, the number of domain users defaults to 20. **Note:** Each user account on a domain requires space allocation for mail and puts a load on the network when actively in use.
- ◆ **Class of Service (COS)** (displays if you have COS and LDAP provisioning enabled): Allows you to assign a default COS to the domain that is used if a user is not assigned an individual COS. Select from your configured Classes of Service. If you select a COS for a domain, the attributes of that COS are applied to the domain regardless of any specifications you make on this page; instead, make those changes on the **Class of Service** page to the COS itself. See [“Managing Classes of Service” on page 317](#).
- ◆ **Enable Distribution Lists:** Specifies whether administrators of the domain can create and add users to distribution lists. The value is either **On** (selected) or **Off** (not selected). By default, distribution lists are enabled.
- ◆ **Enable Mail Forwarding:** Specifies whether users can enable automatic forwarding for their mailboxes. The value is either **On** (selected) or **Off** (not selected). By default, mail forwarding is enabled.
- ◆ **Enable Automatic Replies** (also known as Vacation Mail): Whether users can enable automatic replies for their folders. The value is either **On** (selected) or **Off** (not selected). By default, automatic replies are enabled. When enabled, the **Auto-reply** link displays in the user’s **Options** menu in WebMail.
- ◆ **Junkmail Manager Host:** The IP address or hostname of the appliance on which Junk Mail Manager is licensed and configured.

This option only displays if you have LDAP provisioning for JMM enabled; see [“Adding Junk Mail Manager User Accounts” on page 166](#) for details.

Once you click **Add Domain**, the new domain is added to the domain list table and is automatically the “selected” domain (indicated in the bottom left corner) so you can continue configuring it. The domains display in alphabetical order, so the new domain you add might not be on the first page; use **Prev** and **Next** to page through the list.

Creating an Administrator for a Delegated Domain

An administrator is a user with special privileges; a delegated domain administrator has privileges to administer only the delegated domain in which her or his account was created. See [“About Users and Administrators” on page 289](#) for more details. To create a delegated domain administrator, follow these steps.

1. On the **Domains > Administration** page, select the domain for which you want to create an administrator. (Select the radio button for the domain and click the **Select Domain** button.)
Result: The currently selected domain is displayed in the bottom left corner.
2. Click **Users** in the left page menu to display the **Domains > User** page for the selected domain.
3. On the **Domains > User** page:
 - a. Enter a User Name and password for the new administrator.
 - b. Select the **Domain administrator** role checkbox.
 - c. Configure optional settings for the new administrator:
 - ❖ **Folder Quota:** The amount of space this administrator’s account can consume in this domain.
 - ❖ **JMM (Junk Mail Manager) Folder Quota** (displays if JMM is an enabled service for this user): The amount of space this user’s JMM account can consume in JMM.
 - ❖ **Aliases:** Alternate email addresses. Click **More >>** to add more aliases.


- ❖ **Class of Service:** Sets of features and restraints (quotas, etc.) that you configure; COS must be enabled and configured for this option to display. See [“Managing Classes of Service” on page 317](#) for details.
4. When you are finished entering information for the new domain administrator, click the **Add User** button on the **Domains > User** page.

Result: The new user is added to the system with the parameters specified and the privileges of delegated **Domain administrator**. When this user logs in to that delegated domain by entering *username@delegateddomain* in the **Username** field on the **Login** page, the **Domains** pages for that delegated domain display and this user can administer for that delegated domain’s users, folders, distribution lists, the domain signature, over-quota message, white list, black list, mailing list exemptions, message filters, and catch-all address.

For more details about working with users, see [“Managing User Accounts” on page 288](#).

Adding Delegated Domain Administrators to the Postmaster DL

Once you have created delegated domain administrators, ensure that they receive the postmaster emails for that delegated domain so that they are notified of any problems with the domain. To do this, follow these steps.

1. On the **Domains > Administration** page, select the domain for which you want an administrator.
Result: That domain displays as selected in the bottom left corner.
2. On the **Domains > Distribution Lists** page click the **Edit** icon  for the postmaster DL.
Result: The **Edit Distribution List** page displays.
3. From the users in the **Add to postmaster** column, select the delegated domain administrators that you want to add to the postmaster DL and click **Add Member**. To remove users, click **Remove**. Finish by clicking **Done**.
Result: The selected users are added to (or removed from,

respectively) the postmaster DL. Alerts and other mails sent automatically to the postmaster DL for that delegated domain are also received by the users you added.

Note: When you add delegated domain administrators to the postmaster DL, remove the "Administrator" entry from the DL.

For more details about working with distribution lists (DLs), see [“Managing Distribution Lists” on page 310](#).

Finding a Delegated Domain

If have a large number of delegated domains, you can search for the domain you’re interested in rather than paging through the list. (The system can support over 100,000 delegated domains.)

To find a delegated domain, on the **Administer Domains** page, enter a name in the **Domain Name** text box and click **Find** to display only those domains matching the entered name. You can use the question mark (?) wildcard to match any single character, or the asterisk (*) wildcard to match zero or more characters of any kind. Click **Clear** to empty the options of any text that you have entered and re-display the entire domain list (ten names display per page).

Selecting a Domain

Before you can modify or administer a delegated domain, you need to select it on the **Domains > Administer Domains** page (see Figure 33).

To select a domain:

1. Locate the domain you want to select in the table of domains shown on the **Domains > Administer Domains** page. You can page through the list using the **Prev** and **Next** links, or search for a domain as described in the previous section, “Finding a Delegated Domain.”
2. Select the radio button for the domain and click **Select Domain**.

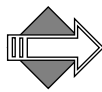
The domain that’s currently selected is displayed in the bottom left corner of the **Administer Domains** page.

The screenshot shows the 'Administer Domains' page in the Mirapoint Message Server Administration interface. The page includes a sidebar with navigation options like Users, Folders, and Distribution Lists. The main content area has input fields for Domain Name (deldom1.com), Domain Disk Quota (1046 KB), and Maximum Users (500). There are checkboxes for 'Enable Distribution Lists', 'Enable Mail Forwarding', and 'Enable Automatic Reply'. A table lists domains, with 'example.com' selected. A 'Select Domain' button is highlighted, and a 'Domain: <example>' indicator is shown at the bottom left. Annotations with arrows point to the 'example.com' row and the 'Domain: <example>' indicator.

Figure 33 Domains > Administer Domains Page, Select a Domain

Once a domain has been selected, all of the **Domains** pages operate only on that domain; additionally, the **Domains > Catch-All** and **Domains > Message Filters** pages only display after a delegated domain has been selected.

When you select a domain, the **Domain** *domain name* indicator in the bottom left corner of the all of the **Domains** pages changes to the current selected domain and all specifications you make using the **Domains** pages apply only to that domain. For example, if you create a user, **george**, while the delegated domain **example.com** is selected, you create an Inbox that is addressable as **george@example.com**. If, however, you create a user when no delegated domain is selected as current, you create an Inbox in your system's primary DNS domain.



Domain Administrators cannot select domains. If you are a Domain Administrator you must log in directly to your domain by entering your user name plus domain name in the **User** option on the **Login** page; for example, **DomAdmin@example.com**. All of the pages and options that display only affect the domain to which you logged in.

Accessing a Delegated Domain User's Folder

To access a user's folder in a delegated domain, you must have administrator permissions for that domain. As a system administrator, you have administration permissions for the primary domain, but not for any delegated domains; those privileges are assigned to the delegated domain administrator.

If you need to access a user's folder in a delegated domain, you can designate yourself as a domain administrator and adjust the permissions on the user's folder so you can access it.

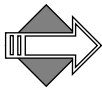
Note: You must have system administrator permissions to designate yourself (or anyone else) as a domain administrator.

To assign yourself domain administrator permissions:

1. Create a user account for yourself within the delegated domain. ([“Adding Users” on page 292](#) describes how to do this.)
2. Designate yourself as an administrator by selecting the delegated domain on the **Domains > Administration** page, and then using the **Domains > Add User** page to add yourself as that delegated domains' administrator. (See [“Creating an Administrator for a Delegated Domain” on page 263](#) for more information.)
3. Adjust the permissions of the folder you want to access to include your administrator account. ([“Changing Folder Access Control” on page 305](#) describes how to do this.)
4. Use a standard IMAP or WebMail client to access the messages in the folder.

Editing Delegated Domains

To edit a delegated domain, you must first select it, see [“Selecting a Domain” on page 265](#) for details.




If you select a COS for a domain, the attributes of that COS are applied to the domain regardless of any specifications you make on the **Domains** pages; instead, make those changes on the **Class of Service** page to the COS itself. See [“Managing Classes of Service” on page 317](#).

Basic Configuration Options

The basic configuration options that can be set on the **Administer Domains** page are:

- ◆ **Domain Disk Quota:** The maximum disk space in kilobytes that the domain can use. The default is no quota, implying unlimited disk space. To restore the default, set the disk quota to -1 (minus one).
- ◆ **Maximum Users:** The maximum number of users allowed in the domain. The value must be a non-negative integer. Specifying a value of 0 allows the domain to contain an unlimited number of users. Default is 20.
- ◆ **Class of Service (COS)** (displays if you have COS and LDAP provisioning enabled): Select from your configured Classes of Service.
- ◆ **Enable Distribution Lists:** Specifies whether administrators of the domain can create and add users to distribution lists.
- ◆ **Enable Mail Forwarding:** Specifies whether domain users can enable automatic forwarding for their mailboxes.
- ◆ **Enable Automatic Replies** (also known as Vacation Mail): Specifies whether users in the domain can enable automatic replies for their folders.
- ◆ **Junkmail Manager Host:** The IP address or hostname of the appliance on which Junk Mail Manager is licensed and configured. This option only displays if you have LDAP provisioning for JMM enabled.

To modify these options, click the **Edit** icon  for the domain you want to modify, make your changes, and click **OK**. To set other configuration options, use the links in the left page menu. These options are discussed in the following sections.

Creating Folders for a Delegated Domain

You create folders for a delegated domain in the same way that you create folders for the primary domain, by using the **Domains > Folders** page (see Figure 34 for an example) for the selected delegated domain.

Enter a folder name and click **Add**. Be sure to expand the **user** folder so your new folder is created as a sub-folder of the **user** folder, if you want that folder to receive mail addressed to that domain. See [“Managing Folders” on page 300](#) for details. See [“Folder Access Control Lists” on page 301](#) for details on folder access control.

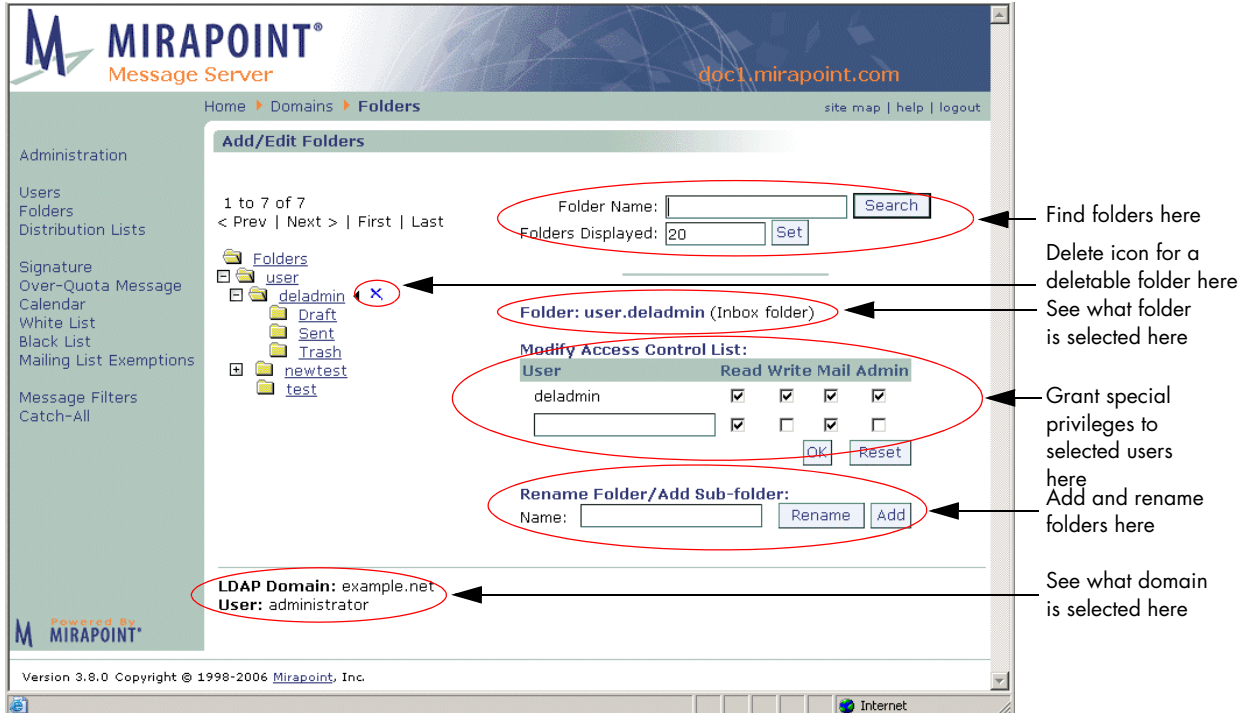



Figure 34 Delegated Domains Folders Page

Creating Distribution Lists for a Delegated Domain

Use the **Domains > Distribution Lists** page (see Figure 35 for an example) for the selected delegated domain to create domain specific distribution lists (DLs). Enter a DL name and click **Add**; then click the

Edit icon  for that DL to open the **Edit Distribution List** page. Select users or DLs in the **Add to DL name** column and click **Add Member**. See [“Managing Distribution Lists” on page 310](#) for details.

Click the Edit icon on the Add Distribution List page to open the Edit Distribution List page

Home > Domains > Distribution Lists

Add Distribution List

DL Name: newDL
Add Find Clear

1 to 2 of 2 <Prev | Next>

DL Name	Edit
<input type="checkbox"/> mailer-daemon	
<input type="checkbox"/> postmaster	

Remove

LDAP Domain: example.net
User: administrator

Signature
Over-Quota Message
Calendar
White List
Black List
Mailing List Exemptions

Message Filters
Catch-All

Powered by
MIRAPPOINT

Version 3.8.0 Copyright © 1998-2006 Mirapoint, Inc.

Home > Domains > Distribution Lists

Edit Distribution List

Members in postmaster

Member Name:
Add Find Clear

1 to 3 of 3 <Prev | Next>

Member Name
<input type="checkbox"/> deladmin
<input type="checkbox"/> newtest
<input type="checkbox"/> postmaster@localhost

Remove

Done

LDAP Domain: example.net
User: administrator

Add to postmaster

Display List: Users | DLs

User Name:
Full Name:
Find Clear

1 to 3 of 3 <Prev | Next>

User Name	Full Name
<input type="checkbox"/> deladmin	
<input type="checkbox"/> newtest	
<input type="checkbox"/> test	

<< Add Member

Find existing users or DLs here

Select and add users or DLs here

Figure 35 Delegated Domains Distribution List Page

Creating a Signature for a Delegated Domain

The **Domain > Set Signature** page (see Figure 36) lets you create a signature that most mailers automatically append to the body of messages; the signature might appear to the email recipient as an attachment, depending on how the mailer handles multipart MIME messages. Enter into the **Signature** option the text that you want appended to all email emanating from that domain; the current size

limit on the signature is 1024 bytes. Click **Apply** to enter your changes. Click **Clear** to empty the options of any text that you have entered.

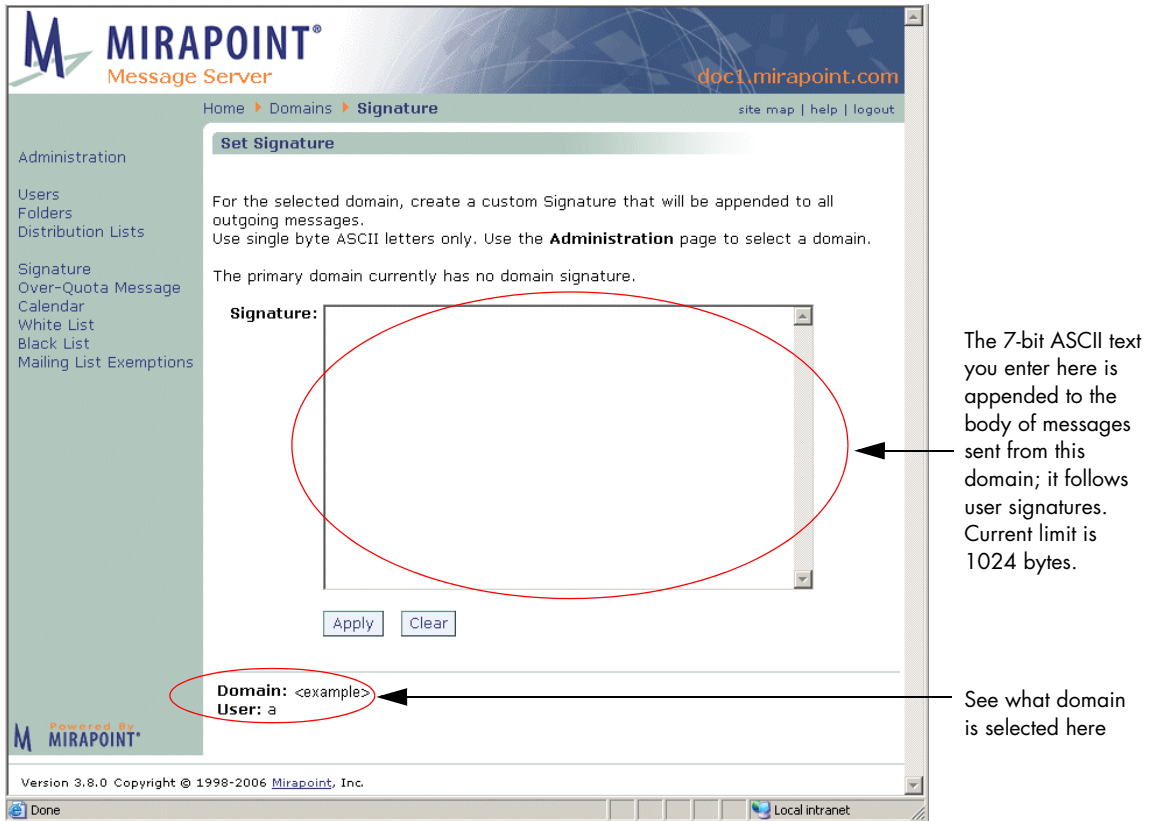


Figure 36 Domains > Signature Page

Customizing the Over-Quota Message

Use the **Domains > Over-Quota Message** page (see Figure 37 for an example) to customize the warning message that is delivered when a user's folder has gone over its allocated size limit. Specify the **From** field

and select the character set. Click **Apply** to instantiate your changes; click **Restore to Default** to use the system default Over-Quota message.

MIRAPOINT®
Message Server
doc1.mirapoint.com

Home > Domains > Over-Quota Message

Administration

Users
Folders
Distribution Lists

Signature
Over-Quota Message
Calendar
White List
Black List
Mailing List Exemptions

Set Over-Quota Message

For the selected domain, create a custom Over-Quota message that users will receive when they have reached their folder quota. This message is overwritten if a brand with a custom Over-Quota message is used by that domain.

This is the over-quota message for the primary domain:

From:

Subject: Over-Quota!

Message: One or more messages could not be delivered to you because they would have put you over quota. The system will keep trying to deliver these messages. To receive them, you must delete some old messages.

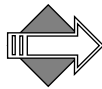
Charset: Unicode (UTF-8)

Domain: <example>
User: a

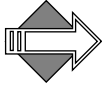
Version 3.8.0 Copyright © 1998-2006 Mirapoint, Inc.

See what domain is selected here

Figure 37 Domains > Over-Quota Message Page



The over-quota message you customize on the **Domains > Over-Quota Message** page is associated with the domain that you select in the **Domain > Administration** page. If the domain is assigned to a named brand, this over-quota message overrides the named brand's over-quota message. The Over-Quota Message also can be edited for the primary domain. If you edit it for the primary domain, it applies to all the domains that have **Default** as their over-quota message.



The over-quota message is triggered when the IMAP **Quota Warning** value is reached; by default this is 90% so when a folder reaches 90% of its quota, the over-quota message is sent. The **Quota Warning** value can be modified on the **System > Services > IMAP** page. In delegated domains, the quota warning level is inherited from the primary domain.


Establishing Delegated Domain Policies

Delegated domain policies are the features and controls (filters, quotas, etc.) that are allowed per domain. You create delegated domain policies by setting up antispam and content filters on a domain basis. What you need to know to create policies for domains is discussed in detail in [Chapter 8, “Policy Tasks.”](#)

Changing the User Limit in a Delegated Domain

You can change the default user limit (20 users) in a delegated domain. If you have an unlimited user license on your system, you can set this value to unlimited.

To change the user limit for a delegated domain, use the

Domains > Administration page (see Figure 32). Click the **Edit** icon  for the domain you want to modify, change its **Maximum User** option and click **OK**.

Limiting Delegated Domain Service Policies

You can limit the services, or features, available to users in a delegated domain by creating a COS specifically with the attributes that you want and assigning it to the domain. To create a COS, see [“Managing Classes of Service” on page 317](#).

Allowing a Domain to Span Multiple Servers

To allow a domain to span multiple Message Servers:

1. Establish the same delegated domain on two (or more) Message Servers. You add domains through the **Domains > Administer**

Domains page, for more information see [“Adding Delegated Domains” on page 260](#).

2. Include LDAP records with the appropriate mailhost for each user. For more information, see [“Managing Delegated Domains” on page 258](#).
3. Make sure that your LMR, OMR, and WebMail OMR are set to route to all domains. For more information, see [“Managing Delegated Domains” on page 258](#).

Configuring Calendar Options for Domains

You can configure calendar options separately for each domain; however, the default values are optimal for most deployments.



In a multi-tier environment, you must have the LDAP Routing license in order for Group Calendar to work.

The calendar options you can configure include:

- ◆ **Main Configuration page:** Basic calendar settings including:
 - ❖ **Domain Settings:** Whether users can attach files to events and a size limit for those attachments.
 - ❖ **Default User Settings:** When the user’s day starts and ends, when they receive email and mobile reminders, the default user view, and when summaries are set. Users can change these settings.
- ◆ **Search Configuration page:** What databases are used for searches, necessary database parameters, and how many search results display per page.
- ◆ **Resources page:** What resources, such as conference rooms and equipment, are available for selection from the **New Event Schedule** tab’s **Choose a Resource** option.
- ◆ **Subscribed page:** Other calendars that you want to display in the calendar of the delegated domain’s users; or that you want available to them to subscribe to. To set up a calendar that can be subscribed to, including creating a calendar for subscription use, see [“Calendar—Setting Up Calendar Subscriptions” on page 282](#).

Before making Calendar configurations through the Administration Suite, you must add the Group Calendar URL to each delegated domain. To do this, follow these steps.

Adding Group Calendar to Delegated Domains

Adding group calendar must be done at the command line (CLI) for each delegated domain. To do this, follow these steps.

1. Telnet your Message Server and log in as administrator. From a command line, enter:

```
User: telnet hostname.yourdomain.com
OK hostname.yourdomain.com admind 3.8 server ready
User: Administrator
Password:
OK User logged in
```

2. Select the delegated domain by entering this command where *delDomName* is the name of the delegated domain that you want to administer:

```
hostname.com> domain setcurrent delDomName
OK Completed
```

3. Enter **Url Add** so group calendar users can find each other, possibly on different servers. If you choose, replace *User Lookup* with a custom name for this lookup. You must change *delDomName* to the name of the current delegated domain. Note, this URL uses “127.0.0.1” (“localhost”), change this to your LDAP server, if appropriate:

```
hostname.com> url add groupcalendar:userlookup "User
Lookup" ldap://127.0.0.1:389/
miDomainName=delDomName,ou=domains,o=miratop?cn,miloginid?sub?(&(|(objectclass=person)(objectclass=inetorgperson)(objectclass=mirapointUser))(|(uid=$(cn)*)(miloginid=$(cn)*)(sn=$(cn)*)(givenname=$(cn)*)))" "(uidalias=miloginid)"
OK Completed
```

Note: The system LDIF uses **miloginid** to identify the user, not **uid**. In fact, the LDIF does not contain a uid at all. For this reason, the search query must be defined to return miloginid instead of uid (this is the **?cn,miloginid?** portion of the URL). Since Calendar assumes that uid is the attribute used to uniquely identify users, this URL

must tell it to use `miloginid` instead (this is the `(uidalias=miloginid)` portion of the URL).

4. Enter **Url Add** again so calendar users can locate resourcegroups, possibly on different servers. If you choose, replace *Group Lookup* with a custom name for this lookup. You must change *delDomainName* to the name of the current delegated domain. Note, this URL uses “127.0.0.1” (“localhost”), change this to your LDAP server, if appropriate:

```
hostname.com> url add groupcalendar:grouplookup "Group Lookup"
"ldap://127.0.0.1:389/
miDomainName=delDomainName,ou=domains,o=miratop?mail?sub?(mail=*(
cn)*)" "(cnalias=mail)"
```

If you need to re-enter the **Url Add** command, first delete the previous one with this command where *name* is the name of the url you are deleting and *instance* is the particular instance you are deleting:

```
hostname.com> url delete "name:instance"
OK Completed
```

For example, this command...

```
hostname.com> url delete groupcalendar:userlookup
OK Completed
```

...deletes the URL you added in step 3, above.

5. Set the Group Calendar mode to LDAP (or ALL; ALL looks in LDAP first and then locally for users), enter this command:

```
hostname.com> calendar set groupcalmode ALL
OK Completed
```

Note: The **userlookup** query (step 3) describes a user URL mapping for group calendar, while the **grouplookup** query (step 4) describes a group URL mapping. In the examples above, **User Lookup** and **Group Lookup** are just arbitrary labels for the class instance. The **ldap://** URLs are very complicated, being built up by substituted components into a DN.

Now, you can use the Administration Suite **Domains > Calendar** pages to add a resourcegroup and resources and set other calendar defaults as described in the next sections.

Setting Domain & User Defaults (Main Configuration)

Use the **Domains > Calendar > Main Configuration** page (see Figure 38 for an example) to set basic calendar defaults.

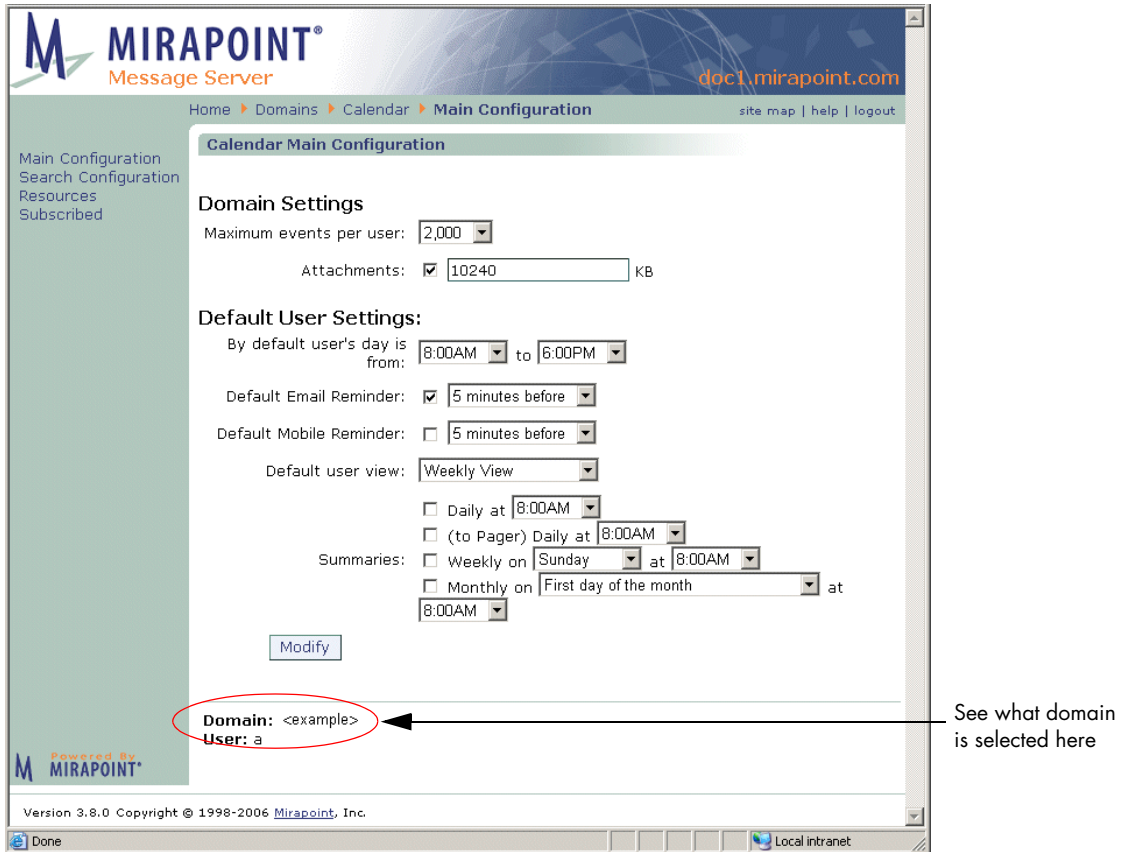


Figure 38 Domains > Calendar > Main Configuration Page

Specify the following:

- ◆ **Maximum events per user:** Maximum number of events allowed per calendar. The default is 2000, which enables each WebCal user to have up to 2000 events in their calendar.

- ◆ **Attachments** (default is enabled; users can attach files to event invitations): Whether attachments to event invitations are allowed. Also, the maximum size for same; default size allowed is 10240kb.
- ◆ **By default, user's day is from/to** (default is 8am to 6pm): Time at which the user's day begins and ends; select from a pull-down list of hours.
- ◆ **Default Email Reminder** (default is enabled; users receive email reminders of events): Whether email reminders of an event are sent or not, and the number of minutes before an event that an email reminder should be sent.
- ◆ **Default user view** (default is Weekly view): Default calendar view (daily, weekly, monthly, or horizontal-weekly).
- ◆ **Default Mobile Reminder** (default is disabled; users do not receive mobile reminders): Whether mobile reminders are sent; select to enable. **Note:** These summaries are sent to the **Mobile Device** number entered by the user on their **Options > Calendar > Reminders** (Corporate Edition) or **Calendar > Preferences** (Standard Edition) page, respectively. Also, specify the number of minutes before an event that a pager reminder should be sent.
- ◆ **Summaries** (default is deselected for all; no summaries are sent): When summaries of Calendar events are sent; select and specify times for up to four default notification schemes:
 - ❖ **Daily:** When to send a daily email summary.
 - ❖ **(to Pager) Daily:** When to send a daily pager summary.
 - ❖ **Weekly on:** When to send a weekly summary.
 - ❖ **Monthly on:** When to send a monthly summary.

Click **Modify** to enter your changes.

Calendar—Configuring Search

Use the **Domains > Calendar > Search Configuration** page (see Figure 39 for an example) to set up default search parameters.

The screenshot shows the 'Calendar Search' configuration page in the Mirapoint Message Server. The page includes a navigation breadcrumb: Home > Domains > Calendar > Search Configuration. On the left, there is a sidebar with links for Main Configuration, Search Configuration, Resources, and Subscribed. The main content area is titled 'Calendar Search' and contains the following fields:

- User search method: A dropdown menu set to 'LDAP and local'.
- Maximum number of search results to display: A text input field containing '100'.
- LDAP Search parameters:
 - LDAP Server: A text input field containing 'localhost'.
 - Port: A text input field containing '389'.
 - Base DN: An empty text input field.
 - Search filter: A text input field containing '(&(|(objectclass=person)(objectclass=inetorgperson)(objectclass=org...))'. An arrow points to this field with the label 'LDAP Query String'.
 - A 'Set' button is located below the search filter field.
- Domain: A text input field containing '<example>'. An arrow points to this field with the label 'See what domain is selected here'. The 'Domain' label and the input field are circled in red.
- User: A text input field containing 'a'.

The footer of the page includes the Mirapoint logo and the text 'Powered by MIRAPOINT'. The browser's address bar shows 'Local intranet'.

Figure 39 Domains > Calendar > Search Configuration Page

Specify the following:

- ◆ **User search method:** Controls whether calendar uses LDAP, the local system, or both to find users and distribution lists.
 - ❖ **LDAP and local** (default): Searches both your LDAP database and calendar users local to the machine.
 - ❖ **Local only:** Searches only users local to the machine.
 - ❖ **LDAP only:** Searches only your LDAP database.

- ◆ **Maximum number of search records to display:** Maximum number of records returned. Default is 100. When using LDAP, this number is restricted by the configured **Ldap Search Slimit**; for more information, see the CLI Help About Ldap.
- ◆ LDAP Search parameters (only displays if LDAP routing is licensed), these include the following:
 - ❖ **LDAP server:** The hostname of the machine that runs your LDAP service.
 - ❖ **Port:** The port to use to connect to the LDAP server.
 - ❖ **Base dn:** The part of the LDAP DIT at which you want searches to start.
 - ❖ **Search filter:** You can change the LDAP search filter if needed.

Click **Set** to save your changes.

Calendar—Configuring Resources

Use the **Domains > Calendar > Resources** page (see Figure 40 for an example) to add resources such as meeting rooms and projectors. Be sure to select the desired delegated domain first.

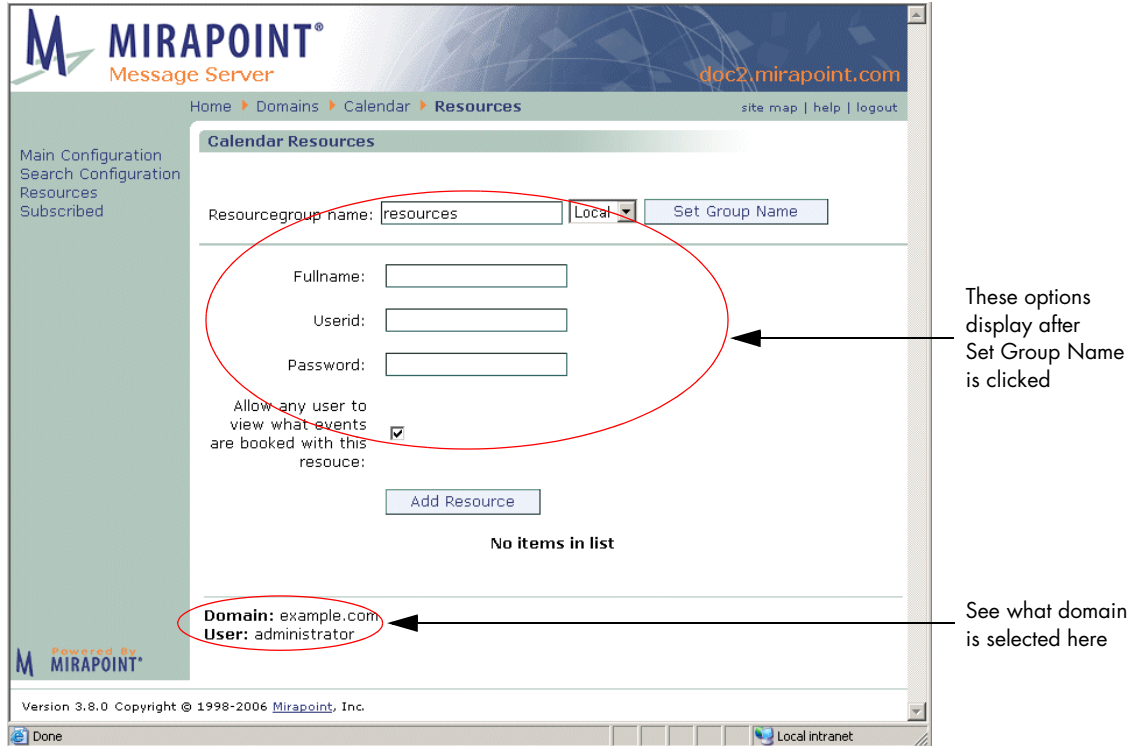


Figure 40 Domains > Calendar > Resources Page

1. In the **Resourcegroup name** option, enter a name for the mailgroup or distribution list that holds all of your calendar resources; for example, resources. Also, select a database, **Local** or **LDAP**. If you select **Local**, the distribution list is created locally. If you select **LDAP**, a mailgroup of the specified name is added to your LDAP. Click **Set Group Name**.
Result: Additional options display that enable you to set actual

resources. This entry becomes a distribution list if **Local** is selected; if **LDAP** is selected, it is a mailgroup.

2. Specify the following for each resource (meeting rooms, equipment such as projectors, and so forth) that you want to make available for calendar users. This information is added to the local resource repository. If you are using LDAP, you must enter already configured information.
 - ❖ **Fullname:** The name of the resource as you want it to appear in the **Choose a Resource** drop-down list of the **Schedules** tab for calendar new events.
 - ❖ **Userid:** Since this resource is treated as a user by the system, enter an identifier.
 - ❖ **Password:** Enter a password for the resource.
 - ❖ **Allow any user to view what events are booked with this resource** (default is enabled): This sets permissions so that all calendar users can see when the resource is available.
3. Click **Add Resource**.

Result: If you are using the **Local** database, your entries are written to the system and become available in the calendar **Schedules** tab **Choose a Resource** drop-down list. If you are using **LDAP**, the entries are made available in the calendar **Schedules** tab **Choose a Resource** drop-down list; lookups are sent to your LDAP database. Please note: Resources show up in address book as users.

Calendar—Setting Up Calendar Subscriptions

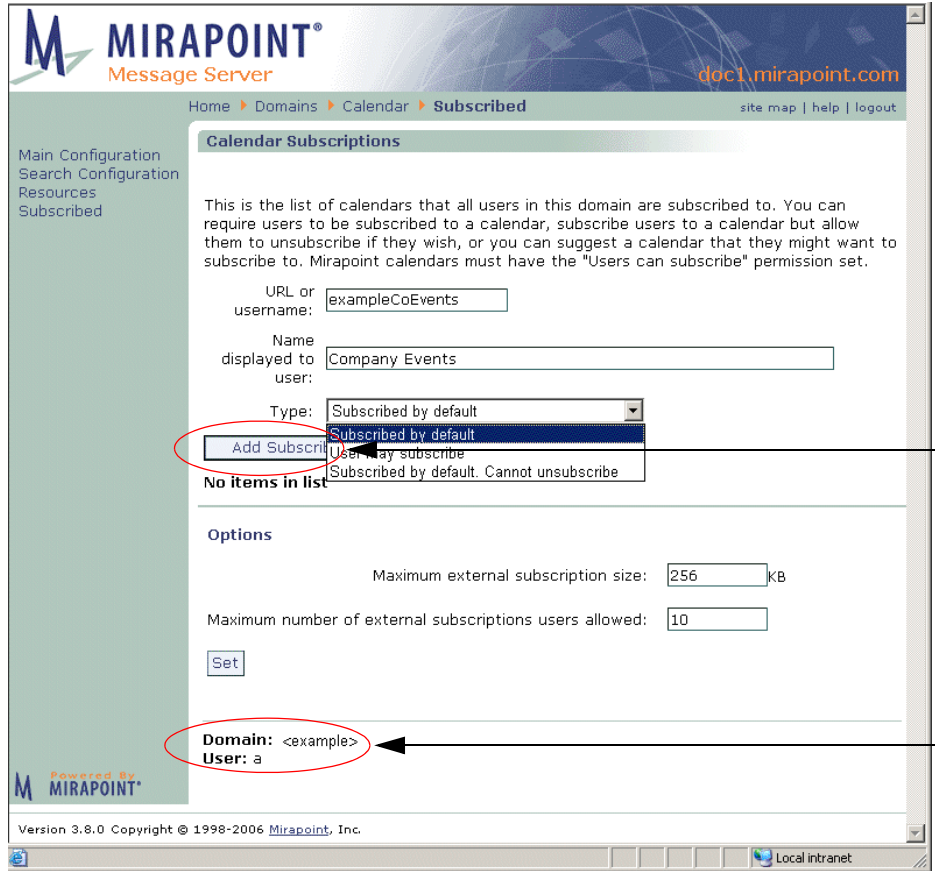
Use the **Domains > Calendar > Subscribed** page (see Figure 41 for an example) to subscribe users to other calendars, such as the Human Resources calendar of your company. Doing this is a two-procedure process as you must first have a calendar ready for other users. Both procedures are discussed in this section.

Creating a Calendar

You create calendars specifically for sharing. You can also share public iCal calendars.

To create a calendar:

1. Create (or request the creation of) a user account with the calendar name that you want; for example, “exampleCoEvents.” Note: The relationship between a calendar and a messaging user account is like that between a folder and a user account. However, a user can have only one calendar. Like user logins, calendar UIDs are *user@domain* for delegated domain users.
Result: That account has a default calendar available for use; you have a username to enter into the **URL or username** option of the **Domains > Calendar > Subscriptions** page (procedure follows)
2. Log in to the account and populate its calendar with the events that you want made available to other users.
Result: The calendar becomes filled with events.
3. On the **Options > Calendar > Sharing Controls** page (Corporate Edition) or the **Calendar > Preferences > Access Permissions** page (Standard Edition), select the Publish Calendar option.
Result: The permissions necessary for a calendar to be subscribed to are set.
4. Send out an email to users advising them that they can subscribe to this calendar. Or, use the following procedure to subscribe users to the calendar by default.
Result: When a user subscribes to another calendar, all that calendar’s events display in the user’s calendar with a green flag indicating a “subscribed-to” event.





Click here to add calendars

See what domain is selected here

Figure 41 Domains > Calendar > Subscribed Page

Subscribing Users to System Calendars



To subscribe users to other calendars in the system:

1. Go to the **Calendar > Subscriptions** page and specify:
 - ❖ **Username** of the calendar (the calendar must have permissions set so it can be subscribed to, see [“Creating a Calendar” on page 283](#) for details.
 - ❖ **Name displayed to user:** The name of the Calendar that users see; for example “U.S. Holidays.”
 - ❖ **Type:** Restrictions on the subscription, either:
 - **Subscribed by default** (default choice): The calendar displays in all configured user’s calendars; users can choose to unsubscribe (remove it from their calendar) by clicking the **Delete** icon  for it on their **Subscriptions** page.
 - **User can subscribe:** The calendar is available on all user’s **Subscriptions** page, as a **Suggestion**; they must subscribe to the calendar (click on it) to see the events.
 - **Subscribed by Default, Cannot unsubscribe:** The calendar displays in the user’s calendar, they cannot unsubscribe (the **Delete** icon  does not display).
2. Click **Set** to save your changes.
Result: The calendars that you make available in this way display on each users **Subscriptions** page.

Subscribing Users to Public iCal Calendars

Alternatively, you can make any public iCal calendar served via HTTP available to users. To do this:

1. Locate the calendar on the Internet and note the URL. (One source of shared calendars is icalshare.com, which publishes a free directory of shared calendars.)
Result: You have a URL to enter into the **URL or username** option of the **Domains > Calendar > Subscriptions** page (procedure follows).
2. On the **Calendar > Subscriptions** page, specify the following:

- ❖ **URL of the iCal calendar.** For example, `http://icalx.com/public/icalshare/US32Holidays.ics`.
- ❖ **Name displayed to user:** The name of the Calendar that users see; for example “U.S. Holidays.”
- ❖ **Type:** Restrictions on the subscription, either:
 - **Subscribed by default** (default choice): The calendar displays in all configured user’s calendars; users can choose to unsubscribe (remove it from their calendar) by clicking the **Delete** icon  for it on their **Subscriptions** page.
 - **User can subscribe:** The calendar is available on all user’s **Subscriptions** page, as a **Suggestion**; they must subscribe to the calendar (click on it) to see the events.
 - **Subscribed by Default, Cannot unsubscribe:** The calendar displays in the user’s calendar, they cannot unsubscribe (the **Delete** icon  does not display).
- ❖ **Maximum number of external subscriptions users allowed:** Sets the maximum number of external calendars to which each user can subscribe. Default is 10.
- ❖ **Maximum external subscription size:** Sets the maximum size of each external calendar to which users can subscribe, in KB. Default is 256.

Adding Directory Services to Delegated Domains

A directory service is an address book database. Adding a directory service must be done at the command line (CLI) for each delegated domain. To do this, follow these steps.

1. Telnet your Message Server and log in as administrator. From a command line, enter:

```
User: telnet hostname.yourdomain.com
OK hostname.yourdomain.com admin 3.8 server ready
User: Administrator
Password:
OK User logged in
```

- Select the delegated domain by entering this command:

```
hostname.com> domain setcurrent delegateddomainname
OK Completed
```

This is the **url add** command syntax (do not use a period or other special characters in the *instance* name):

```
url add "addrbook:instance" "description" "ldapurl" "options"
```

Add the directory service by entering this command all on one line where *delDom* and *Delegated Domain Directory* are identifiers for this directory service, *hostname* is the name of the machine with the LDAP database you are using (localhost=127.0.0.1), *port* is usually 389, *baseDN* is where you want the directory service lookups to start (this must match the delegated domain; example follows), and *sub* is your search filter (example follows). Basic syntax example:

```
hostname.com> url add addrbook:delDom "Delegated Domain Directory" "ldap://hostname:port/baseDN??sub?" ""
OK Completed
```

This example (below) uses Internal LDAP (127.0.0.1) and the Mirapoint schema plus a filter needed for Group Calendar. The variables, *delDom*, and *DelDom Directory* reflect the delegated domain to which this directory service is being added. The variable *delDomName.com* must be the name of the delegated domain to which this directory service is being added. Please note: Resources display as users in address book.



Mirapoint recommends using this example URL, modified as needed.

```
hostname.com> url add "addrbook:delDom" "DelDom Directory"
"ldap://127.0.0.1:389/
miDomainName=delDomName.com,ou=domains,o=miratop??sub?(&(object
class=mirapointmailuser)(|(sn=$(cn))(givenname=$(cn))(cn=$(cn))
(mail=$(mail)*)(maillocaladdress=$(mail)))" ""
OK Completed
```

This example uses *bindDN* and *password* to authenticate access (do not use unless you are very familiar with LDAP URLs).

```
hostname.com> url add addrbook:delDom "Delegated Domain Directory" "ldap://hostname:port/baseDN??sub?"
"(binddn=CN=Administrator,CN=Users,DC=adhostname,DC=yourdomain,
DC=com)(bindpasswd=password)"
OK Completed
```


This example shows how to supply a different search query filter; replaces “filter” in the syntax (do not use unless you are very familiar with LDAP URLs).

```
hostname.com> url add addrbook:org "Company Directory" "ldap://
hostname:port/
baseDN??sub?(&/ (cn=$(cn)) (mail=$(mail)))/ (objectclass
=person) (objectclass=inetorgperson))" ""
OK Completed
```

Deleting Delegated Domains

Use the **Domains > Administration** page (shown in Figure 32) to delete delegated domains. When you delete a domain, all folders, email messages, user accounts, distribution lists, and configuration data belonging to the domain are destroyed.

To delete a delegated domain:

1. Locate the domain you want to delete in the table of domains shown on the **Domains > Administer Domains** page. You can page through the list using the **Prev** and **Next** links, or search for a domain as described in [“Finding a Delegated Domain” on page 265.](#)
2. Click the **Delete** icon  for the domain you want to remove.
3. Click **OK** to confirm that you want to delete the domain and all of the data associated with the domain.

Result: All folders, email messages, user accounts, distribution lists, and configuration data belonging to the domain are destroyed.

Note: LDAP entries for the delegated domain are not deleted (unless you are using the LDAP GUI). You must clean up the LDAP directory separately.

Managing User Accounts

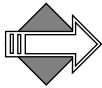
A user **account** specifies a login name and password that provides a user with access to the system. Each user has a main folder called the **Inbox**. Additional information associated with each user account includes

calendar data, WebMail settings, personal address book, personal dictionary, and forward and autoreply settings.

A password is a secret text string (numbers and letters) that is case sensitive and up to 80 characters long. The user's login name is used as the address for their Inbox. By default, user folders reside in the system folder called **user**.

About Users and Administrators

A **user** is a person who has an account on the system; an **administrator** is a user with special privileges. The initial administrator account is configured during setup; there are several types of administrator accounts that you can add later. A delegated domain administrator can only be created in a "selected" domain. A helpdesk administrator has the same privileges as a delegated domain administrator but is created in the primary domain and can log in to any domain. The quarantine administrator role is discussed below.



When you designate a user as an administrator, also add the user to the Service Reporting distribution list. For information about adding users to distribution lists, see ["Adding and Populating Distribution Lists" on page 312](#).

End-users can perform the following account management tasks on their own accounts using the WebMail **Options** pages or the Administration Suite **Account** pages (when an end-user logs in to the Administration Suite, they see only the **Account** pages):

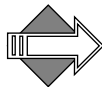
- ◆ Change their own password
- ◆ Set folder access control lists
- ◆ Set message filters and some Junk Mail Control options
- ◆ Set forwarding and automatic replies for messages

About the Quarantine Administrator User

As of release 3.6, there is a new way to manage email messages that receive the **Send to Quarantine folder** filter action: grant any user the new **Quarantine Administrator** role and enter that address for your filter. When a user with the Quarantine administrator role logs into

WebMail, they have two additional command buttons in their mail toolbar, **Deliver** and **Rescan**. The **Deliver** button releases selected quarantined message back into the mail queue; this could apply to any message quarantined by a content filter such as the Corporate Word list filter. The **Rescan** button submits selected messages to additional antivirus scanning; this is used only for messages quarantined by RAPID antivirus.

Users created in delegated domains, including Quarantine Administrator users, are restricted to the delegated domain in which they were created.



Only messages that received the **Send to Quarantine folder** filter action are eligible for the **Deliver** function through the Quarantine Administrator's WebMail. Those messages arrive in quarantine with special coding that allows them to be released back into the mail queue and delivered to the addressees without any indication that they were ever quarantined. Only messages that receive the RAPID AV quarantine action are eligible for the **Rescan** button.

For more information on the **Send to Quarantine folder** filter action, see [“How the Content Filtering Quarantine Works” on page 337](#).

User Account Requirements

For users to receive messages on a Mirapoint appliance, each must have a **user account** that specifies the following information:

- ◆ **Login name**—A unique text string identifying a user. Login names are case-insensitive and between one character and 80 characters long. Login names can include these 7-bit ASCII characters:
 - ❖ Letters (“A” through “Z” and “a” through “z”)
 - ❖ Numbers (“0” through “9”)
 - ❖ Minus (-) and underscore (_)
 - ❖ Blank space (); leading spaces are not allowed for POP login
 - ❖ Period (.) is allowed when using LDAP provisioning

Non-ASCII characters can be encoded in login names using modified UTF-7. See [“International Login Names” on page 291](#).

To support periods (.) in user folder addresses, you can create user names with underscores—for example **Firstname_Lastname**—and incoming mail for **Firstname.Lastname** automatically gets delivered.

- ◆ **Password**—A secret text string known only to its owner. When users log into POP, IMAP, WebMail, or Administration Suite, they must specify a login name and password to verify their identity. Passwords are case-sensitive and limited to 80 characters. You can set minimum length and required characters for user passwords with the **Auth Set** command. Non-ASCII passwords are allowed, although different input methods can cause incompatibility across platforms, so ASCII passwords are safer.
- ◆ **Full Name**—The preferred name of the person using the account; for example, their first and last names.

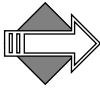
Email addresses should use ASCII alphanumeric characters (A-Z, a-z, 0-9) plus any of the following characters: + (plus), -(minus), . (period), _ (underscore).

These characters are definitely not allowed in email addresses:

! (exclamation point), " (double quote), # (number sign), \$ (dollar sign), % (percent), ((open parenthesis),) (close parenthesis), , (comma), : (colon), ; (semi-colon), < (less than), > (greater than), @ (at sign), [(open bracket),] (close bracket), \ (backslash), ` (accent grave), | (pipe).

These characters might be allowed but are generally not used:

& (ampersand), ' (single quote), * (asterisk), / (slash mark), = (equal sign), ? (question mark), ^ (circumflex), { (open brace), } (close brace), ~ (tilde).



On a RazorGate appliance, the number of users is limited to 20. This number can be raised by updating a license. (20 is usually sufficient, since only administrators need access to RazorGate appliances.)

International Login Names

Mirapoint appliances support international (8-bit) user names—user names are stored internally using UTF-8 encoding. For example, in the user name *soutien-clientèle*, the e-grave would be encoded as +AOg-: *soutien-client+AOg-le*.

Reserved Login Names

Login names are case-insensitive. You cannot create user accounts with the following reserved names:

- ◆ **administrator**—Users with special privileges.
- ◆ **administrators**—An account for all administrators.
- ◆ **anonymous**—By convention, users accessing a system with this login name don't have to enter a password. Anonymous logins are not permitted.
- ◆ **anybody**—A wildcard name.
- ◆ **anyone**—A wildcard name.
- ◆ **nobody**—A user account with severely restricted privileges.

Adding Users

Use the **Add User** page (see Figure 42 for an example) to modify user accounts, including the class of service for an account (if COS is

enabled), or to add, find, or modify system users, including setting folder quotas, and assigning administrator privileges.

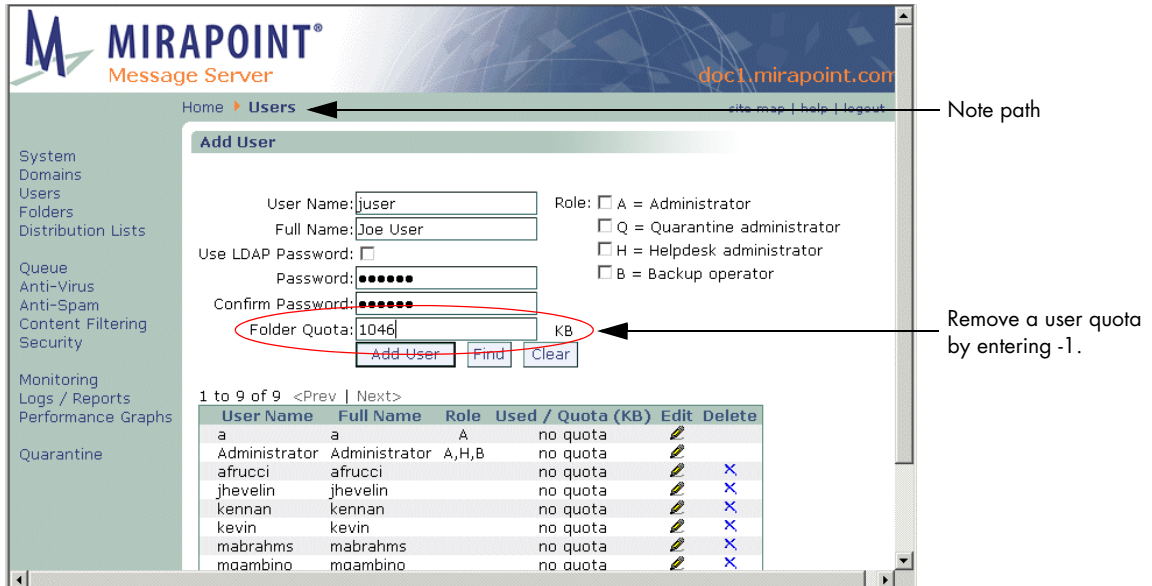


Figure 42 Mirapoint Add User Page



To manage a user in a delegated domain, select the domain first.

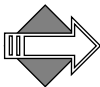
To add a new user, follow these steps on the **Add User** page.

1. All existing users, ten per page, display in a table on the **Add User** page. Click **Prev** and **Next** to page through the list of names. Click **Find** to display only those users matching the entered name. Click **Clear** to empty the options of any text that you have entered and re-display the entire user list (ten names display at a time)

2. Make these specifications:
 - ❖ **User Name:** This becomes the name of that user's folder under the **user** system directory, the first part of their email address, and their login name.
 - ❖ **Role:** Leave this option deselected (default) for regular users; select one of the following for administrators:
 - **Administrator:** This user has access to the full Administration Suite interface and is able to configure new users, domains, services, and so forth. If you logged in to a delegated domain, or selected a delegated domain first, the administrator you create here is for that domain only. See [“Creating an Administrator for a Delegated Domain” on page 263](#) for details.
 - **Quarantine Administrator:** This user has special access to WebMail and can examine, release to the mail queue, or reject (delete without notifying the addressee) or rescan messages that received the **Send to Quarantine folder** or the RAPID quarantine action. For details, see [“About the Quarantine Administrator User” on page 289](#).
 - **Helpdesk administrator:** This user has limited privileges; only the Administration Suite **Domain** pages and Mail logs for domains are available to them.
 - **Backup operator:** This user can perform all tasks necessary for system backups using the CLI. This is a read-only role that cannot change the system in any way.
 - ❖ **Full Name:** This name is displayed in messages alongside the user name.
 - ❖ Password options (select one method). **Note:** If LDAP provisioning is enabled, the **Use LDAP Password** checkbox does not display, whatever password is entered is written to LDAP automatically.
 - **Checkbox: Use LDAP Password:** Select this option if your LDAP is set up with passwords the local machine can access. If you select this option, you cannot specify a

password. This option does not display if LDAP provisioning is enabled.

- **Password:** A password for the user; if you use this option, the password is not entered into your LDAP database; it is local to the machine.
 - **Confirm Password:** Enter the password again.
 - ❖ **Folder Quota:** A quota for that user's system folder; all of their subfolders are included in the total set quota. You can completely remove a quota from a folder by entering -1. If a user is assigned a Class of Service (COS), the COS value for this option overrides any value entered here.
 - ❖ **JMM Folder Quota** (only displays if Junk Mail Manager is a service for this user): How many spam messages this JMM account accepts before being over-quota. If a user is assigned a COS, the COS value for this option overrides any value entered here.
 - ❖ **Alias(es)** (only displays if you have LDAP provisioning enabled; see [“Setting Up a User Directory Service” on page 80](#) for details): Use this option to set up alias email addresses for your users, the alias's domain must exist in LDAP. Please note: Mail addressed to the alias must be fully qualified (include the domain).
 - ❖ **Class of Service:** Select from any of your configured Class Of Services. This option only displays if you have enabled and configured Class of Service (COS).
3. Click **Add User**
Result: The new account is added to the user list table and a folder for them is added to the **user** folder hierarchy (see [“Managing Folders” on page 300](#) for details). The accounts display in alphabetical order, so the new user you add might not be on the first page; use **Prev** and **Next** to page through the list.




To change a user password, follow the steps described in [“Editing Users” on page 296](#).

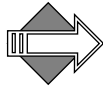
Finding a User

If you have a large number of users, you can search for the user you're interested in rather than paging through the list. (The system can support up to 500,000 users.)

To find an existing user, on the **Add User** page, enter a name in the **User Name** text box and click **Find** to display only those users matching the entered name. You can use the asterisk (*) wildcard, for any kind of character including the folder hierarchy separator period (.), or the percent sign (%) wildcard, for any kind of character NOT including the folder hierarchy separator period (.). Click **Clear** to empty the options of any text that you have entered and re-display the entire user list (ten names display per page).


Editing Users

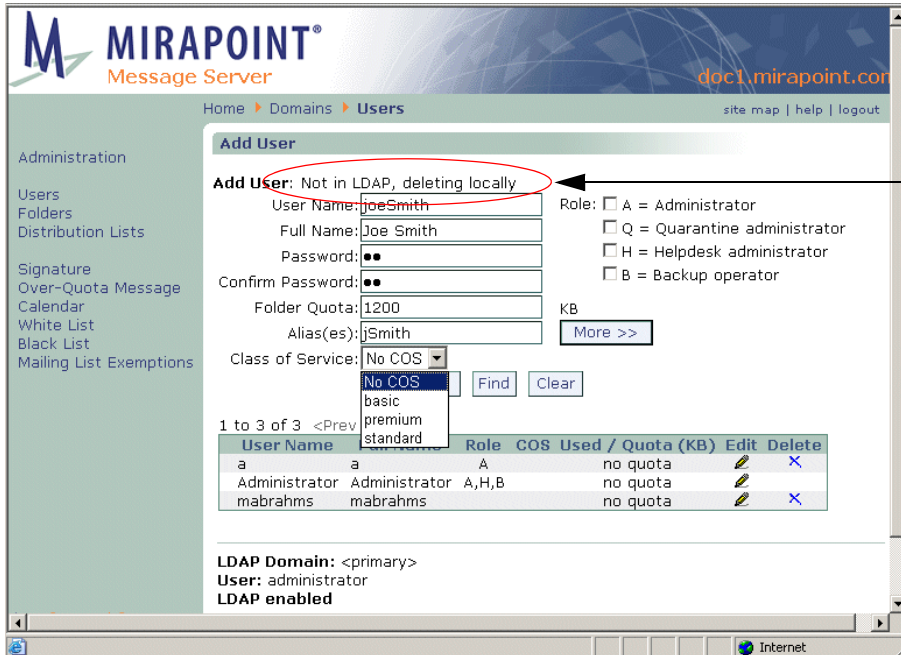
You can change a user password, folder quota, class or service, aliases, or role. To modify a configured user's account options, on the **Add User** page, click the **Edit** icon  for the user you want to modify. On the **Edit User** page, make the changes you want and click **OK** or **Cancel**. Result: If you click **OK**, the page displays a message confirming the modification. If you click **Cancel**, the **Add Users** page re-displays, your changes to that user are not made.



You can completely remove a quota from a folder by entering -1.

Deleting Users

To delete a user, on the **Add User** page, click the **Delete** icon  for the user you want to remove; click **Delete** to confirm. See Figure 43.



This message displays if the user you are deleting was added locally, not with the LDAP-enabled page

Figure 43 Mirapoint Add User Page, Deleted non-LDAP User

Viewing Presence/Last Login Times

To view the activity of an end user, you can look at the User Audit Trail report. This is discussed in detail in [“Using the User Audit Trail” on page 251](#).

Another way to view the logins of a user is through the Mail > Logins > Detailed report.

Establishing User Account Policies

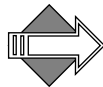
User account policies are the features and controls (filters, quotas, etc.) that are allowed per user. You create account policies by setting up antispam, quotas, and content filters on a per-user basis. What you need to know to create policies for individual user accounts is discussed in detail in [Chapter 8, “Policy Tasks.”](#)

Bulk Provisioning Users

Rather than adding users one at a time using the **Add User** page, you can enable LDAP autoprovisioning, write a script to convert your existing user database into LDAP, and import those user records into internal LDAP. Follow these steps:

1. Access the command line interface (CLI) by telnet-ing to your Message Server on the default telnet port (port 23) and logging in as the Administrator:

```
User: telnet hostname.domain.com
OK hostname.domain.com admind 3.8 server ready
User: Administrator
Password: password
OK User logged in
```



CLI commands are *not* case-sensitive. To make the examples easier to read, they are shown in mixed case.

2. Enable LDAP autoprovisioning by entering this command:

```
hostname.com> Ldap Set Autoprovision On
OK Completed
```

When users log in for the first time, or when the first e-mail arrives for them in their inbox, their account is automatically created from their user record in LDAP.

3. Locate a file of user data, for example names and e-mail addresses listed one per line.

If you find CSV (comma separated variable) data in Mirapoint AddressBook format, you can run the Perl program shown below to convert that data into LDAP data interchange format. AddressBook format stores the last name in field1, the first name in field2, and the e-mail address in field3. Later fields are not needed here.

```

#!/usr/local/bin/perl
while ( <> ) {
    @field = split /,/, $_ ;
    if (@field[2] =~ /@/) {
        ($uid, $domain) = split /@/, @field[2], 2 ;
print "dn: miloginid=$uid,miDomainName=primary,ou=domains,o=miratop\n" ;
        print "objectClass: mirapointUser\n" ;
        print "objectClass: mirapointMailUser\n" ;
        print "mail: ", @field[2], "\n" ;
        print "miloginid: ", $uid, "\n" ;
        print "cn: ", @field[1], " ", @field[0], "\n" ;
        print "mailhost: ", $domain, "\n" ;
        print "userPassword: ", reverse(split //, $uid), "88\n" ;
        print "\n" ; $lines++ ;
    }
}
if ($lines == 0) {
    print "CSV data lacks e-mail address in 3rd field\n" ;
}

```

Passwords are created by spelling the user's name backwards and appending "88". Change this, in case this book falls into the wrong hands. Furthermore, encourage all users to change their passwords as soon as possible.

4. Once you have created LDAP data interchange format from your script or the Perl program shown above, place it into an accessible file on an FTP or HTTP server.
5. Now import it to your LDAP server. This example uses output file "userdb.ldif" on the "example.com" web server.

```

> Dir Importldif o=miratop c http://example.com/userdb.ldif
NN of NN records inserted
OK Completed

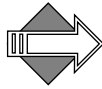
```

6. Test the set up by logging in as a newly created user. Inbox, folders, and junk mail filter will be present after a successful login.

Managing Folders

A **folder** is a container that can store email messages and other folders. It also has attributes such as a disk quota, access control and possibly filters.

On Mirapoint systems, folders are created and exist in a hierarchy. The base of the hierarchy, or tree, is called the **root**. The period (.) character is used as the folder hierarchy separator. The main mail folder for any account is the **Inbox** folder, where email messages addressed to the user are delivered. When you use the Administration Suite to create a new user account, an Inbox for that user is created automatically. The Inbox name takes the user's login name. For example, the Inbox for a user with the login name **glenn** would be named **user.glenn**. When **glenn** logs in to his account, however, the name appears to him as "Inbox."



The **Folders > Add/Edit Folders** page opens with the system folders displayed at the top-most level; see Figure 44 for an example. The **user** folder contains all of the user account mail folders; click the **user** folder to expand the tree view to show all defined user folders; see Figure 46 for an example.

When you open the **user** folder tree view, the page displays additional options for managing existing user folders. When the **user** folder view is closed, you can add new folders to the system.

Folder Naming Conventions

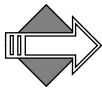
Every folder on a Mirapoint message server must have a unique name. Folder names, including any subfolders, are limited to 200 bytes in length.

- ◆ Letters (A through Z and a through z)
- ◆ Numbers (0 through 9)
- ◆ Space ()
- ◆ Minus (-)
- ◆ Underscore (_)

Special Characters You Cannot Use

You cannot use the following characters in folder names because they have special meanings:

- ◆ Period (.)—Used as a hierarchy separator in folder paths. Folder paths cannot start or end with a period, nor can they contain two periods in a row.
- ◆ Slash (/)—Reserved for the system.
- ◆ Plus (+)—Used to address subfolders of user Inboxes or shared folders that do not belong to a particular user.
- ◆ Asterisks (*), percent signs (%), and double quotes (") are limited by IMAP.

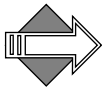


Mirapoint appliances support international (8-bit) folder names—folder names are stored internally using UTF-8 encoding. For example, the folder `user.gsantos.Español` appears on disk as:

```
spool/
  user/
    gsantos/
      espan\xCC\x831
```

Folder Access Control Lists

An access control list (ACL) allows you to specify who can see and use a folder. An ACL is a list of users you create along with the access permissions you're allowing for each. This enables you to control who has what access permissions on a folder. When a user account is created, an **Inbox** folder for them is automatically created and they are automatically granted “administrator” privileges (read/write/mail/Admin, see Table 27, “Access Control Permissions,” below, for explanations) for that folder. When you create a subfolder, it takes the same ACL as its parent folder; when you create a primary folder, it takes the system default ACL **anyone read**. You can use the **Add/Edit Folders** page to change those access permissions or grant another user (yourself, for example) permissions. You do this by looking up the user's folder on this page and modifying the ACL for the folder.



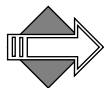
In all access permissions, the **anyone** user refers to all users of that system.

Table 27 describes what the access control permissions mean.

Table 27 Access Control Permissions

Field	Description
read	The user can see that the folder exists, open the folder, read messages in the folder, copy messages from the folder, and see which messages were read. (Equivalent to the l, r, and s IMAP permissions.)
write	The user can copy messages into the folder and modify state information for the folder, such as \Flagged, \Answered, and \Draft flags for each message. This permission allows the user to modify the \Deleted state for any message. (Equivalent to w, i, and d IMAP permissions.)
mail	The user can submit messages to the SMTP service for delivery to the folder. (Equivalent to the p IMAP permission.)
admin	The user can change the ACL on the folder and create subfolders and ACLs. (Equivalent to c and a IMAP permissions.)

Finding/Viewing Folders



The **Folders > Add/Edit Folders** page (see Figure 44 for an example) opens with the system folders displayed at the top-most level. The **user** folder contains all of the user account mail folders; click the **user** folder to expand the tree view to show all defined user folders.

To find and view a folder, either expand the tree hierarchy to expose the folder that you want to work on (click **Prev** and **Next**, **First** and **Last** as needed), or enter a folder name in the **Folder Name** option box and click **Search**. You can use these wildcards:

% (Percent sign): represents any character except period (.). Use the Percent sign to search for a specific folder name.

* (Asterisk) represents any character including period (.).

If **Search** is used: How many matching folders were found, and which of the folders in the found list is selected, is indicated next to the **Search** button in the tree view. For example, if you enter **newbie.sent** and there are seven folders that match, the indicator would look like this: (1/7)

meaning “The first of seven matches is selected.” If you click Next, the indicator changes to (2/7), and so on. Additionally, the tree view expands to show the found folder with the Selected icon ◀ and the Delete icon ✕ next to it. The Access Control List grid shows the current ACLs set on the folder.

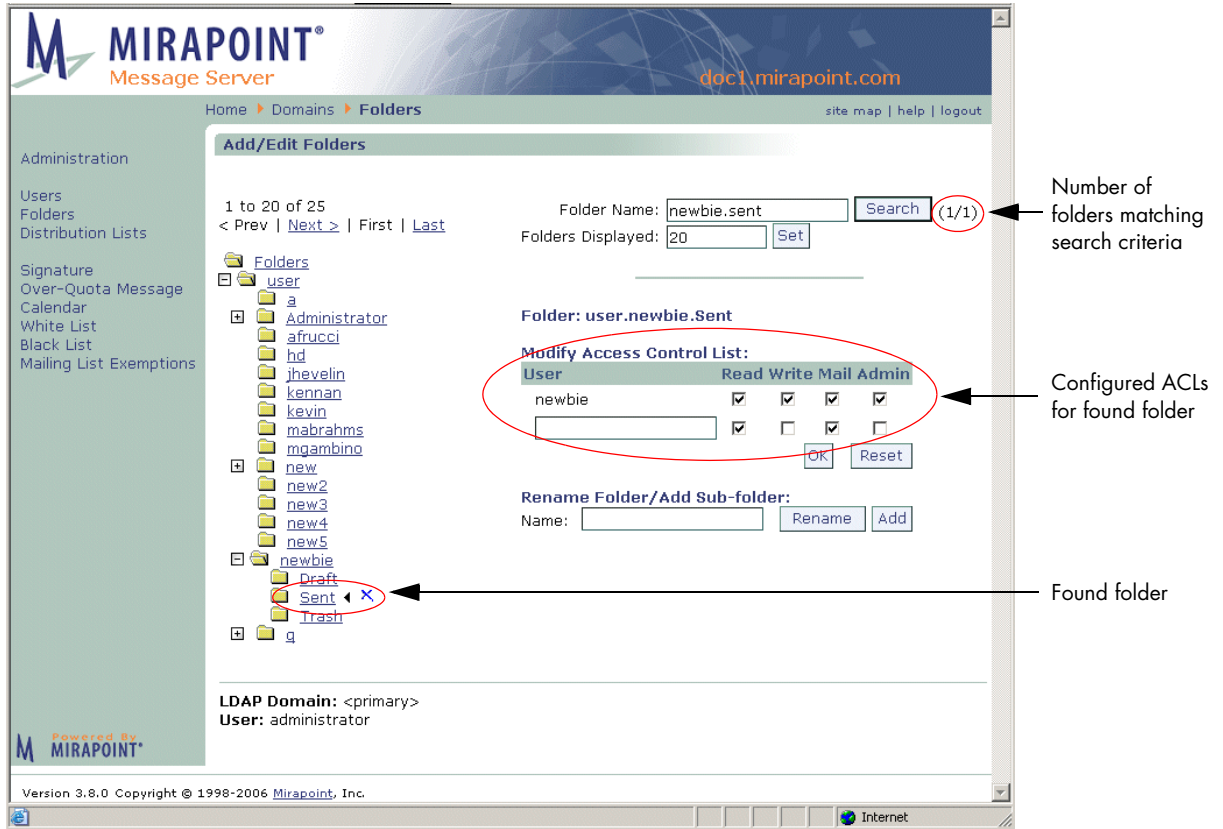




Figure 44 Mirapoint Folders Page—Find Folder Search Result

Adding Folders

Use the Add/Edit Folders page to add, rename, delete, or modify user folders, including the access control list for a folder. You can add top-level system folders that can be shared by users, or you can add sub-folders to existing user accounts. The Add/Edit Folders page opens with

the system folders displayed at the top-most level; see Figure 45 for an example. The **user** folder contains all of the user account mail folders.

To add a folder, enter a name in the **Rename Folder/Add Subfolder** option box and click **Add**; see [“Folder Naming Conventions” on page 300](#) for details. The new folder displays the **Selected** icon  and the **Delete** icon  that you can use to remove the folder.

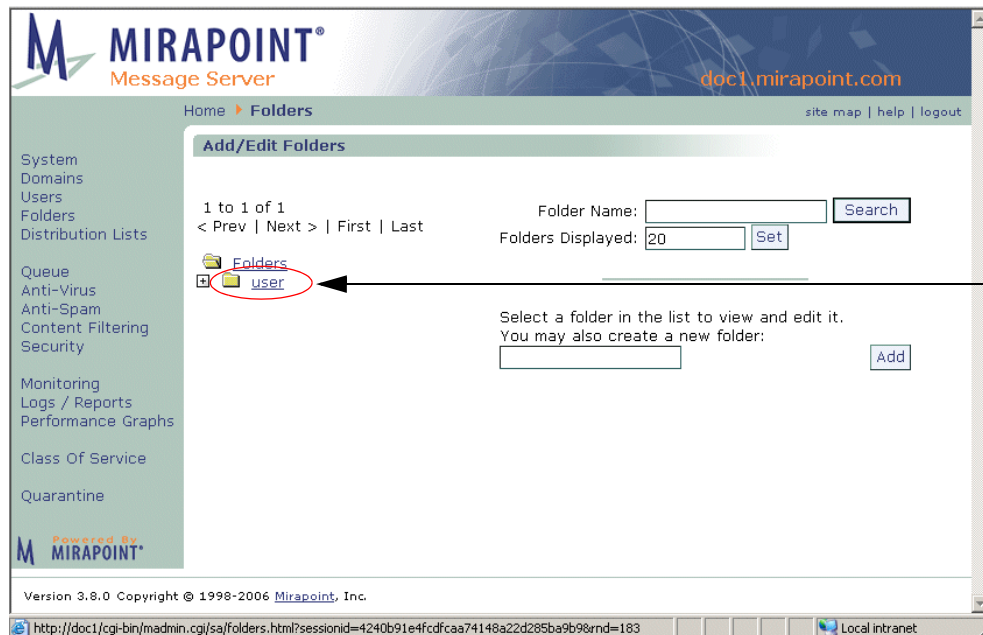
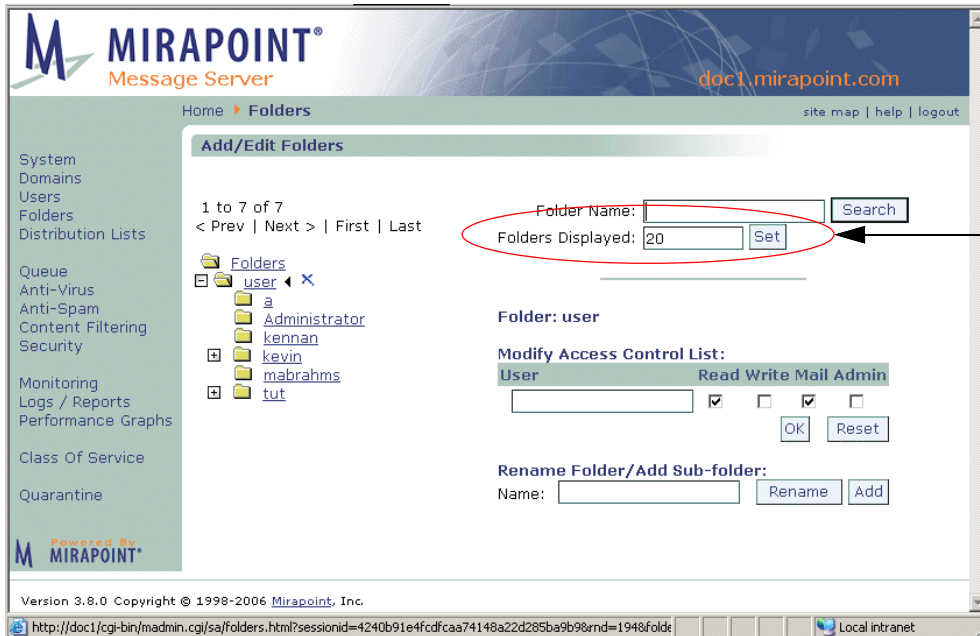


Figure 45 Mirapoint Folders Page—Collapsed View

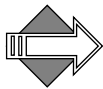


If you add a folder without selecting the **user** directory, it is added at the same level as the **user** directory. The folder will be addressable as part of the mail system as *+folder@domain*, but not associated with particular users. To make a top-level folder accessible to one or more users, you must set permissions on it. For more information about setting permissions, see [“Changing Folder Access Control” on page 305](#).



Select how many folders display on this page at a time here

Figure 46 Mirapoint Folders Page—Expanded View



A newly added user folder does not have the default folders (**Draft**, **Sent**, and **Trash**) until the user receives mail or logs in via WebMail/XML; at that time those folders are created automatically.

Changing Folder Access Control

If you want to share a folder you must change the permissions of that folder for the users you want to share it with, or for the “anyone” user that is the equivalent of all users on the system.

To receive mail addressed directly to a subfolder, you must set the **Write** permission on that folder.

To change the access control list for a folder:

1. On the **Add/Edit Folders** page, find the user's folder (described in [“Finding/Viewing Folders” on page 302](#)).

Result: The folder displays and the **Access Control List** grid shows the current ACLs set for the owner of that folder.

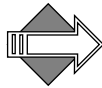
2. In the empty text field in the **Modify Access Control List** area, enter the login name for the user whose permissions you want to change on the selected folder; select or deselect checkboxes before clicking **OK** or after (click **OK** to enter changes). You must have at least one permission checkbox selected to display the user in the list.

Result: The user appears in the **User** list showing the permissions.

To undo the changes you just made, click **Undo**.

To return the ACL permissions to the original settings, click **Reset**—before you click **OK**.

You can remove someone from an access control list, no longer allowing them the ability to access your folders, by deselecting all of their checkboxes and clicking **OK**. You can change the Access Control permissions at any time to discontinue privileges you previously set.

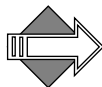


Keep in mind that when you create subfolders, they inherit the permissions set on their parent folders. For example, if you create a folder *archive.foo*, set some permissions on it, and then create a subfolder *archive.foo.bar*, the permissions set on *archive.foo* are copied to *archive.foo.bar*.

Changing a Folder Quota

You change the quota for a folder on the **Edit User** page by selecting the user that owns the folder and modifying their **Folder Quota**. Folder quotas apply to all folders and sub-folders combined.

For example, if a user's top-level "Inbox" folder has a quota of 100MB, that "Inbox" folder, plus all its subfolders, cannot exceed 100MB in content.



If a separate quota is specified for a sub-folder, that folder is immediately counted against the top-level folder quota. For example, the Trash folder is always assumed to need 1 MB of the top-level folder quota. If the top-level quota is 10MB, that means the Trash folder takes up 1 MB and all other folders can contain up to 9MB.

Renaming a Folder

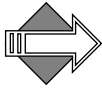
To rename a user folder follow these steps.

1. On the **Add/Edit Folders** page, find the user's folder (described in [“Finding/Viewing Folders” on page 302](#)).
Result: The folder displays and the **Access Control List** grid shows the current ACLs set for the owner of that folder.
2. Enter a name in the **Name** text box and click **Rename**.
Result: The folder is renamed as specified.

Adding a Sub-folder

To add a user sub-folder follow these steps.

1. On the **Add/Edit Folders** page, find the user's folder (described in [“Finding/Viewing Folders” on page 302](#)).
Result: The folder displays and the **Access Control List** grid shows the current ACLs set for the owner of that folder.
2. Enter a name in the **Name** text box and click **Add**.
Result: The folder is added as specified and appears in the tree view as selected.



Keep in mind that when you create subfolders, they inherit the permissions set on their parent folders. For example, if you create a folder *archive.foo*, set some permissions on it, and then create a subfolder *archive.foo.bar*, the permissions set on *archive.foo* are copied to *archive.foo.bar*.

Creating a Shared Folder

You can create a folder that can be shared by any or all users and accessed via WebMail, IMAP, or XML. This can be useful in group situations where you would like members of a group to be able to send mail to a common folder that all can access. to do this, follow these steps.

1. On the **Add/Edit Folder** page, click the **user** folder to open the tree and then add a new folder to be shared.

Result: The new folder displays as a subfolder of **user** and is selected.

2. In the Access Control List grid, enter “anyone” to share the folder with all users on the system, select the **Mail** privilege to allow users to send mail to the folder, and select the **Read** checkbox to allow users to access messages sent to the folder. To enable users to copy messages to the folder or delete messages, grant them the **Write** privilege. To enable users to create subfolders, grant them the **Admin** privilege. When you’re done modifying the access control list, click **OK**.

Result: The new folder is available for all users to send messages to and view.

3. Send a message to all appropriate users that you have created a shared folder; tell them the folder name and advise them to subscribe to the folder using their **Shared Folders** page. They must locate the folder on that page and then click the **Subscribe** option. Result: Once subscribed to, the shared folder displays and messages can be addressed to it. To view the messages, users must open the shared folder. To send messages to it, use the folder name; for example, if the shared folder name is “SharedPubs” then messages to it would be addressed:


+SharedPubs@example.com

Deleting a Folder

To delete a user folder follow these steps.

1. On the **Add/Edit Folders** page, find the user's folder (described in [“Finding/Viewing Folders” on page 302](#)).

Result: The folder displays and the **Access Control List** grid shows the current ACLs set for the owner of that folder.

2. Click the **Delete** icon  next to the selected folder. Result: A confirmation page displays.

3. Click **OK** or **Cancel**.

Result: If you click **OK**, the folder is deleted. If you click **Cancel** the delete operation is terminated and you are returned to the main **Add/Edit Folders** page. When you delete a folder, all email

messages, subfolders, and configuration data belonging to that folder are destroyed.

Note: To delete a folder, you must have admin privileges. To add admin privileges to a folder for all administrators, edit the folder's ACL and add an entry for **Administrators** and select the **admin** privilege.

Sending Messages to User Sub-Folders

For mail to be delivered directly to a subfolder in a user's Inbox, the following two conditions must be met:

- ◆ The wildcard user "anyone" for that folder must have the **Mail** access privilege.
- ◆ A plus (+) character must be included in front of the name of the subfolder in the **To** address line. For example, to send a message to the **help** subfolder of glenn's inbox, use this address:

`glenn+help@example.com`

Managing Messages

This section describes some of the message management options available to you as administrator.

Sending Messages to Folders

In addition to sending messages to user's inboxes, you can send messages directly to users' subfolders and other shared folders that are not associated with a particular user.

For mail to be delivered directly to a folder, the wildcard user "anyone" must have the **Mail** access privilege.

To send a message directly to a user's subfolder, you append a plus (+) character and the name of the subfolder to the user's inbox address. For example, to send a message to the **help** subfolder of glenn's inbox, use this address:

`glenn+help@example.com`

To send mail to a shared folder that is not associated with a user, preface the folder name with the plus (+) character. For example, to send a message to a shared mailbox named **bulletins**, use this address:

+bulletins@example.com

You can also send messages to a subfolder of a shared mailbox. In this case, a period (.) is used as a delimiter. For example, if **collectibles** is a subfolder of the shared **forsale** folder, you could address it like this:

+forsale.collectibles@company.com

Managing Distribution Lists

A **distribution list** (DL) is a named list of email addresses. When you send a message to a distribution list, the message is forwarded to all addresses on the list. You can create or delete DLs, and add addresses to (or remove them from) an existing DL using the **Distribution List** page in the Administration Suite.

Each entry in a distribution list can be the login name of a registered user, the name of another distribution list, a folder name (use the plus character (+) as in **+archive@example.com**), or any valid email address. For example, you might define a distribution list named **sales** that has the entries shown in Figure 47.

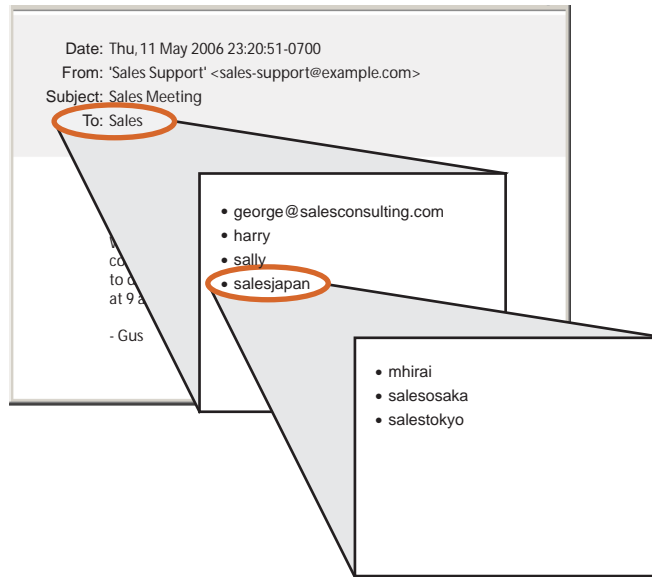


Figure 47 Example of Distribution List Named Sales

In Figure 47, `george@salesconsulting.com` is a remote address, `harry` and `sally` are registered users in the same domain as `sales-support@example.com`, and `salesjapan` is itself a distribution list that contains the entries `mhirai`, `salesosaka`, and `salestokyo`, where `mhirai` is a registered user and `salesosaka` and `salestokyo` are both distribution lists.

Distribution List Naming Conventions

DL names are composed of letters, numbers, minus (-), period (.), and underscore (_) characters. They are case-insensitive and limited to 64 characters. DLs are used to group users together into convenient mailing lists.

DLs can also be used as aliases for individual users. The DLs are processed before users. For example, if you have a user named `sallyr` and a DL named `sallyr` that contains `sallyr` and `+archive.sallyr@archive.foo.com`, messages sent to `sallyr` are delivered to both the archive folder and the user.

Each entry in a distribution list can be the login name of a registered user, the name of another distribution list, a folder name (use the plus sign (+) as in +archive@example.com), or any valid email address.

Reserved Distribution List Names

You cannot create DLs with the following reserved names:

- ◆ abuse
- ◆ backup-alerts
- ◆ backup-status
- ◆ daily-reports
- ◆ mailer-daemon
- ◆ nobody
- ◆ operator
- ◆ postmaster
- ◆ schedule-output
- ◆ system-alerts
- ◆ system* (cannot use “system” as the initial name in a DL)
- ◆ virus-alerts
- ◆ weekly-reports

For more information about the default distribution lists created during installation and used by the Mirapoint system, see [“Internal Distribution Lists for Monitoring” on page 201](#).

Adding and Populating Distribution Lists

A distribution list has no assigned members when it is first added. Once you've added the distribution list (DL), you then add users or other distribution lists as members by editing the DL.

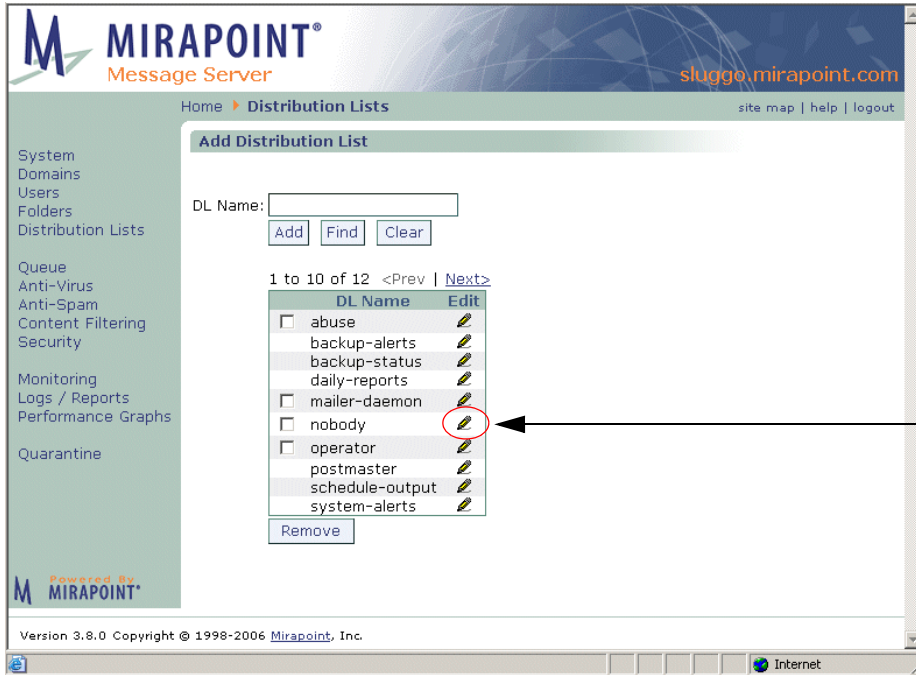
Adding a user's email address to a distribution list ensures that person receives any mail sent to that list. You can add local or LDAP users, remote users, or other distribution lists.

Use the **Distribution Lists** page to add, find, select to edit, or remove a DL; see Figure 48 for an example. All existing DLs display in a table on

the **Add Distribution List** page, ten per page. Click **Prev** and **Next** to page through the list.



To add a distribution list in a delegated domain, select the domain first.



Click a DL's Edit icon to add or remove members

Figure 48 Add Distribution List Page

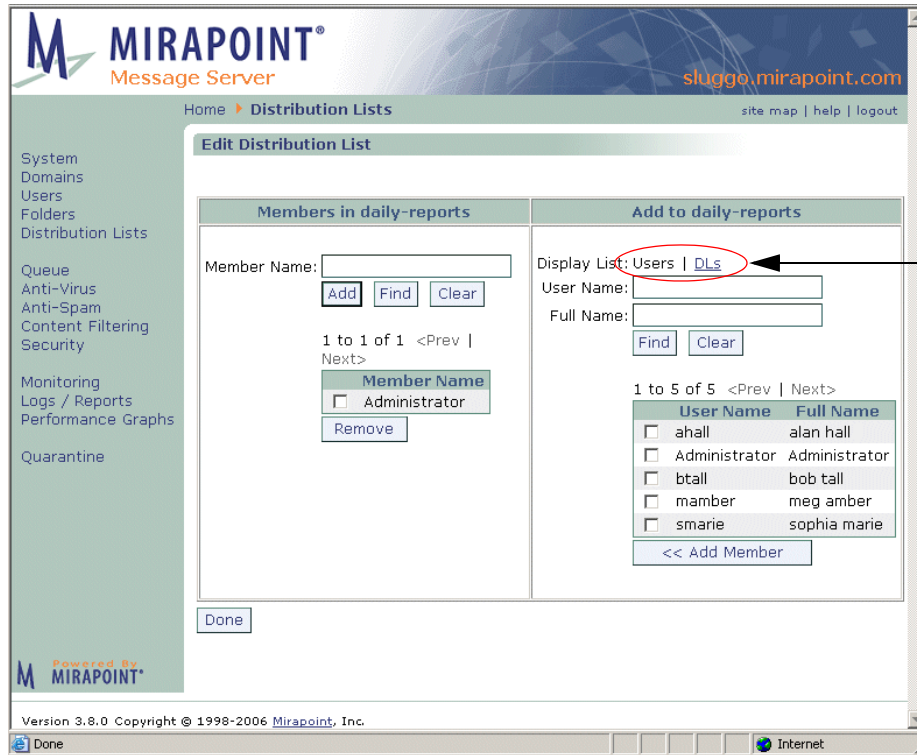



Figure 49 Edit Distribution List Page

To add and populate a distribution list, follow these steps.

1. On the **Add Distribution List** page, enter a name in the **DL Name** text box and click **Add**.
Result: The new distribution list is added to the DL list table. The DLs display in alphabetical order, so the new DL you add might not be on the first page; use **Prev** and **Next** to page through the list.
2. Click the **Edit** icon  for the new DL.
Result: The **Edit Distribution List** page (see Figure 49 for an example) for that DL displays.
3. Use the **Display List** options in the **Add to DL name** area to choose to display a list of configured users or configured DLs.
Result: If you click **DLs**, the list table below changes to display, ten

per page, all available DLs. If you click **Users** (default), the list table below displays all available users, ten per page.

4. Select from the list of available users or DLs in the **ADD to DL name** area; click **Prev** and **Next** to page through the list. When you find a user or DL that you want, select it and click **Add Member**.

To add a member manually, enter the user's name or email address in the **Member Name** text box in the **Members in DL name** area and click **Add**. (If the member is not a registered user of the domain, you must enter the member's complete email address.)

To find a user or DL so you can add it, enter the user or DL name in the **User/DL Name** text box in the **Add to DL name** area, and click **Find** to display only those users or DLs that match the entered text (you can use wildcards). Clicking **Clear** causes the text box to clear and the list to again display all available users or DLs, ten per page.

Result: If you click **Add Member** in the **Add to DL name** area, that user or DL is added to the DL. If you click **Add** in the **Members in DL name** area, that user or DL is added to the DL. **Note:** Once a user or DL is added to the DL, their name still displays in the **Add to DL name** area.

5. To remove a user from the DL, select their name in the list table and click **Remove**.

Result: The selected name disappears from the **Members** list.

6. When you are finished editing the DL, click **Done**.


Result: You are returned to the **Add Distribution List** page.

Finding Distribution Lists

To find an existing distribution list, on the **Add Distribution List** page (see Figure 48 for an example), enter a name in the **DL Name** text box and click **Find** to display only those distribution lists matching the entered name. You can use the asterisk (*) wildcard, for any kind of character including the folder hierarchy separator period (.), or the percent sign (%) wildcard, for any kind of character NOT including the folder hierarchy separator period (.). Click **Clear** to empty the options of any text that you have entered and re-display the entire DL list (ten names display per page).

Editing Distribution Lists

Use the **Edit Distribution List** page (see Figure 49 for an example) to add or remove users or distribution lists (DLs) to existing distribution lists. To edit a DL, follow these steps.

1. On the **Add Distribution List** page (see Figure 48 for an example), find the DL that you want to edit and click its **Edit** icon . **Note:** Non-deletable, system-created distribution lists do not have a checkbox by their name.
Result: The **Edit Distribution List** page (see Figure 49 for an example) for that DL displays.
2. Make changes to the members as needed, see [“Adding and Populating Distribution Lists” on page 312](#) for details. When you are finished, click **Done**.
Result: You are returned to the **Add Distribution List** page.

Deleting Distribution Lists

To remove a distribution list, follow these steps.

1. On the **Add Distribution List** page (see Figure 48 for an example), find the DL that you want to remove, select it and click **Remove**.
Note: Non-deletable, system-created distribution lists do not have a checkbox by their name and cannot be removed.
Result: A confirmation page displays.
2. Click **OK** or **Cancel**.
Result: If you click **OK**, the DL is deleted. If you click **Cancel** the delete operation is terminated and you are returned to the main **Add Distribution List** page.



This procedure deletes a distribution list whether or not it is empty. You do not receive a warning before the information is deleted, and you cannot recover the information if you change your mind.

Policy Tasks

This chapter describes how to manage policies for your domains and users. Policies control the features and limits (quotas, etc.) available to users. The following topics are included:

- ◆ [Managing Classes of Service](#): How to use the Class of Service pages. Classes of Service are a way to create a set of policies and apply that set to a domain or an individual user.
- ◆ [Managing Storage Policies](#): How to set up storage quotas on domains and user folders.
- ◆ [Managing Content Policies \(Domain Filters\)](#): How to set up content filters on a domain-wide basis.

Managing Classes of Service

Mirapoint appliances enable you to control service availability and mailbox settings by domain or user. To control access to a particular service, you need to enable Class of Service (COS) checking for that service—otherwise, all users can access the service (as long as the service is licensed and enabled).

A “Class of Service” (COS) is a logical grouping of COS-enabled services and limits that can be assigned to users on a domain or individual basis. Classes of service are defined by service managers and created by administrators using the **Class of Service** pages.

The COS mechanism can be used to make different levels of service available to your users. For example, the “Gold” COS service plan

might include all available services, while the “Silver” service plan might include a subset.

User and COS information are stored in your LDAP database. If COS checking is enabled for a service, LDAP lookups are used to determine whether or not to permit users to access that service.

If COS checking is *not* enabled for a service, all users on the system can access the service. (No LDAP lookup is done before granting access to the service.)

Class of Service Features and Configuration Options

COS must be initially configured using the command line interface (CLI); for details see [“Enabling COS” on page 321](#). The services displayed on the **Class of Service** page depend on what you have licensed and enabled (turned “ON”). For more information about these features, see the Features Overview section in the *Mirapoint Administrator’s Planning Guide*. If you enable all possible services, these are the choices displayed on the **Class of Service** page.

- ◆ **Anti-Spam:** WebMail antispam scanning (inbound only).
- ◆ **Anti-Virus:** WebMail antivirus scanning (inbound only).
- ◆ **Automatic Reply:** WebMail auto-reply feature.
- ◆ **Calendar:** WebCal Direct (Personal).
- ◆ **Enterprise UI:** WebMail/WebCal Corporate Edition.
- ◆ **Message Filters:** WebMail message filters feature.
- ◆ **Forwarding:** WebMail mail forwarding (vacation mail) feature.
- ◆ **External Mail:** WebMail External POP mail feature.
- ◆ **Group Calendar:** WebCal Direct (Group).
- ◆ **IMAP:** Message sending and receiving service.
- ◆ **Junkmail Manager (JMM)*:** Spam mail management function.
- ◆ **Message Expiration:** WebMail message automatic deletion.
- ◆ **Message Undelete:** Retrieve recently deleted messages feature.
- ◆ **POP:** Message sending and receiving service.
- ◆ **Quota for Mailbox:** Allows a quota to be set.

- ◆ **Sender Anti-Spam:** Outbound antispam scanning.
- ◆ **Sender Anti-Virus:** Outbound antivirus scanning.
- ◆ **SSL:** HTTPS secure connections.
- ◆ **WebMail:** WebMail Direct.

Some of these features require additional configuration:

- ◆ **Folder Quota:** The amount of disk space available for the user's message storage. Messages are rejected if the folder is over-quota. This is the only COS option that can be overridden on the LDAP Enabled User page.
- ◆ **Junk Mail Message Expire (Message Expiration configuration):** How long a message can remain in the user's **Junk Mail** folder before being expired and deleted.
- ◆ **Trash Message Expire (Message Expiration configuration):** How long a message can remain in the **Trash** mail folder before being expired and deleted.
- ◆ **JMM Message Expire (Junk Mail Manager configuration):** How long a message can remain in the JMM quarantine before being expired and deleted.
- ◆ **JMM Mailbox Quota (Junk Mail Manager configuration):** The amount of disk space available for the user's JMM quarantine folder. Messages are rejected if the folder is over-quota.
- ◆ **Message Undelete (Message Undelete configuration):** Provides a **deletedmessages** folder hierarchy where messages deleted from user folders (a two-step process) can be retrieved by an administrator. Some IMAP clients allow users to access the **deletedmessages** folder and retrieve messages themselves.
- ◆ **Anti-Spam Warning (Sender Anti-Spam configuration):** Places the word "Spam?" in the **Subject** line of messages that were ranked as spam (junkmail) by the anti-spam scanner.

Note that not all services should be COS enabled on every appliance. For example, **Sender Anti-spam** and **Sender Anti-virus** would only be enabled on a server acting as an Outbound Message Router. Similarly, many services only make sense on a server acting as a message store, and the Antivirus and Antispam services apply to appliances acting as MailHurdle message screeners or inbound message routers.

Click the Edit icon on the Class of Service page to open the COS LDAP Editor page

LDAP Class of Service Editor

COS Name:

1 to 2 of 2 <Prev | Next>

COS Name	Edit	Delete
pewter		
security		

LDAP enabled

Configuration for security

Mailbox Quota: KB

Junk Mail Message Expire: days

Trash Message Expire: days

Message Undelete: KB

Anti-Spam Warning: Place the word 'Spam' in subject

Services for security

Applied Services	Available Services
<input type="checkbox"/> Anti-Spam	<input type="checkbox"/> Calendar
<input type="checkbox"/> Anti-Virus	<input type="checkbox"/> Corporate Edition
<input type="checkbox"/> Automatic Reply	<input type="checkbox"/> Forwarding
<input type="checkbox"/> Message Filters	<input type="checkbox"/> External Mail
<input type="checkbox"/> IMAP	<input type="checkbox"/> Group Calendar
<input type="checkbox"/> Message Expiration*	<input type="checkbox"/> i-mode Mail
<input type="checkbox"/> Message Undelete*	<input type="checkbox"/> Quota for Mailbox
<input type="checkbox"/> POP	<input type="checkbox"/> WAP Calendar
<input type="checkbox"/> Sender Anti-Spam*	<input type="checkbox"/> WAP Mail
<input type="checkbox"/> Sender Anti-Virus	<input type="checkbox"/> Webmail
<input type="checkbox"/> SSL	<input type="button" value="Add Service"/>

* has configuration

LDAP enabled

Powered By MIRAPPOINT

Version 3.8.0 Copyright © 1998-2006 Mirapoint, Inc.

Additional options display for some features once selected

Services that require configuration are starred

Figure 50 Class of Service Edit Page

Enabling COS

The **Class of Service** page link only displays if you have COS enabled for your system. You do this through the CLI:

- ◆ Use the **Cos** command to enable each feature that you want to be able to assign to a COS.
- ◆ Use the **Conf** command to display the **Class of Service** pages.

For more information about enabling COS, see the CLI **Help About Cos** and **Help About Conf**).


With the Class of Service pages, you can create classes of service; however, you must have LDAP provisioning configured to assign the classes of service that you create to users and/or domains.

With LDAP provisioning enabled, the **User** and **Domain** pages display the **LDAP Enabled** flag at the bottom of the page (see [“Setting Up a User Directory Service” on page 80](#) for details) and enable you to write values to your LDAP database.

Adding and Populating a Class of Service

The **Class of Service** page (see Figure 50 for an example) allows you to configure classes of service that can then be granted to domains or users through the **LDAP Enabled Domains** or **Users** pages.

To add and populate a Class of Service follow these steps on the **COS Editor** page(s); see Figure 50 for an example.

1. Enter a **COS Name** on the **Class of Service** page and click **Add**.
Result: The name of the new COS appears in the **Class of Service** list. That COS option appears on the **Domains** and **Users** pages.
2. To configure the new COS, click its **Edit** icon .
Result: The **COS Editor** page opens. Initially, all available services display in a table to the right.
3. Select the features that you want to make available to users of this Class of Service. Choose from the features that you have enabled; see [“Class of Service Features and Configuration Options” on page 318](#) for details. Click **Add Service** to add an available service;

click **Remove Service** to remove a service. Services that require configuration are starred (*); see Figure 50 for an example.

Note: The COS is added to your directory server LDAP database. Services that aren't available on this machine can be added to the COS as long as they are licensed and enabled on the directory server.

Result: The selected services are added to the Class of Service and displayed in a table. COS configuration options are shown at the top of the page.

4. Depending on which services you elected to add to the new COS, you might have to enter configuration data; see [“Class of Service Features and Configuration Options” on page 318](#) for details. Click **Apply**

Result: The conditions for the COS are entered into the system.

5. When you are finished, click **Done**.
Result: You are returned to the **Add/Edit/Find COS** page.

You can now go to the **Users** or **Domains** page and assign them COS; see “Assigning Classes of Service” next, for details.

Assigning Classes of Service

If you assign a COS to a domain or user, only those services included in the COS are available to them. For example, if the COS does not include **Forwarding**, then that option does not display when they access WebMail. Assigning a COS to a particular user overrides the COS assigned to the domain the user belongs to. If no COS is assigned to the user or the user's domain, the defaultCOS is used.

You assign a defined COS to a domain on the LDAP Enabled **Domains > Administration** page. Once assigned, the COS values are used at next login for all users in that domain.

You assign a defined COS to an individual user on the LDAP Enabled **Users** or **Domains > Users** page. Once assigned, the COS values are used at next login.

One COS value, **Folder Quota**, can be modified on the LDAP Enabled **Add User** page. This provides a way to override the folder quota for

selected users. All other COS services and values can only be overridden by manually changing a user's LDAP "miservice" record.

Finding Classes of Service

To find a configured COS, on the **LDAP Class of Service Editor** page, enter a name in the **COS Name** text box and click **Find** to display only those classes of service matching the entered name. You can use the question mark (?) wildcard, for any single character, or asterisk (*) wildcard, for any kind of character. Click **Clear** to empty the options of any text that you have entered and re-display the entire COS list (ten names display per page).

Using Patterns

Several tasks require you to specify a **pattern** for user, folder, or other names. Patterns are case-insensitive except where otherwise noted and can contain these wildcard characters:


- ◆ Question mark (?) (non-folder names only): Matches any single character. For compatibility with the IMAP4 protocol, question mark (?) is not interpreted as a wildcard in folder names.
- ◆ Asterisk (*): Matches zero or more characters of any kind. For folders, this includes the folder hierarchy separator period (.).
- ◆ Percent sign (%) (folder names only): Matches zero or more characters, not including folder hierarchy separators. This wildcard is provided for compatibility with the IMAP4 protocol—it is interpreted as a wildcard only in folder names.

In the example given below, the pattern **ann?**, used to find a user, would match the former names and the pattern **jo***, used to find a folder, would match the latter folders:

```
anna anne  
jo joe john jon jon.bulk jon.personal
```


Editing Classes of Service

To edit a class of service, follow these steps on the COS page.

1. Find the COS that you want to change and click its **Edit** icon .
Result: The **COS Editor** page opens, see Figure 50.
2. Make your changes, adding or removing features; when you are finished, click **Done**. Click **Apply** before clicking **Done**.
Result: Your changes are applied to all users of that COS at next login.

Deleting Classes of Service

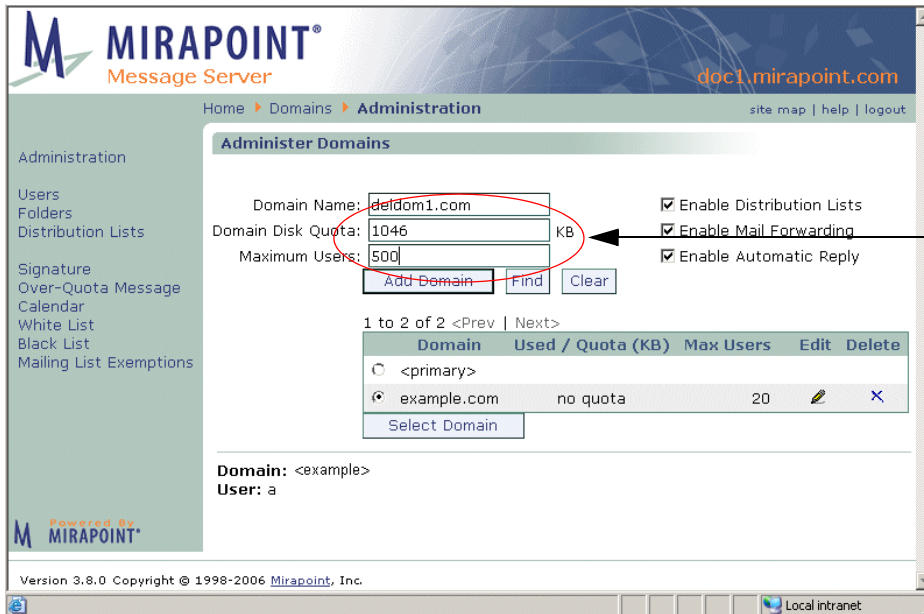
To delete a class of service, follow these steps on the COS page.

1. On the **COS Editor** page, click the **Delete** icon  of the Class of Service you want to delete. Click **Prev** and **Next** to page through the list of names, as needed.
Result: A confirmation page displays.
2. Click **OK** or **Cancel**.
Result: If you click **OK**, the selected Class of Service disappears from the **Class of Service** list. If you click **Cancel**, the Class of Service is not deleted. Both options return you to the **COS Editor** page. Users and domains assigned the COS revert back to the default services and values assigned that domain or user at next login.

Managing Storage Policies

Storage polices (quotas) let you control how much disk space a domain can use, how many users can be created for a domain, and how much folder space individual users can use. Additionally, you can set up a special “Deleted Messages” folder that allows users to retrieve mail they have deleted (for a period of time); and “Message Expiration” that determines how long messages can be stored before being automatically deleted. These features can be included in a Class of Service and

assigned to domains or individual users; **Message Undelete** and **Message Expiration** can only be implemented through COS.



Set a size limit for a domain and a user limit here

Figure 51 Domains > Administer Domains Page, Domain Quotas

Administration

- Users
- Folders
- Distribution Lists
- Signature
- Over-Quota Message
- Calendar
- White List
- Black List
- Mailing List Exemptions

Home > Domains > Users

doc1.mirapoint.com

site map | help | logout

Add User

User Name: Role: A = Administrator
 Q = Quarantine administrator
 H = Helpdesk administrator
 B = Backup operator

Full Name:

Password:

Confirm Password:

Folder Quota: KB

Alias(es): More >>

Class of Service: Find Clear

1 to 3 of 3 <Prev

User Name	Role	COS	Used / Quota (KB)	Edit	Delete
a	a	A	no quota		
Administrator	Administrator	A,H,B	no quota		
mabrahms	mabrahms		no quota		

LDAP Domain: <primary>
 User: administrator
 LDAP enabled

Remove a user quota by entering -1.

Choose from configured COS

Figure 52 Mirapoint Add User Page, Quota and COS Included

Creating Storage Policies

If you are using classes of service, consider which COS should have storage policies and which policies you want to apply. The storage policy features available to you through the COS pages, with all LDAP COS enabled are:

- ◆ **Message Expiration:** WebMail automatic message deletion. Selecting this COS feature requires the specification of **Trash Message Expire** (when the user's **Trash** mail is deleted).
- ◆ **Message Undelete:** Retrieve recently deleted messages feature. Selecting this feature requires the specification of a **deletedmessages** folder where messages deleted from user folders can be retrieved by an administrator. Note: Some IMAP clients allow users to access the **deletedmessages** folder and retrieve messages themselves.
- ◆ **Quota for Mailbox:** Allows a quota to be set on user folders.

- ◆ **Junk Mail Message Expire (Message Expiration configuration):** How long a message can remain in the user's **Junk Mail** folder before being expired and deleted.

Additionally, if you select Junk Mail Manager as a COS feature, you can set these storage quotas:

- ◆ **JMM Message Expire (Junk Mail Manager configuration):** How long a message can remain in the JMM quarantine before being expired and deleted.
- ◆ **JMM Mailbox Quota (Junk Mail Manager configuration):** The amount of disk space available for the user's JMM quarantine folder. Messages are rejected if the folder is over-quota.

Setting Up Message Undelete

The Message Undelete service enables users and administrators to recover messages that have been deleted by mistake. When this service is enabled, deleted messages are moved to a Deleted Messages folder.

If a deleted message is larger than the undelete quota, it is temporarily allowed in the Deleted Messages folder. For example, if a user deletes a 20 MB message but only has a 10 MB **Message Undelete** quota, all messages except the 20 MB message are removed from the Deleted Messages folder. The next time the user deletes a message, regardless of size, the 20MB message is removed from the Deleted Messages folder.

If recovering messages from the deleted messages folder would cause the user to exceed their mail quota, no messages are undeleted.

Messages in the **Deleted Messages** folder cannot be read, only restored to their previous folder. If a WebMail user has set the **Delete to Trash** preference, undeleted messages are restored to their **Trash** folder, not the folders from which they were originally deleted.

You must use the command line interface (CLI) and the Administration Suite to set up Message Undelete. To access the CLI, telnet to your Message Server on the default telnet port (port 23) and log in as the Administrator:

```
User: telnet hostname.domain.com
OK hostname.domain.com admind 3.8 server ready
User: Administrator
```

```
Password: password
OK User logged in
```

To make this service available to all users, you can run the **Mailbox Set Undeletequota** command from the command line. For example:

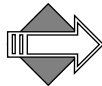
```
Mailbox Set Undeletequota 10485760
```

To make this service available to selected domains or users, you need to COS-enable the **Msgundelete** service:

```
Cos Enable Msgundelete
```

Now, use the Administration Suite pages to complete the set up:

1. Go to the **LDAP Class of Service Editor** page and click the **Edit** button for the COS to which you want to add the undelete service.
2. Select the **Message Undelete** service in the Available Services list and click **Add Service** to add it to the COS.
3. Specify the mail undelete quota in KB and click the **Apply** button.



The IMAP client in Netscape Messenger allows users to subscribe to the **/deletedmessages** hierarchy, where they can find their deleted folder. However with the IMAP client in Outlook and Outlook Express, the Mirapoint system must run UW namespace for proper functioning of **Saved** and **Sent** folders combined with access to the **/deletedmessages** hierarchy. Note that namespace (Cyrus or UW) is box-wide, applies to IMAP only, and can be switched at any time, although switching may cause disruption to the user community.

Setting Up Message Expiration

The Message Expiration facility enables old messages to be deleted automatically once they've reached a certain age.

You must use the command line interface (CLI) and the Administration Suite to set up Message Expiration. To access the CLI, telnet to your Message Server on the default telnet port (port 23) and log in as the Administrator:

```
User: telnet hostname.domain.com
OK hostname.domain.com admind 3.8 server ready
User: Administrator
```


Password: **password**
OK User logged in

To make this service available to selected domains or users, you need to COS-enable the **Msgexpiration** service:

Cos Enable Msgexpiration

Now, use the Administration Suite pages to complete the set up:

1. Go to the **LDAP Class of Service Editor** page and click the **Edit** button for the COS to which you want to add the message expiration service.
2. Select the **Message Expiration** service in the Available Services list and click **Add Service** to add it to the COS.
3. Configure the message expiration policy by setting the **Junk Mail Message Expire**, **Trash Message Expire**, and **JMM Message Expire** options. These options let you specify how many days to keep messages before they can be automatically deleted from the specified folder.
4. When you're done, click the **Apply** button to save your changes.

Editing Storage Policies

Storage policies can reside in a Class of Service, or they can be assigned directly to a domain or user; either through LDAP records or local records. An assigned COS overrides any changes you make on the **Domains** or **Users** pages.

Editing COS Storage Policies

To change storage policies on a COS basis, use the **COS Editor** page for the class of service that you want to modify. Make your changes and click **Apply** and then **Done**. Your changes take place for all domains and users assigned that COS at next log in.


Editing Domain Storage Policies

To change storage policies on a domain basis, follow these steps.

1. On the **Domains > Administration** page, select the domain whose storage quotas you want to change.
Result: That domain becomes “selected,” additional options display in the left page menu, and the domain name displays at the bottom left corner of the page.
2. Change the **Domain Disk Quota** or **Maximum Users** amount and click **OK**.
Result: Your changes take place for all users in that domain at next log in. Note: An assigned COS overrides any changes you make here; instead, change the values to the COS directly.

Editing User Storage Policies

To change storage policies on a per-user basis, follow these steps.

1. On the **Add User** page, find and select the user whose quota(s) you want to change click his or her **Edit** icon . For a user in a delegated domain, select the delegated domain first on the **Domains > Administration** page and then use the **Domains > User** page to select that user to edit.
Result: The **Edit User** page for that user displays
2. Change the **Folder Quota** (the allocated space for all of a single user’s folders) for that user and click **OK**.
Result: The changes take place for that user at next log in. Note: An assigned COS overrides any changes you make here; instead, change the values to the COS directly.

Deleting Storage Policies

Storage policies can reside in a Class of Service, or they can be assigned directly to a domain or user; either through LDAP records or local

records. An assigned COS overrides any changes you make on the **Domains** or **Users** pages.

Deleting COS Storage Policies

To delete storage policies on a COS basis, use the **COS Editor** page for the class of service that you want to modify. Remove the **Mailbox Quota** by entering -1 (minus one); you can remove the **Junk Mail Message Expire** and **Trash Message Expire** time limits by entering 0 (zero). Click **Apply** and then **Done**. Your changes take place for all domains and users assigned that COS at next log in.


Deleting Domain Storage Policies

To delete storage policies on a domain basis, follow these steps.

1. On the **Domains > Administration** page, select the domain whose storage quotas you want to delete.
Result: That domain becomes “selected,” extra options display in the left page menu, and the domain name displays at the bottom left corner of the page.
2. Remove the **Domain Disk Quota** or **Maximum Users** amount and click **OK**.
Result: Your changes take place for all users in that domain at next log in.

Deleting User Storage Policies

To delete storage policies on a per-user basis, follow these steps.

1. On the **Add User** page, find and select the user whose quota(s) you want to change click his or her **Edit** icon . For a user in a delegated domain, select the delegated domain first on the **Domains > Administration** page and then use the **Domains > User** page to select that user to edit.
Result: The **Edit User** page for that user displays
2. Remove the **Folder Quota** for that user by entering -1 (minus one) and click **OK**.
Result: The changes take place for that user at next log in.

Managing Content Policies (Domain Filters)

A content policy is a set of rules for what content is allowed to whom. You set content policies on a domain-level basis, you implement content policies through message filters. A message filter is a method of identifying a message and specifying an action for that message. Message filters provide the ability to finely control your mail flow. Administrators can set up domain wide message filters; domain filters are acted on before personal filters.

To establish a content policy for a domain, first consider the message contents typical of the users of that domain and what restrictions you want to apply. You can set up message filters to increase (or decrease) spam sensitivity; delete, reject, or forward certain messages; quarantine certain messages to a folder for examination and possible release back to the mail stream; or remove attachments from certain messages.

Content Filtering Options

There are many options to choose from when creating a filter; this section describes options that you should understand beforehand. The step-by-step procedure is given in [“Creating a Message Filter” on page 339](#).

About the Destination Domain Options

Unless you log in as a delegated domain administrator, or specifically select a domain to administer, or are administering a Junk Mail Manager domain, the option to choose a **Destination Domain** displays for all content filters.

A screenshot of a user interface showing the 'Destination Domain' options for a filter. The text is enclosed in a rectangular box. It lists three options: 'Primary', 'Any', and 'Local', each with a vertical bar to its right. 'Non-local' is also listed with a vertical bar to its right. Below this list, there is a line of text: 'Primary: Applies to the primary domain only'.

Destination Domain: Primary | Any | Local | Non-local
Primary: Applies to the primary domain only

Figure 53 Destination Domain Filter Options

The **Destination Domain** options (see Figure 53 for an example) allow you to specify certain pools of recipient addresses to which the filter applies. The options are:

- ◆ **Primary:** Only filter messages addressed to users on the primary mail domain of the machine on which the filter is created.
- ◆ **Any:** Filter any messages routed to or through the machine on which the filter is created.
- ◆ **Local:** Only filter messages addressed to users (in all domains) on the machine on which the filter is created.
- ◆ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created (the reverse of **Local**).

The order in which these filters are executed is as follows:

- ◆ The **Any** domain filter is always executed before other domain filters; the **Primary** domain filter is executed next.
- ◆ If the message is local (inbound), then **Local** and **Primary** domain filters are executed, in that order, after the **Any** domain filters.
- ◆ If the message is non-local (outbound), then only **Nonlocal** domain filters are executed, after the **Any** domain filters.
- ◆ After the above are executed, delegated domain filters and, then, user filters are executed.

About Filter Priorities and Ordering

Filters you create are assigned one of three priorities: 100, 450, or 500. If you select the **Advanced** filter option, **Filter this message before performing Anti-Virus and Anti-Spam scanning**, that filter is a priority 100 filter. If you do NOT select that option, but do select the **Send to Quarantine folder** option, that filter is a priority 450 filter. By default, filters that you create on the **Content Filtering > Advanced** page, with an action other than quarantine, are processed after antivirus and antispam scanning and are priority 500 filters. Filters are executed in the following priority order:

- 100 (High Priority) filters **Any/Primary** destination domain
- 100 (High Priority) filters **Local/Nonlocal** destination domain

100 (High Priority) delegated domain filters
antivirus scanning
antispam scanning
450 Filters **Any/Primary** destination domain
450 Filters **Local/Nonlocal** destination domain
450 Filters delegated domain filters
500 Filters **Any/Primary** destination domain
500 Filters **Local/Nonlocal** destination domain
500 Filters delegated domain filters

Each domain or folder (user account) can have multiple filters, which are evaluated for each incoming message in the order the filters were created. The default order of operations among content filters is:

antivirus scanning
antispam scanning
domain signatures
domain filters (including primary domain)
end-user filters

Filters are executed in the order indicated on the **Content Filtering > Advanced** page. You can re-order the list to change the processing order.

About MIME and Filtering Attachments

“MIME” stands for Multipurpose Internet Mail Extension; a standard for multipart, multimedia electronic mail messages. MIME standards treat the body of a message as a series of one or more body parts. Each of these parts includes type information (a **Content-Type** field), some also include encoding information (a **Content-Transfer-Encoding** field) and suggestions to the recipient as to how to deal with that part (a **Content-Disposition** field). All MIME parts of a message are considered attachments and filtered if the **Attachment MIME Type** parameter is specified in the message filter.

A normal message with no attachments typically has a **Content-Type** of **text/plain**, its entire body is considered a single text/plain “attachment.” A message with one body part that is just text and another that contains a GIF graphic file, for example, would have the type **multipart/mixed**; the first part would be type **text/plain**, and the

last part **image/gif**. The **image/gif** part would be encoded in the MIME-defined scheme BASE64, and probably have a **Content-Disposition** field that suggests a file name for saving the part on a hard disk or diskette.

You can discover the MIME content-types used in a message by viewing the full message; do this in WebMail by clicking **Open** (Standard Edition), or **Open** and then **Source** (Corporate Edition), when viewing a message.

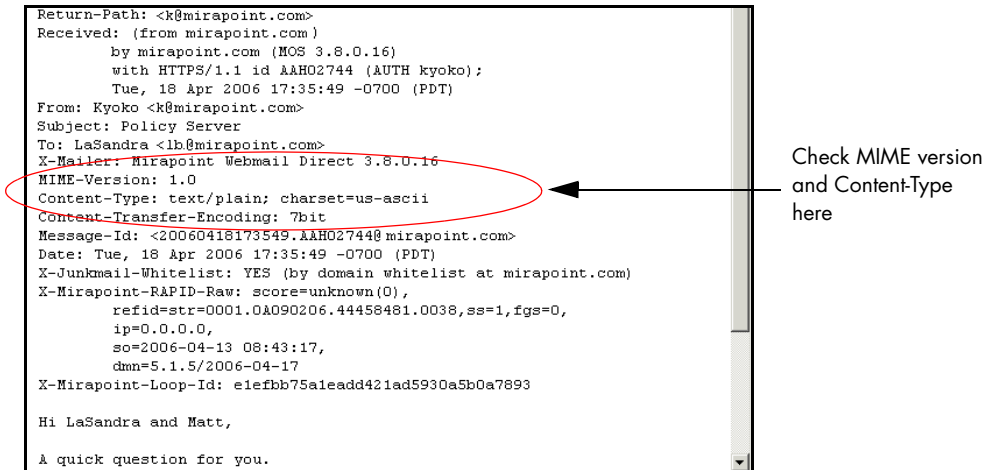


Figure 54 Example Message Source, MIME Type Indicated

Common Virus Attachment Names

The following is a list of file extensions that often have viruses in them. “File extension” refers to the letters after the period in a file name (i.e. the file **word.doc** has the file extension of **.doc**). **Note:** Not all viruses have these extensions; this is just a list of common types.

- .scr
- .vbs
- .pif
- .hta
- .reg
- .bat



Microsoft publishes a list of attachments that they recommend you block at:

<http://office.microsoft.com/en-us/assistance/HA011402971033.aspx>

About the Antispam Scanning Rules and Threshold

The antispam scanner uses one of two mutually exclusive techniques to categorize mail as junkmail (spam): **Principal Edition** or **Signature Edition**. Which antispam scanner you use depends on which licenses you have applied. The **Principal Edition** license is separate from the **Signature Edition** license and both cannot be applied simultaneously.

Antispam scanning **Principal Edition** uses several carefully compiled rule files based on common known factors of junkmail. The more rule matches, the higher the UCE score; a score over 50 classifies the mail as junkmail; this is known as the “antispam scanning threshold.” You can adjust this threshold on the **Anti-Spam > Configuration** page.

Antispam scanning **Signature Edition** uses an entirely different technique of scanning Internet traffic and detecting patterns to create a database of email “signatures” against which incoming email is compared and scored. A UCE score between 35 and 45 is marked “Suspect,” in the SDRAW message header; such mail is not classified as spam. A score between 50 and 60 is marked “Bulk” in the SDRAW header and is classified as spam. A score of 300 is marked as “Spam” and classified as spam. The **Signature Edition** scoring model is non-contiguous (spam mail is not scored between 61 and 299, it is either 50-60 or 300). These score cut-off points are referred to as “cliffs.”

For each rule in the rule file, or each signature “cliff,” that a scanned message matches, the message is awarded a **UCE score**. This score can be adjusted in a message filter. Careful study has determined that the default **Threshold**, UCE score = 50, is optimal for both scanners. Setting the spam **Threshold** below 50 causes more messages to be identified as spam, resulting in more false positives (messages wrongly identified as spam). Setting the **Threshold** above 50 causes fewer messages to be identified as spam, resulting in more false negatives (missed spam). You can set the threshold to any number between 1 and 300 for experimentation.



If you use RAPID anti-spam (signature edition), add an **Any** filter that discards messages that score above 299. For Principal edition, we recommend that you direct messages to the Junk Mail or JMM folder rather than discarding them so that users can retrieve false positives.

Understanding Quarantine Management

Currently there are two basic types of quarantines:

- ◆ **Quarantine that allows release:** This type of quarantining is done by the content filters and the RAPID antivirus engine. The **Quarantine Administrator** user role is required for the filter **Send to Quarantine folder** address, or **RAPID Quarantine folder** address, used so that these messages can be delivered back to the mail stream after examination and/or, in the case of the RAPID antivirus, re-scanned by one of the signature based antivirus engines.
- ◆ **Quarantine that does not allow release:** This type of quarantining applies to messages determined to have live viruses by one of the signature-based antivirus engines. For virus-infected messages, you can use the E-mail address antivirus configuration forwarding option to send those messages to a machine where they can be examined, if desired; you would not want to ever release these messages back to the mail stream.

How the Content Filtering Quarantine Works

The **Send to Quarantine folder** filter action is available for all content filters. **Send to Quarantine folder** generates a new message from **Administrator@hostname** that contains the original message and sends it to the specified quarantine address.

The quarantine address can be any WebMail user account that has the role of **Quarantine Administrator**. The quarantine administrator monitors the quarantine folder and determines what to do with quarantined messages. If a message is released back to the mail queue through the **Deliver** button, only the original message is delivered.



When using the **Send to Quarantine folder** filter action to filter all mail to or from a particular user, use the **To (message envelope)** or **From (message envelope)** options so that mail sent to that user from a

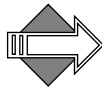
distribution or mailing list is filtered. See “Creating a Message Filter” on page 339 for more information about setting filter options.

Note that the content filtering quarantine is separate from the antivirus and JMM quarantines. For information on the Anti-Virus quarantine, see “How Antivirus Quarantine Works” on page 398”. For information on the Junk Mail Manager quarantine, see “How Junk Mail Manager Quarantine Works” on page 445”.

About Domain Filtering to a Quarantine Folder

Any of the content filters can be set to quarantine messages to a folder where a delegated domain Quarantine Administrator can view them and, if desired, release them back to the mail stream.

To create a filter for a delegated domain, be sure to select the domain on the **Domains > Administration** page and then use the **Domains > Message Filters** page. That page works in an identical manner to the top-level **Content Filtering > Advanced Content Filters** page except that there is no **Destination Domain** option; the domain is the current selected delegated domain.



If you use the **Send to Quarantine Folder** option for a domain-level filter, be sure to enter the address of a Quarantine Administrator for that delegated domain.

Monitoring a Quarantine Folder

Different Quarantine Administrators have different needs for monitoring their quarantine folders. To handle messages quarantined by content filters or the RAPID antivirus engine, a quarantine administrator should check the quarantine folder several times a day.

Messages quarantined by one of the signature-based antivirus engines contain live viruses and should not be released back to the message stream. The quarantine is intended for administrative investigation and does not require frequent monitoring.

Releasing Messages From Quarantine

When a Quarantine Administrator logs in to WebMail, there are two additional command buttons in the toolbar: **Deliver** and **Rescan**.

For messages quarantined by a content filter, you can use the **Deliver** button to release selected messages back to the mail stream. Released messages are delivered with no indication that they were quarantined.

Messages quarantined by the RAPID antivirus scanner should be re-scanned by one of the signature based engines by using the **Rescan** button once enough time has elapsed for the virus definitions to be updated, especially if the messages have a low score (50-60). Virus infected messages are acted on as configured by the antivirus engine; clean messages are delivered to the specified recipients. Automatic release of RAPID-quarantined messages occurs eight hours after quarantining, by default. This can be changed using the CLI.

Creating a Message Filter

Use the **Content Filtering > Advanced** pages or, for a delegated domain, the **Domains > Message Filters** pages (you must select a delegated domain for the **Message Filters** link to display) to create domain level content filters. See Figure 55 and Figure 56 for examples.

The screenshot shows the 'Advanced Content Filters' page in the Mirapoint Message Server. The 'Destination Domain' dropdown is set to 'Primary'. Below it, there is an 'Add Filter' button. A table lists the following filters:

Order	Domain Message Filters	Edit	Delete
1	Perform Anti-Virus and Anti-Spam scanning		
2	Blocked Addresses filter		
3	Unnamed Rule 0 contains tokens that can be edited only using the command line interface.		
4	Blocked Attachments filter		

Annotations on the right side of the screenshot indicate: 'Select the filter scope here' pointing to the 'Destination Domain' dropdown, and 'To add a new filter, click here' pointing to the 'Add Filter' button.

Figure 55 Advanced Content Filters Page, Add Filter

MIRAPPOINT®
Message Server
doc1.mirapoint.com

Home > Content Filtering > Advanced site map | help | logout

Add/Edit Advanced Content Filter

Filter Conditions - Add New Filter

Filter Name: NoDI-AllMail

Select the conditions for your filter:

If all of these conditions are met: More >>

To/CC: [] contains [] dl-all

From: [] does not match [] @*.mirapoint.com

Note:

- To remove a condition, select "-- Choose Type --" in the Filter Type box and click OK.
- To match all alpha-numeric characters, leave the Value box blank.

Apply to all messages

Filter Actions

Take the following action when conditions are met:

Keep (process normally)

Forward to: []

Forward excerpt to: []

Send to Quarantine folder: [] user.UserName[.Folder.Folder....]

Note: UserName must have quarantine administrator role.

Reject (refuse message and return it to the sender)

Discard (message is irrevocably lost)

Modify UCE (Junkmail) score by: [] (-1000 to 1000)

Remove attachments that meet attachment conditions

Do not apply any more filters to this message if action is taken

Filter this message before performing Anti-Virus and Anti-Spam scanning

OK Cancel

Version 3.8.0 Copyright © 1998-2006 Mirapoint, Inc.

To add more conditions to the filter, click here

Figure 56 Add/Edit Advanced Content Filter Page

To create a message filter follow these steps.

1. On the **Add Advanced Filter** page (see Figure 55), in the **Destination Domain** area specify the scope for the filter you are creating. **Note:** If you select a domain before coming to this page or if you log in as

a domain administrator, or if this is for a Junk Mail Manager domain, these options do not display.

- ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
- ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
- ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
- ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.

Result: The filter looks only at mail addressed to the selected user group. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. Click **Add Filter**.

Result: The **Add/Edit Filter** page displays (see Figure 56).

3. On the **Add/Edit Filter** page, in the **Filter Conditions - Add New Filter** area specify a **Filter Name**, and target condition; use the **More>>** button to display another row of condition options; select one:

- ❖ **If all of these conditions are met:** Filter action is done only if all of the specified conditions are true.
- ❖ **If any of these conditions are met:** Filter action is done if at least one of the specified conditions is true.

For either of these selections, proceed next to Step 4.

Alternatively, you can select the last radio button:

- ❖ **Apply to all messages:** Filter action is done on all your mail regardless of the conditions. This option is useful as a final filter in a series of filters to direct all other mail to be acted on.

If this is your selection, proceed next to Step 7.

4. Choose a filter type; this is the part of the message that the filter scans. What filter type you select determines what value you must enter (text, special characters, or integers):

- ❖ **From:** The sender line.
- ❖ **To/CC:** The recipient's lines (does not include BCC recipients, you cannot filter on the BCC field).
- ❖ **Subject:** The subject line.
- ❖ **Body:** The message body; text and text attachments including Plain text, HTML text, and Rich Text. If you are looking for an 8-bit string, this option might be best. **Note:** This option might take longer than the **Body (raw MIME data)** option as all data must be converted to Unicode (with whitespace removed) before the search can be performed. **Important!** Because whitespace is removed, this filter with a condition of **contains**, and a value of **sex**, would trigger on the phrase “serious EXpense”.
- ❖ **Body (raw MIME data):** The message text as you would see it if you clicked **Open** in WebMail for that message. If you’re looking for a word (ASCII text) in a message, this option might be best.
- ❖ **Body (binary):** Use this to find the binary value of an alphanumeric string in the message. For example, to use this option to find the “Yen” character (hex A5), you would enter `\xA5`. **Note:** Use backslashes (\) to separate characters; backslashes (\) not followed by “x” are ignored; A-F part is case-insensitive. An example is given in [“Filtering Out All jpegs Using Body\(Binary\)” on page 377](#).
- ❖ **To (message envelope):** A specific recipient's address; this enables filtering on a particular user even on mail coming to them via a distribution list or blind copy. Useful especially for domain filters.
- ❖ **From (message envelope):** A specific sender's address; this is similar to **Return-path** but helps ensure that the responsible party for the mail is filtered. For example, this option can be useful in filtering on mailing list copies; the mailing list manager would be the **From (message envelope)** address.
- ❖ **Return-path:** The return-path address; not useful with domain filters as the return path might be re-written, use **From (message envelope)** instead.
- ❖ **X-Junkmail:** The X-Junkmail header that is added to messages that the **Junk Mail** filter categorizes as spam. For detailed

information on Mirapoint X-Headers, see [“Reading Message Envelopes and Headers” on page 235](#).

- ❖ **X-Junkmail-Whitelist:** The **X-Junkmail-Whitelist** header that is added to messages that come from senders on a safelist.
- ❖ **X-Mirapoint-Virus:** The **X-Mirapoint-Virus** header that is added to messages that are found to contain viruses. This can be useful as a filter for virus deleted messages; for details, see [“Filtering Out “Virus Deleted” Messages” on page 375](#).
- ❖ **X-Mirapoint-Virus-Scanfailure:** The **X-Mirapoint-Virus-Scanfailure** header that is added to messages that are found to contain non-cleanable viruses. Generally, this is an encoded attachment; warn users to never open attachments from unknown sources.
- ❖ **X-DSN-Junkmail, X-DSN-Junkmail-Status, and X-DSN-Mirapoint-Virus:** Delivery status notification (DSNs) headers. Messages with an **X-Junkmail, X-Junkmail-Status, or X-Mirapoint-Virus** header sometimes generate DSNs to the sender. Since spam and virus senders typically never accept such mail, these DSN messages can accumulate in the mail queue. DSN messages always contain an **X-DSN-Junkmail, X-DSN-Junkmail-Status, or X-DSN-Mirapoint-Virus** header. Filter on these objects to prevent DSN messages from accumulating in your mail queue. This selection works best when **Destination Domain = Any or Non-local**.
- ❖ **Attachment MIME Type:** The attachment media type. Choices include the top level MIME types: text, multipart, message, application, image, audio, video, and model; use the **matches** rather than the **contains** content condition (next bullet item) and search for something specific like **“application/vbs”**. For more information, see [“About MIME and Filtering Attachments” on page 334](#).
- ❖ **Attachment file name:** The attachment name. You can use the asterisk wildcard; for example, ***.vbs**.
- ❖ **Attachment size (bytes):** The value must be an integer.
- ❖ **UCE (Junkmail) score:** An integer to be added to the message’s UCE score; you can set any number between 1 and 300. Changing this value affects antispam scanning; for details see [“About the Antispam Scanning Rules and Threshold” on page 336](#).

- ❖ **Message size (bytes):** The value must be an integer.
5. Choose a content condition for the filter type:
 - ❖ **contains:** The object must contain the text you enter. Wildcards are not recognized; the asterisk (*), ampersand (&), and question mark (?) are taken literally. For example, the filter condition: “contains” “doc” would be met with any of these words: “doc”, “document”, “doctor” and so forth.
 - ❖ **does not contain:** The object must not contain the text you enter. **Note:** Use the asterisk (*) wildcard and this option to filter on mail with empty To/CC lines.
 - ❖ **matches:** The object must match the text you enter. Wildcards can be useful (step 6 describes available wildcards); for example, the condition **matches** “Dr. Spock” would only be met by “Dr. Spock,” but the condition **matches** “Dr. Sp*” would be met by “Dr. Spock”, “Dr. Spark”, “Dr. Sproul”, and so forth.
 - ❖ **does not match:** The object must not match the text you enter. Wildcards can be useful.
 - ❖ **regex-matches:** The object must match the regular expression you enter; use with regular expressions only. Can be used to adjust the UCE score; for details see [“regex Filtering to Modify the UCE Scoring” on page 374](#).
 - ❖ **does not regex-match:** The object must not match the regular expression you enter; use with regular expressions only. Can be used to adjust the UCE score; for details see [“regex Filtering to Modify the UCE Scoring” on page 374](#).
 - ❖ **is less than:** The object value must be less than the integer you enter. Wildcards can be useful.
 - ❖ **is more than:** The object value must be more than the integer you enter. Wildcards can be useful.
 6. Enter a value for the filter type in the text box; use text or integers as appropriate. You can use the following wildcard characters:
 - ❖ **Asterisk (*):** Matches any sequence of zero or more characters. Example: to find all attachments with filenames ending in

“.vbs”, use these filter conditions: **Attachment file name:** matches “*.vbs”

- ❖ **Question mark (?):** Matches any single character. Example: to find all messages from “Maria” or “Marie”, use these filter conditions: **From: matches “Mari?”**

Use these wildcards as “starts with,” **something* or *?something*; or “ends with,” *something** or *something?*.

Result: The conditions for the filter are set as specified. Click **More>>** if you want to add further conditions.

7. In the **Filter Action** area specify a response; select one:

- ❖ **Keep (process normally):** Matching messages are sent to the specified recipients. This option is useful in conjunction with other filters or options; see [“Filtering “Keep” Use Examples” on page 376](#).
- ❖ **Forward to (default):** Enter any email address. Matching messages are forwarded as specified. **Important!** The **Forward to** action sends the message directly to the specified email address but does not save a copy on the system.
- ❖ **Forward excerpt to:** Enter any email address. The first 160 characters of matching messages are forwarded as specified. Use this option in conjunction with wireless devices.
- ❖ **Send to Quarantine folder:** Enter the fully-qualified name of a folder that belongs to a user who has been assigned the **Quarantine Administrator** role. The syntax for specifying the folder name is **user.UserName.FolderName**. The folder name is optional; if no folder name is specified, messages are sent to the user’s Inbox. Mail that meets the filter conditions is sent to the quarantine folder and the quarantine administrator can determine whether to restore the message to the mail queue or reject it. For more information, see [“How the Content Filtering Quarantine Works” on page 337](#). For information on the Quarantine Administrator user, see [“About the Quarantine Administrator User” on page 289](#). **Note:** For domain-specific filters, the quarantine folder must belong to a user with the **Quarantine Administrator** role in that delegated domain.
- ❖ **Reject (refuse message and return it to the sender):** Matching message are bounced back to the sender. The recipient receives a message that the action was taken.

- ❖ **Discard (message is irrevocably lost):** Matching messages are deleted. The recipient does not receive a message that the action was taken.
- ❖ **Modify UCE (Junkmail) score:** Enter an integer. Matching messages are given the specified UCE score in addition to any other UCE score the anti-spam scanner awards; and acted on accordingly by the **Junk Mail** filter. This selection automatically deselects the **Remove attachments that meet attachment conditions** and **Do not apply any more filters to this message if action is taken** options (described below) and places the new filter rule before the **Junk Mail** filter rule. **Note:** Without JavaScript enabled, these adjustments might have to be done manually.

Additionally, you can specify:

- ❖ **Remove attachments that meet attachment conditions** (deselected by default): Attachments that meet the specified conditions are removed from the message.
- ❖ **Do not apply any more filters to this message if action is taken** (selected by default): Any filters listed after this filter are not applied to the message.
- ❖ **Send Recipient(s) the following message** (deselected by default): The message recipient is sent the message if the filter conditions are met. You can modify the **From**, **Subject**, **Message** text, or encoding of the message.

8. Click **OK** to save the new filter.

Result: The system accepts the settings and a description of the filter appears above the **Filter Conditions** box; incoming messages and attachments are filtered and acted on as directed. If you click **Cancel**, no filter is created and you are returned to the filter list page.

Reordering a List of Filters

Before and during message acceptance on the system, SMTP authentication, relay and blocked domains, and RBL's (real time blackhole lists) are processed. After message acceptance, the default order of operations among content filters is as follows: Anti-virus

(whichever engine is closest to the edge), then Anti-spam (includes all antispam filters that are configured), then domain signatures are added, then domain filters (including primary domain). You can modify this order or operation as described in this section.

Each incoming message is filtered in the order the filters appears in the **Advanced** page filter list, from top to bottom. Changing the order of the filters in this list changes the sequence in which each filter's conditions are applied. When a specified condition is met, filter processing for the message continues, unless the **Do not apply any more filters to this message if action is taken** checkbox is selected (as it is by default).

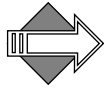


Figure 57 Advanced Content Filters Page, Reordering Filters

Reorder the filters as follows:

- ◆ In the filter list, move a filter up in the order by clicking the **up-arrow** ▲ in the **Order** column.
- ◆ In the filter list, move a filter down in the order by clicking the **down-arrow** ▼ in the **Order** column.
- ◆ On the filter edit page, move a filter either above or below the **Perform Anti-Virus and Anti-Spam scanning here point**, by selecting, or deselecting, the **Filter this message before performing Anti-Virus and Anti-Spam scanning** option.

Repeat until you are satisfied with the order.



See [“About the Destination Domain Options” on page 332](#) for information on how the Destination Domain for a filter affects the order in which it is executed. See [“About Filter Priorities and Ordering” on page 333](#) for more information on filtering ordering.

Attaching a Signature to All Messages From a Domain

To attach a signature to all mail from a domain, see [“Creating a Signature for a Delegated Domain” on page 270](#).

Using Wire Taps

Use this feature to monitor all mail sent to or from a particular address. On the **Wire Taps** page, specify the address you want to monitor and the forwarding address to which you want to copy messages.

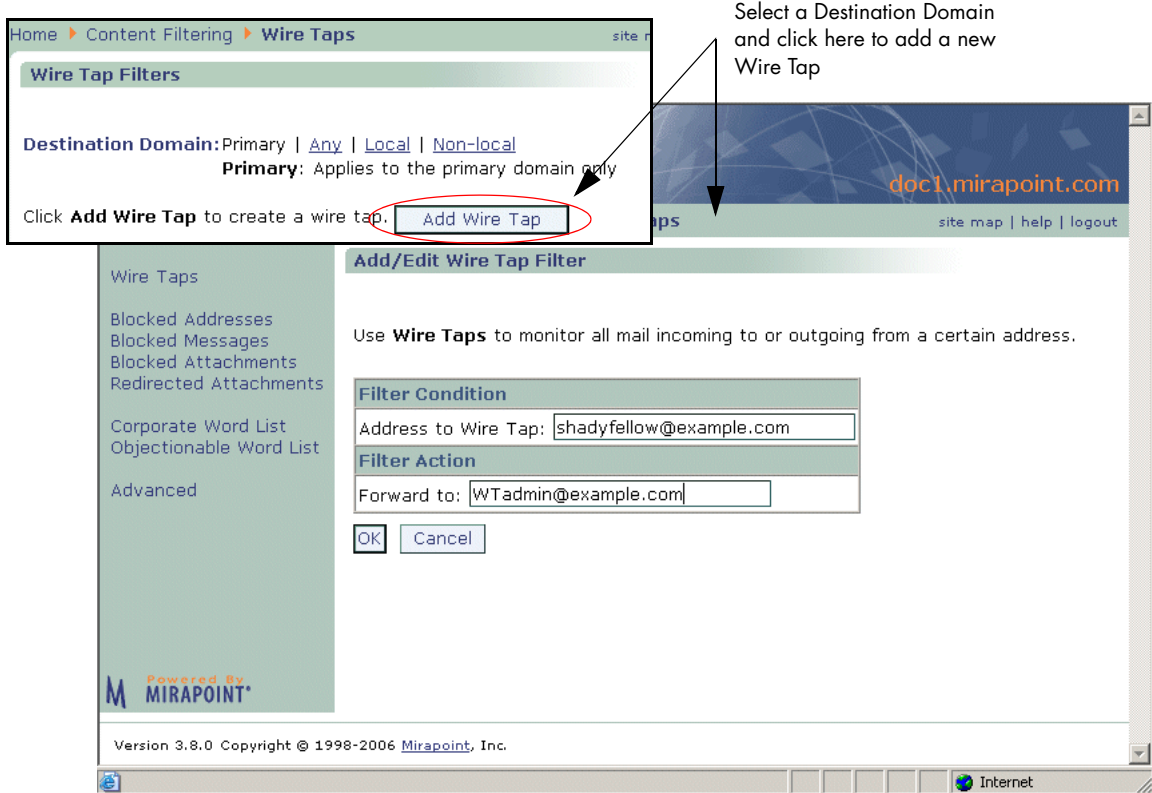


Figure 58 Content Filtering > Wire Tap Page

To create, edit, or delete a Wire Tap follow these steps on the **Content Filtering > Wire Taps** page (see Figure 58 for an example).

1. In the **Destination Domain** area specify the scope for the filter you are creating. **Note:** If you select a domain before coming to this

page or if you log in as a domain administrator, these options do not display. Select one:

- ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
- ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
- ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
- ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.


Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. To add a wire tap, click **Add Wire Tap**.


Result: The **Add/Edit Wire Tap** page opens.

3. Enter an email address in the **Address to Wire Tap** text box and another in the **Forward to** option and click **OK**.

Result: The **Wire Taps** page is refreshed and the updated list of wire taps includes the new wire tap. Mail sent to or coming from the specified **Address** has a copy sent also to the specified **Forward to** address. Additionally, the X-MirapointEnvelopeTo and X-MirapointEnvelopeFrom headers are added; an address not listed in the To or Cc headers, but listed in the EnvelopeTo header, is a Bcc address. This filter displays on the **Content Filtering > Advanced** page and can be edited or deleted from that page.

4. To edit a wire tap, click the wire tap's **Edit** icon .

Result: The **Add/Edit Wire Tap** page opens. Click **OK** to apply changes; click **Cancel** to terminate the edit.

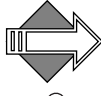
5. To delete a wire tap, click the wire tap's **Delete** icon .

Result: A **Confirm Delete** page opens; click **Delete** or **Cancel**.

Example Wire Tap Addresses Entries

allan@example.com: Specifically adds the user **allan** from **example.com** to your Wire Tap list; any incoming mail from **allan@example.com** is forwarded as specified.

@spamcity.com: Adds any address at **spamcity.com** to your Wire Tap list; any incoming mail from any user in the **spamcity.com** domain is forwarded as specified.



You cannot use wildcards with the Content Filtering word lists.



An empty **Address to Wire Tap** option causes all mail for that Destination Domain to get wire tapped.

Using Word List Filters

Word List filters use a list of words, phrases, or addresses that you create to filter messages. How to manage the filter list is similar for all the list filters. Filter lists are processed as follows:

- ◆ A wordlist is imported for the current domain. Each line forms a pattern, which is UTF-8 normalized, as defined by the Unicode specification. Upper case letters are converted to lower case.
- ◆ Each pattern is parsed into words and delimiters. Words are composed of ASCII alphanumeric characters (hex 30-39, 41-5A, 61-7A) plus all characters above hex 80, the range of Unicode characters. Delimiters include spaces and ASCII punctuation marks (hex 20-2F, 3A-40, 5B-60, 7B-7E).
- ◆ The filter attribute (portion of an email message) is also UTF-8 normalized, unless it is a header address or **bodydecodedbinary** attachment. This is because header addresses must be ASCII, and binary attachments are not Unicode.
- ◆ Implicit delimiters are placed at the beginning and end of both the pattern and the filter attribute.
- ◆ **Attachment MIME Type** and **Attachment file name** filter types receive special treatment to make them easy to parse:
 - ❖ If the wordlist pattern starts with a period (.) it is interpreted as a file extension. The filter attribute attachment is searched for that file extension, ensuring that the file-extension name ends with a space, semicolon (;) or slash (/).

- ❖ If the wordlist pattern starts with a slash (/) it is interpreted as a MIME type. The filter attribute attachment is searched for that MIME type, ensuring that the MIME type ends with a space, semicolon (;) or slash (/).
- ❖ Normal wordlist search continues if the above two steps fail to match.

For each pattern (line), wordlists are compared as follows:

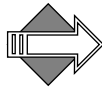
- ◆ The search library understands UTF-8 and calculates the number of bytes forming each Unicode character, and compares Unicode codepoints, converting the filter attribute from upper to lower case.
- ◆ The pattern and filter attribute are compared word by word, moving forward one word at a time, words being separated by delimiters.
- ◆ Strings of delimiters are treated as a single delimiter. Any delimiter matches any other delimiter.
- ◆ If all the words match and we run out of words in the pattern, the comparison returns **MATCH**, and searching terminates.
- ◆ Otherwise when the comparison reaches the end of the filter attribute without matching all words in the pattern, comparison returns **NOMATCH**, and searching continues with the next pattern (line) in the wordlist, if any.

The intention is that all the following match the “end start” pattern:

```
Fragment end... start another!
Fragment end? Start another.
Fragment end!! Start another.
“Fragment end.” “Start another.”
```

Also, pattern “a@b.com” matches any of the following, but neither “a1@b.com” nor “abba@b.com” addresses (all these forms are in common use today):

```
a@b.com
"a"@b.com
<a@b.com>
<"a"@b.com>
```



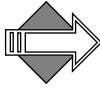
The pattern “user1@example.com” matches input “user1????example.com” because all delimiters match each other, and multiple delimiters are compressed to a single delimiter.

Managing a Filter List

All of the **Content Filtering** filters, except **Wire Taps**, use a filter list that you create as the trigger for the filter. For example, the **Blocked Addresses** filter list contains the addresses that you want blocked. You can create the filter and then create the filter list, or you can create the filter list first and then the filter. You can also import a filter list, a simple text file with entries separated by line breaks, or export a filter list. A filter list can contain words, phrases, or addresses.



You cannot separate entries with spaces or semi-colons; each entry must be on a separate line. Therefore, you must make your entries one at a time. Wildcards are not accepted.



Wordlists match on whole words, not parts of words. Whitespaces in phrases match with any number of like, empty, characters. For example, the phrase “**a big match**” matches “**a big match**”.

Import List
Enter a file and click **Import** to overwrite the current list.

File:

Charset:

Export List
Click **Export** to save the list to a text file.

Charset:

Import a word list you have created here

Export a word list you have created here; you can then import that word list to other word list filters

Add/Edit List
Alternatively, manage the contents of the list here. Wildcards are not accepted.

E-mail Address or Domain:

Word List editor for Blocked Addresses

Add/Edit List
Alternatively, manage the contents of the list here. Wildcards are not accepted.

Attachment name or MIME type:

Word List editor for Blocked and Redirected Attachments

Add/Edit List
Alternatively, manage the contents of the list here. Wildcards are not accepted.

Word or phrase:

Word List editor for Corporate and Objectionable Word Lists

Figure 59 Word List Editor for Word List Content Filters

To create, edit, delete, import, or export a filter list for any content filter (**Blocked Addresses**, **Blocked Messages**, **Blocked Attachments**, and so forth), follow these steps. on the filter list pages, respectively. See Figure 59 for examples.

1. To add an initial filter list, either import an existing word/phrase/address list; or, in the **Add/Edit List** area, enter text in the option; your choices are ONE of the following:
 - ❖ **E-mail Address or Domain:** Blocked Addresses filter uses this to know whose mail to block.
 - ❖ **Word or Phrase:** Blocked Messages, Corporate Word, and Objectionable Word filters use this to know what words or phrases to act on. Remember: Wordlist filters match on whole words, not parts of words. Phrases can match unexpectedly.
 - ❖ **Attachment name or Mime type:** Blocked Attachments and Redirected Attachments filters use this to know what attachments to act on. For more information, see [“About MIME and Filtering Attachments” on page 334](#).

Click **Add**. Repeat as needed.

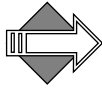
Result: In the **Edit List** area, a filter list table displays your trigger text.

2. To edit the filter list, do one of the following:
 - ❖ Enter new address, word, or attachment information in the text box and click **Add**.
 - ❖ Select an address, word, or attachment (respectively) in the list and click **Remove**.
Note: You cannot simply edit a filter list entry; you must delete the entry you want to change and then add it back.

Result: If you enter new text and click **Add**, that new filter trigger displays in the filter wordlist. If you select an address, word, or attachment (respectively) and click **Remove**, a **Confirm Delete** page opens; click **Remove** or **Cancel**.

3. To delete a filter list, select each entry you want to delete and click **Remove**. To delete the entire list, select all of the entries and click **Remove**.
Result: A confirmation page displays. Click **Remove** to finish, click **Cancel** to terminate the operation and make no changes.

4. To import a filter list, enter the filename and path of the list (a text file) or browse to it and click **Import**.
Result: The selected list is loaded to the page and displays in the **Edit List** area. **Note:** The imported list overwrites the existing list. To save your existing list, export it and incorporate it into the new list before importing the new list.
5. To export a filter list, click the **Export** button.
Result: A **File Download** dialog box opens allowing you to open the list file or save it as a text file.



You cannot use wildcards with the Content Filtering word lists.

Forward to vs. Send to Quarantine Folder

The content filtering word list filters offer two options, **Forward to** and **Send to Quarantine folder**, that appear similar; however, there are two important differences in these two filter actions:

- ◆ The address you can enter. For the **Forward to** option, enter any email address; for example, **UserName@example.com**. If you know the user is local to the machine, you can just enter the User Name. For the **Send to Quarantine Folder** option, you must enter the fully qualified folder address of a user local to the machine. For example, **user.UserName.FolderName**. If you omit the **FolderName**, messages are sent to the specified user's **Inbox**. You must preface the address with **“user.”** The user must have the Quarantine Administrator role to use the Deliver button. See [“About the Quarantine Administrator User” on page 289](#) for more information.
- ◆ The way the actions treat the message. The **Forward to** option simply delivers the message to the forwarding address. The **Send to Quarantine folder** option uses special coding to “wrap” the message so that if it is released back to the mail queue (through the office of the **Deliver** button) it is delivered to the recipients without indication that it was in quarantine.

Using Blocked Addresses

Use the **Blocked Addresses** page to specify certain addresses or domains from which incoming mail should trigger the selected **Blocked Addresses** filter action. For details on creating your Blocked Addresses list, see [“Managing a Filter List” on page 353](#).

The screenshot shows the 'Add/Edit Blocked Addresses Filter' page in the Mirapoint Message Server. The page is titled 'Add/Edit Blocked Addresses Filter' and includes a navigation menu on the left with options like 'Wire Taps', 'Blocked Addresses', 'Blocked Messages', 'Blocked Attachments', 'Redirected Attachments', 'Corporate Word List', 'Objectionable Word List', and 'Advanced'. The main content area is divided into 'Filter Condition' and 'Filter Action' sections.

Filter Condition: If a mail message is from anyone on the Blocked Address List.

Filter Action:

- Forward to: []
- Send to Quarantine folder: `user.BAadmin.blkdAddresses` `user.UserName[.Folder.Folder....]`
 Note: UserName must have ~~Quarantine administrator~~ role.
- Reject (refuse message and return it to the sender)
- Discard (message is irrevocably lost)

Send the recipient(s) the following notification message:

From: Administrator

Subject: Your mail has been filtered

Message: Your mail from `$(sender)` with subject `$(subject)` has been `$(action)` by `$(filtername)` filter. Please send mail to `Badmin@$(domain)` for further information.

Unicode (UTF-8)

`$(sender)`=Sender `$(subject)`=Subject `$(action)`=Action
`$(attachments)`=List of attachments `$(domain)`=Current Domain
`$(filtername)`=Filter name that triggered the notification

OK Cancel

Annotations:

- An arrow points to the 'Send to Quarantine folder' option with the text: "This user must have the Quarantine Administrator role and a local folder".
- A red circle highlights the notification message text, with an arrow pointing to it from the text: "You can add to or modify this text".

Figure 60 Content Filtering > Blocked Addresses Page

To create, edit, or delete a **Blocked Addresses** filter, follow these steps on the **Content Filtering > Blocked Addresses** page (see Figure 60).


1. In the **Destination Domain** area specify the scope for the filter you are creating. **Note:** If you select a domain before coming to this page or if you log in as a domain administrator, these options do not display. Select one:
 - ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
 - ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
 - ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
 - ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.


Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. Create a **Blocked Addresses** list; to do this, see [“Managing a Filter List” on page 353](#) for details; example list entries follow this procedure.
3. To add an initial **Blocked Addresses** filter, click **Add Filter**.
Result: The **Add/Edit Blocked Addresses** page displays.
4. Choose a filter action:
 - ❖ **Forward to** (default): Any email address; matching messages are sent there. For more information, see [“Forward to vs. Send to Quarantine Folder” on page 355](#).
 - ❖ **Send to Quarantine folder:** The address of a WebMail user, local to the box, with the Quarantine Administrator role; specified as `user.UserName.FolderName` (*FolderName* being optional), OR `user.QuarantineAdmin` to send matching messages to Quarantine Manager. For details, see [“How the Content Filtering Quarantine Works” on page 337](#).
 - ❖ **Reject (refuse message and return it to the sender)** (default)
 - ❖ **Discard** (message is irrevocably lost)

5. Optionally, you can select the **Send Recipient(s) the following message** checkbox. You can change the **From, Subject, Message** text, and/or encoding as desired.
6. Click **OK** to save your changes.

Result: If you click **OK**, the **Blocked Addresses** page is updated to display the **Blocked Addresses** filter table, which shows the selected filter action for the Blocked Addresses filter. The filter also displays on the **Content Filtering > Advanced** page and can be edited or deleted from that page.

If you click **Cancel**, your changes are not saved and the page is updated to show the previously-saved settings.
7. To change the filter action, click the **Edit** icon  in the filter table.

Result: The **Add/Edit Blocked Addresses** page displays. Click **OK** to apply changes; click **Cancel** to terminate the edit.
8. To delete the **Blocked Addresses** filter, click the **Delete** icon  in the filter table.

Result: A confirmation page opens; click **Delete** or **Cancel**.

Example Blocked Address List Entries

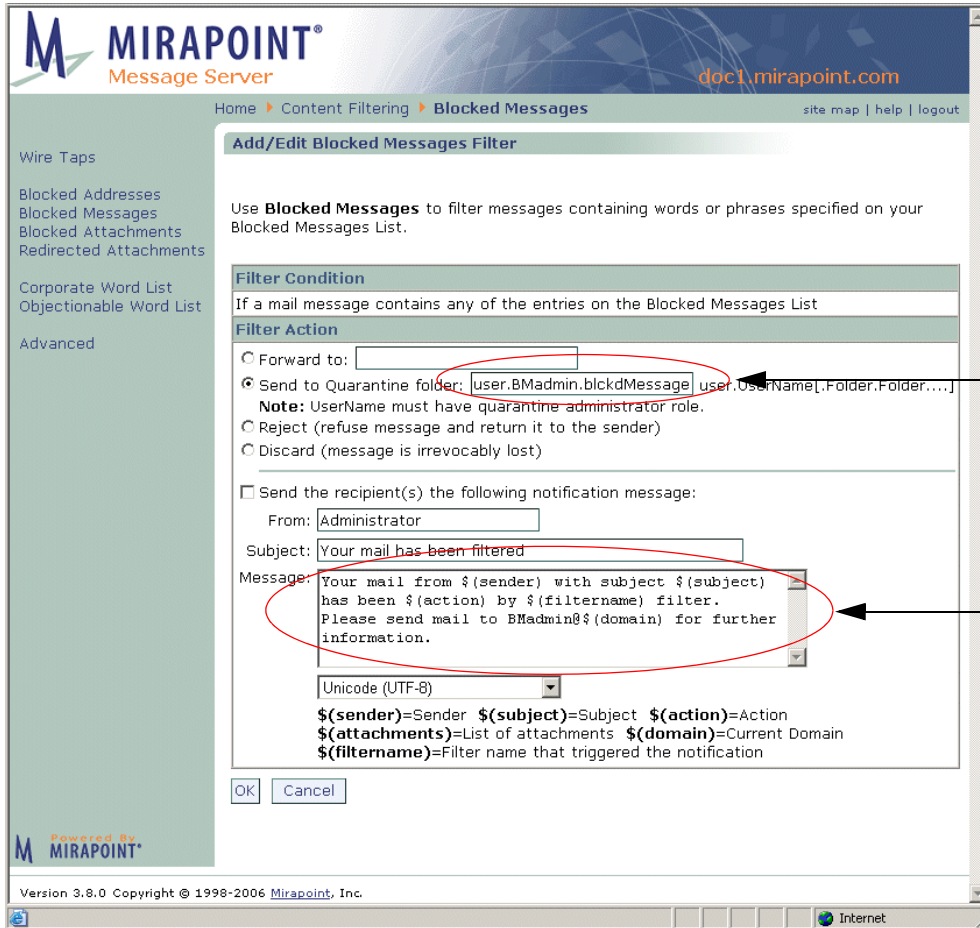
Use the **Add/Edit List** area of the **Blocked Addresses Filter** page to create your own list. Below are example list entries for Blocked Addresses.

allan@example.com: Specifically adds the user **allan** from **example.com** to your Blocked Addresses filter list; any incoming mail from **allan@example.com** is acted on as specified by the Blocked Address filter action.

@spamcity.com: Adds any address at **spamcity.com** to your Blocked Addresses filter list; all mail coming from any user at the **spamcity.com** domain is acted on as specified by the Blocked Address filter action.

Using Blocked Messages

Use the **Blocked Messages** page to specify certain words or phrases that should trigger the selected **Blocked Messages** filter action. For details on creating your Blocked Messages list, see [“Managing a Filter List” on page 353](#).



This user must have the Quarantine Administrator role and a local folder

You can add to or modify this text



Figure 61 Content Filtering > Blocked Messages Page

To create, edit, or delete a Blocked Messages filter follow these steps on the **Content Filtering > Blocked Messages** page (see Figure 61).

1. In the **Destination Domain** area specify the scope for the filter you are creating. **Note:** If you select a domain before coming to this page or if you log in as a domain administrator, these options do not display. Select one:
 - ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
 - ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
 - ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
 - ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.

Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. Create a **Blocked Messages** list; to do this, see [“Managing a Filter List” on page 353](#) for details; example list entries follow this procedure.
3. To add an initial **Blocked Messages** filter, click **Add Filter**.
Result: The **Add/Edit Blocked Messages Filter** page displays.
4. Choose a filter action:
 - ❖ **Forward to** (default): Any email address; matching messages are sent there. For more information, see [“Forward to vs. Send to Quarantine Folder” on page 355](#).
 - ❖ **Send to Quarantine folder:** The address of a WebMail user, local to the box, with the Quarantine Administrator role; specified as `user.UserName.FolderName` (*FolderName* being optional), OR `user.QuarantineAdmin` to send matching messages to Quarantine Manager. For details, see [“How the Content Filtering Quarantine Works” on page 337](#).
 - ❖ **Reject** (refuse message and return it to the sender) (default)
 - ❖ **Discard** (message is irrevocably lost)

5. Optionally, you can select the **Send Recipient(s) the following message** checkbox. You can change the **From, Subject, Message** text, and/or encoding as desired.
6. Click **OK** or **Cancel**.
Result: If you click **OK**, the **Blocked Messages** page is updated to display the **Blocked Messages** filter table, which shows the selected filter action for the Blocked Messages Filter. The filter is also listed on the **Content Filtering > Advanced** page and can be edited or deleted from that page. If you click **Cancel**, your changes are not saved and the **Blocked Messages** page is updated to show the previously-saved settings.
7. To change the filter action, click the **Edit** icon  in the filter table.
Result: The **Add/Edit Blocked Messages** page displays. Click **OK** to apply changes; click **Cancel** to terminate the edit.
8. To delete the **Blocked Messages** filter, click the **Delete** icon  in the filter table.
Result: A confirmation page opens; click **Delete** or **Cancel**.

Example Blocked Messages List Entry

Use the **Add/Edit List** area of the **Blocked Messages Filter** page to create your own list. Below is an example list entry for Blocked Messages.

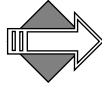
make big money: Specifically adds the phrase **make big money** to your Blocked Messages filter list; any incoming mail containing that phrase is acted on as specified by the Blocked Messages filter action.



You cannot separate entries with spaces or semi-colons; each entry must be on a separate line. Therefore, you must make your entries one at a time. Wildcards are not accepted.

Using Blocked Attachments

Use the **Blocked Attachments** page to specify that mail containing certain attachment names or types should trigger the selected **Blocked Attachments** filter action. For details on creating your Blocked Attachments list, see [“Managing a Filter List” on page 353](#). To understand this filter better, see [“About MIME and Filtering Attachments” on page 334](#).



There is a list of attachments that Microsoft recommends to block that you can view at

<http://office.microsoft.com/en-us/assistance/HA011402971033.aspx>

MIRAPPOINT®
Message Server
doc1.mirapoint.com

Home > Content Filtering > Blocked Attachments

Wire Taps
Blocked Addresses
Blocked Messages
Blocked Attachments
Redirected Attachments
Corporate Word List
Objectionable Word List
Advanced

Add/Edit Blocked Attachments Filter

Use **Blocked Attachments** to reject or discard messages based on the Attachment name or MIME type of message attachments.

Filter Condition
If a mail message contains any of the attachment names or MIME types found in the Blocked Attachments List

Filter Action

Forward to:

Send to Quarantine folder:
Note: UserName must have quarantine administrator role.

Reject (refuse message and return it to the sender)

Discard (message is irrevocably lost)

Send the recipient(s) the following notification message:

From:

Subject:

Message:

Unicode (UTF-8)

\$(sender)=Sender \$(subject)=Subject \$(action)=Action
\$(attachments)=List of attachments \$(domain)=Current Domain
\$(filtername)=Filter name that triggered the notification

This user must have the Quarantine Administrator role and a local folder

You can add to or modify this text

Figure 62 Content Filtering > Blocked Attachments Page

To create, edit, or delete a Blocked Attachments filter follow these steps on the **Content Filtering > Blocked Attachments** page (see Figure 62).

1. In the **Destination Domain** area specify the scope for the filter you are creating. **Note:** If you select a domain before coming to this



page or if you log in as a domain administrator, these options do not display. Select one:

- ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
- ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
- ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
- ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.

Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. Create a **Blocked Attachments** list; to do this, see [“Managing a Filter List” on page 353](#) for details; example list entries follow this procedure.
3. To add an initial **Blocked Attachments** filter, click **Add Filter**.
Result: The **Add/Edit Blocked Attachments** page displays.
4. Choose a filter action:
 - ❖ **Forward to** (default): Any email address; matching messages are sent there. For more information, see [“Forward to vs. Send to Quarantine Folder” on page 355](#).
 - ❖ **Send to Quarantine folder:** The address of a WebMail user, local to the box, with the Quarantine Administrator role; specified as `user.UserName.FolderName` (*FolderName* being optional), OR `user.QuarantineAdmin` to send matching messages to Quarantine Manager. For details, see [“How the Content Filtering Quarantine Works” on page 337](#).
 - ❖ **Reject** (refuse message and return it to the sender) (default)
 - ❖ **Discard** (message is irrevocably lost)
5. Optionally, you can select the **Send Recipient(s) the following message** checkbox. You can change the **From**, **Subject**, **Message** text, and/or encoding as desired.
6. Click **OK** or **Cancel**.
Result: If you click **OK**, the **Blocked Attachments** page is updated to display the **Blocked Attachments** filter table, which shows the

selected action for your filter. The filter is also listed on the **Content Filtering > Advanced** page and can be edited or deleted from that page. If you click **Cancel**, your changes are not saved and the **Blocked Attachments** page is updated to show the previously-saved settings.

7. To change the filter action, click the **Edit** icon  in the filter table. Result: The **Add/Edit Blocked Attachments** page displays. Click **OK** to apply changes; click **Cancel** to terminate the edit.
8. To delete the **Blocked Attachments** filter, click the **Delete** icon  in the filter table. Result: A confirmation page opens; click **Delete** or **Cancel**.

Example Blocked Attachments List Entries

Use the **Add/Edit List** area of the **Blocked Attachments Filter** page to create your own list. Below are example list entries.

iloveyou.vbs: Adds the attachment file name **iloveyou.vbs** to your Attachments filter list. Any incoming mail attachment with the name **iloveyou.vbs** is handled according to the selected Attachments filter action.

.vbs: Adds the file extension **.vbs** to your Attachments filter list. Any incoming mail attachment with a **.vbs** extension is handled according to the selected Attachments filter action. **Important!** If you enter **vbs** without the period (**.**), the filter scans the entire attachment name for the letters “vbs”, not just the file extension.

image/gif: Adds the **gif** file type to your Attachments filter list. Any incoming gif attachments, regardless of the file extension, are handled according to the selected Attachments filter action.



Each entry must be on a separate line. You cannot separate entries with spaces or semi-colons—you must add list entries one at a time. Wildcards are not accepted.

Using Redirected Attachments

Use the **Redirected Attachments** page to specify that mail containing certain attachment names or types should trigger the selected **Redirected Attachments** filter action. For details on creating your

Redirected Attachments list, see [“Managing a Filter List” on page 353](#).
 To understand this filter better, see [“About MIME and Filtering Attachments” on page 334](#).

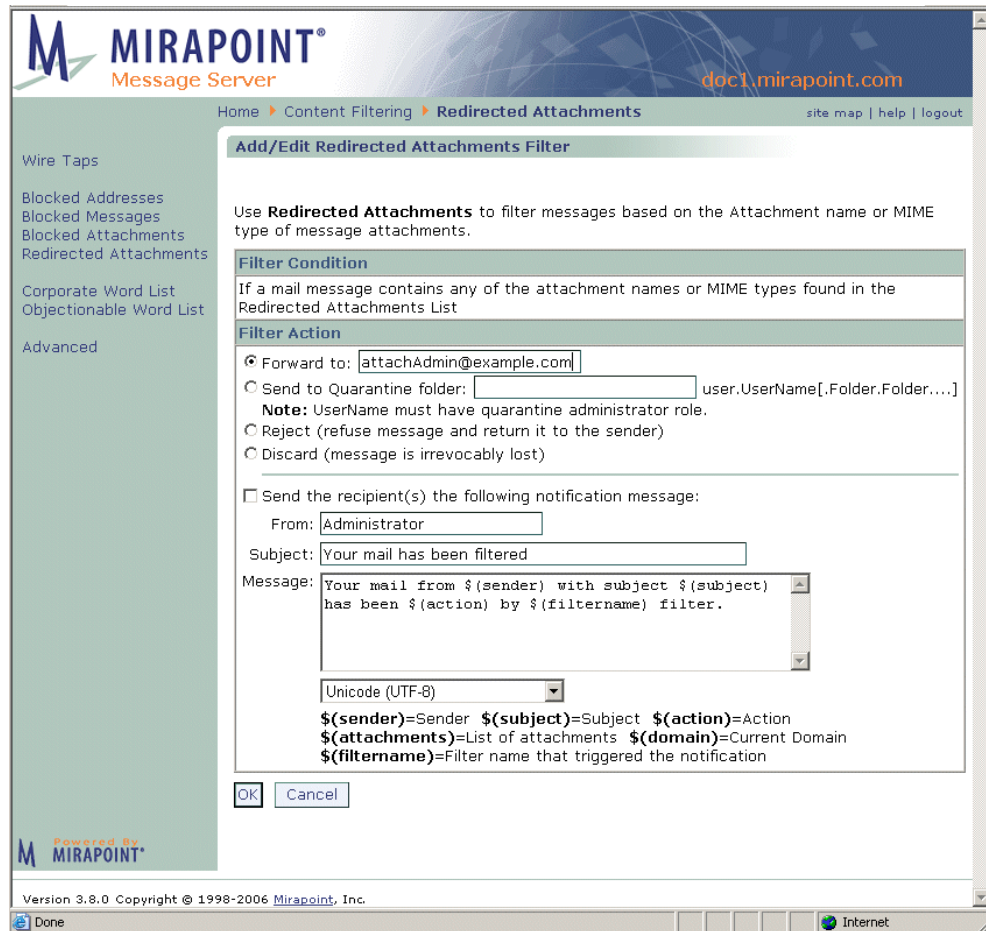


Figure 63 Content Filtering > Redirected Attachments Page

To create, edit, or delete a Redirected Attachments filter follow these steps on the **Content Filtering > Redirected Attachments** page (see Figure 63).

1. In the **Destination Domain** area specify the scope for the filter you are creating. **Note:** If you select a domain before coming to this

page or if you log in as a domain administrator, these options do not display. Select one:



- ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
- ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
- ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
- ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.

Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. Create a **Redirected Attachments** list; to do this, see [“Managing a Filter List” on page 353](#) for details; example list entries follow this procedure.
3. To add an initial **Redirected Attachments** filter, click **Add Filter**.
Result: The **Add/Edit Redirected Attachments** page displays.
4. Choose a filter action:
 - ❖ **Forward to** (default): Any email address; matching messages are sent there. For more information, see [“Forward to vs. Send to Quarantine Folder” on page 355](#).
 - ❖ **Send to Quarantine folder:** The address of a WebMail user, local to the box, with the Quarantine Administrator role; specified as `user.UserName.FolderName` (*FolderName* being optional), OR `user.QuarantineAdmin` to send matching messages to Quarantine Manager. For details, see [“How the Content Filtering Quarantine Works” on page 337](#).
 - ❖ **Reject (refuse message and return it to the sender)** (default)
 - ❖ **Discard** (message is irrevocably lost)
5. Optionally, you can select the **Send Recipient(s) the following message** checkbox. You can change the **From**, **Subject**, **Message** text, and/or encoding as desired.
6. Click **OK** or **Cancel**.

Result: If you click **OK**, the **Redirected Attachments** page is updated to display the **Redirected Attachments** filter table, which shows the selected filter action for the Redirected Attachments filter. The filter is also listed on the **Content Filtering > Advanced** page and can be edited or deleted from that page.

If you click **Cancel**, your changes are not saved and the **Redirected Attachments** page is updated to show the previously-saved settings.

7. To change the filter action, click the **Edit** icon  in the filter table. Result: The **Add/Edit Blocked Attachments** page displays. Click **OK** to apply changes; click **Cancel** to terminate the edit.
8. To delete the **Redirected Attachments** filter, click the **Delete** icon  in the filter table. Result: A confirmation page opens; click **Delete** or **Cancel**.

Example Redirected Attachments List Entries

Use the **Add/Edit List** area of the **Redirected Attachments Filter** page to create your own list. Below are example list entries for Redirected Attachments.

application/x-msdos-program: Specifically adds the executable MS DOS MIME type to your Attachments filter list; any incoming mail attachment with the suffix **com**, **exe**, or **bat**, is acted on as specified by the Attachments filter action.

vbs: Specifically adds the file extension **.vbs** to your Attachments filter list; any incoming mail attachment with the suffix **vbs** is acted on as specified by the Redirected Attachments filter action.



You cannot separate entries with spaces or semi-colons; each entry must be on a separate line. Therefore, you must make your entries one at a time. Wildcards are not accepted.

Using Corporate Word List

Use the **Corporate Word List** page to specify certain words or phrases that should trigger the selected **Corporate Word List** filter action. For details on creating your Corporate Word list, see [“Managing a Filter List” on page 353](#).

MIRAPOINT®
Message Server

Home > Content Filtering > Corporate Word List

site map | help | logout

Wire Taps

- Blocked Addresses
- Blocked Messages
- Blocked Attachments
- Redirected Attachments

Corporate Word List

Objectionable Word List

Advanced

Add/Edit Corporate Word List Filter

Use **Corporate Word List** to filter messages containing words or phrases specified on your Corporate Word List.

Filter Condition

If a mail message contains any of the words found in the Corporate Word List

Filter Action

Forward to:

Send to Quarantine folder: user.UserName[.Folder.Folder....]
Note: UserName must have quarantine administrator role.

Reject (refuse message and return it to the sender)

Discard (message is irrevocably lost)

Send the recipient(s) the following notification message:

From:

Subject:

Message:

Unicode (UTF-8)

\$(sender)=Sender **\$(subject)**=Subject **\$(action)**=Action
\$(attachments)=List of attachments **\$(domain)**=Current Domain
\$(filtername)=Filter name that triggered the notification

Version 3.8.0 Copyright © 1998-2006 Mirapoint, Inc.

Figure 64 Content Filtering > Corporate Word List Page

To create, edit, or delete a Corporate Word List filter follow these steps on the **Content Filtering > Corporate Word List** page (see Figure 64).



1. In the **Destination Domain** area specify the scope for the filter you are creating. **Note:** If you select a domain before coming to this page or if you log in as a domain administrator, these options do not display. Select one:
 - ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
 - ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
 - ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
 - ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.

Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.
2. Create a **Corporate Word list**; to do this, see [“Managing a Filter List” on page 353](#) for details; example list entries follow this procedure.
3. To add an initial **Corporate Word List** filter, click **Add Filter**.
Result: The **Add/Edit Corporate Word List Filter** page displays.
4. Choose a filter action:
 - ❖ **Forward to** (default): Any email address; matching messages are sent there. For more information, see [“Forward to vs. Send to Quarantine Folder” on page 355](#).
 - ❖ **Send to Quarantine folder:** The address of a WebMail user, local to the box, with the Quarantine Administrator role; specified as `user.UserName.FolderName` (*FolderName* being optional), OR `user.QuarantineAdmin` to send matching messages to Quarantine Manager. For details, see [“How the Content Filtering Quarantine Works” on page 337](#).
 - ❖ **Reject (refuse message and return it to the sender)** (default)
 - ❖ **Discard** (message is irrevocably lost)

5. Optionally, you can select the **Send Recipient(s) the following message** checkbox. You can change the **From, Subject, Message** text, and/or encoding as desired.
6. Click **OK** or **Cancel**.

Result: If you click **OK**, the **Corporate Word List** page is updated to display the **Corporate Word List** filter table, which shows the selected filter action for the Corporate Word List filter. The filter is also listed on the **Content Filtering > Advanced** page and can be edited or deleted from that page.

If you click **Cancel**, your changes are not saved and the **Corporate Word List** page is updated to show the previously-saved settings.

7. To change the filter action, click the **Edit** icon  in the filter table.
Result: The **Add/Edit Corporate Word List** page displays. Click **OK** to apply changes; click **Cancel** to terminate the edit.
8. To delete the **Corporate Word List** filter, click the **Delete** icon  in the filter table.
Result: A confirmation page opens; click **Delete** or **Cancel**.

Example Corporate Word List Entries

Use the **Add/Edit List** area of the **Corporate Word List Filter** page to create your own list. Below are example list entries for Corporate Word List.

confidential: Specifically adds the word **confidential** to your Word filter list; any incoming mail containing that word is acted on as specified by the Word List filter action.

phooey: Specifically adds the word **phooey** to your Word filter list; any incoming mail containing that word is acted on as specified by the Word List filter action.



You cannot separate entries with spaces or semi-colons; each entry must be on a separate line. Therefore, you must make your entries one at a time. Wildcards are not accepted.

Using Objectionable Word List

Use the **Objectionable Word List** page to specify certain words or phrases that should trigger the selected **Objectionable Word List** filter action. This filter is similar to the Corporate Word List, but provides the option of having different filter actions for different words or phrases. For details on creating your Objectionable Word list, see [“Managing a Filter List” on page 353](#).

The screenshot shows the Mirapoint Message Server web interface. The page title is "Add/Edit Objectionable Word List Filter". The breadcrumb navigation is "Home > Content Filtering > Objectionable Word List". The page includes a sidebar with navigation links: "Wire Taps", "Blocked Addresses", "Blocked Messages", "Blocked Attachments", "Redirected Attachments", "Corporate Word List", "Objectionable Word List", and "Advanced".

The main content area contains the following sections:

- Filter Condition:** "If a mail message contains any of the words found in the Objectionable Word List"
- Filter Action:**
 - Forward to: [text box]
 - Send to Quarantine folder: `user.Owadmin.objectWords` user.UserName[.Folder.Folder....]
 - Note:** UserName must have quarantine administrator role.
 - Reject (refuse message and return it to the sender)
 - Discard (message is irrevocably lost)
- Send the recipient(s) the following notification message:
 - From: Administrator
 - Subject: Your mail has been filtered
 - Message: Your mail from `$(sender)` with subject `$(subject)` has been `$(action)` by `$(filtername)` filter.
 - Unicode (UTF-8)
 - Legend: `$(sender)`=Sender `$(subject)`=Subject `$(action)`=Action
`$(attachments)`=List of attachments `$(domain)`=Current Domain
`$(filtername)`=Filter name that triggered the notification

Buttons: [OK] [Cancel]

Footer: Version 3.8.0 Copyright © 1998-2006 Mirapoint, Inc.

Figure 65 Content Filtering > Objectionable Word List Page

To create, edit, or delete a **Objectionable Word List** filter follow these steps on the **Content Filtering > Objectionable Word List** page (see Figure 65).

1. In the **Destination Domain** area specify the scope for the filter you are creating. **Note:** If you select a domain before coming to this page or if you log in as a domain administrator, these options do not display. Select one:
 - ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
 - ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
 - ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
 - ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.



Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. Create an **Objectionable Word** list; to do this, see [“Managing a Filter List” on page 353](#) for details; example list entries follow this procedure.
3. To add an initial **Objectionable Word List** filter, click **Add Filter**.
Result: The **Add/Edit Objectionable Word List** page displays.
4. Choose a filter action:
 - ❖ **Forward to** (default): Any email address; matching messages are sent there. For more information, see [“Forward to vs. Send to Quarantine Folder” on page 355](#).
 - ❖ **Send to Quarantine folder:** The address of a WebMail user, local to the box, with the Quarantine Administrator role; specified as `user.UserName.FolderName` (*FolderName* being optional), OR `user.QuarantineAdmin` to send matching messages to Quarantine Manager. For details, see [“How the Content Filtering Quarantine Works” on page 337](#).
 - ❖ **Reject** (refuse message and return it to the sender) (default)
 - ❖ **Discard** (message is irrevocably lost)

5. Optionally, you can select the **Send Recipient(s) the following message** checkbox. You can change the **From, Subject, Message** text, and/or encoding as desired.
6. Click **OK** to save your changes.

Result: If you click **OK**, the **Objectionable Word List** page is updated to display the **Objectionable Word List** filter table, which shows the selected filter action for the Objectionable Word List filter. The filter is also listed on the **Content Filtering > Advanced** page and can be edited or deleted from that page.

If you click **Cancel**, your changes are not saved and the **Objectionable Word List** page is updated to show the previously-saved settings.

7. To change the filter action, click the **Edit** icon  in the filter table.
Result: The **Add/Edit Objectionable Word List** page displays. Click **OK** to apply changes; click **Cancel** to terminate the edit.
8. To delete the **Objectionable Word List** filter, click the **Delete** icon  in the filter table.
Result: A confirmation page opens; click **Delete** or **Cancel**.

Example Objectionable Word List Entries

Use the **Add/Edit List** area of the **Objectionable Word List Filter** page to create your own list. Below are example list entries for Objectionable Word List.

confidential: Specifically adds the word **confidential** to your Word filter list; any incoming mail containing that word is acted on as specified by the Word List filter action.

phooey: Specifically adds the word **phooey** to your Word filter list; any incoming mail containing that word is acted on as specified by the Word List filter action.



You cannot separate entries with spaces or semi-colons; each entry must be on a separate line. Therefore, you must make your entries one at a time. Wildcards are not accepted.

Filter Examples

The following sections describe different filters that are commonly defined, including word list filters.

regex Filtering to Modify the UCE Scoring

The `regex-matches` filter option matches against the regular expression you enter as the filter condition value. A regular expression is a way of representing data using symbols. You must enter a regular expression if you choose this filter content condition. For a good explanation of regular expressions, see [Posix Basic Regular Expressions](#).

You can use `regex-matches` in a filter to modify the UCE (spam) score that the anti-spam utility assigns to messages. The following filter increases the UCE score by 50 for all mail from “badCompany.com”:

Filter Name: regex-matches badCompany

If all of these conditions are met

From: regex-matches badCompany.*com

Modify UCE (junkmail) score by 50

Do not apply any more filters to this message if action is taken

In a received message header, if the strings "badCompany" and "com" occur separated by any number of characters the UCE (junkmail) score is increased by 50.

Filtering to Discard Messages Based on UCE Score

This filter discards all messages with a UCE score of 299 or greater and a sender not on a safelist. This is useful for preventing RAPID quarantining (the only available action) of spam messages:

Filter Name: UCE score greater than 299

If all of these conditions are met

UCE Score is greater than 299

AND (use More>> to add another condition)

X-Junkmail-Whitelist does not contain YES

Discard

Do not apply any more filters to this message if action is taken

Filtering to Quarantine Messages Based on UCE Score

This filter quarantines messages with a UCE score greater than 50 and senders not safelisted. By using a Quarantine Administrator address, these messages can be examined and released back to the mail stream.

Filter Name: quarantine suspect mail

If all of these conditions are met

UCE Score is greater than 50

AND (use **More>>** to add another condition)

X-Junkmail-Whitelist does not contain YES

Send to Quarantine folder user.UCEquarantineAdmin

Do not apply any more filters to this message if action is taken

Filtering to Discard Messages with Deleted Viruses

This filter discards messages from which a virus has been deleted.

Filter Name: discard deleted viruses

If all of these conditions are met

X-Mirapoint-Virus contains DELETED

Discard

Do not apply any more filters to this message if action is taken

Filtering Out “Virus Deleted” Messages

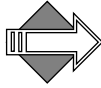
There are many new spamming viruses (for example, Sobig-F) that send themselves to addresses stored on an infected computer. Mirapoint's antivirus utility removes, cleans, or ignores the virus-infected attachment (depending on your antivirus configuration, see “Using Antivirus Scanning” on page 396), modifies the message to say what action was taken using the **X-Mirapoint-Virus** header, and sends the message on. To prevent users from seeing these messages that are often empty except for the antivirus-action-taken message, create a filter using the **Filter Conditions** option: **X-Mirapoint-Virus** header.



To filter virus-deleted message, one or more appliances in your messaging network must be licensed to perform signature-based antivirus detection (Sophos or F-Secure).

An example header of an antivirus-scanned, virus-infected message is:

```
X-Mirapoint-Virus: VIRUSDELETED;
host=spamcity.com;
attachment=[2.2];
virus=W32/Sobig-F
```



The **X-Mirapoint-Virus** actions can be either **VIRUSDELETED**, **VIRUSCLEANED**, or **VIRUSIGNORED**.

To create a filter to discard the antivirus-action-taken original messages with this specific virus header (sent by the W32/Sobig-F virus):

Filter Name: discard Sobig virus deleted messages
If all of these conditions are met
X-Mirapoint-Virus contains Sobig-F
Discard
Do not apply any more filters to this message if action is taken

To filter out all flavors of the Sobig virus, you can use wildcards in the filter:

Filter Name: discard Sobig virus deleted messages
If all of these conditions are met
X-Mirapoint-Virus matches *Sobig*
Discard
Do not apply any more filters to this message if action is taken

As new viruses appear, they can be added to the filter using the **More>>** button in the **Filter Conditions** area.

Alternatively, you could create a filter that with the condition *X-Mirapoint-Virus contains VIRUS* to delete all infected messages, regardless of whether or not they were cleaned.

Filtering "Keep" Use Examples

The **Keep (process normally)** option is most useful in two scenarios:

- ◆ Matching messages should be forwarded to a folder and a copy sent to the specified recipients. To do this you must configure two filters:
 - ❖ Filter One would have these actions:
Forward to: some folder

Do not apply any more filters to this message if action is taken DE-SELECTED.

- ❖ Filter Two would have the same conditions as Filter One, and these actions:

Keep (process normally)

Do not apply any more filters to this message if action is taken SELECTED.

In this way, matching messages would be forwarded to the folder specified in Filter One, and Filter Two would direct a copy to the specified recipients; also, no more filters would be applied.

- ◆ Matching attachments should be removed and the messages sent to the specified recipients. To do this use the **Keep (process normally)** option in conjunction with the **Remove attachments that meet attachment conditions** option. In this way, messages with attachments matching the filter condition would be sent to the specified recipients after the attachments are removed.

Filtering Out All jpegs Using Body(Binary)

To filter out all jpeg files, including those improperly defined in the MIME type or extension (commonly done in spam), you could use a filter like this;

Filter Name: Discard Jpegs

If all of these conditions are met

X-Body(Binary) contains 0xFFD8

AND (use **More>>** to add another condition)

X-Body(Binary) contains 0x4A46494600

Discard

Do not apply any more filters to this message if action is taken



Security Tasks

This chapter discusses Mirapoint security features, the use of MailHurdle, Anti-Virus and Anti-Spam options, and the Junk Mail Manager interface. The following topics are included:

- ◆ [Using Security Features](#): How the security features work including flowcharts on processing.
- ◆ [Working with MailHurdle](#): How to use MailHurdle® including preparing for deployment and all configuration options.
- ◆ [Using Antivirus Scanning](#): How to use the antivirus options available to you.
- ◆ [Using Antispam Scanning](#): How to use the antispam options including Allowed Senders, Blocked Senders, and so forth.
- ◆ [Configuring NIC Failover](#): How to allow an appliance to seamlessly switch to a second network connection if the first one fails.
- ◆ [Using Security Quarantine](#): How to use the various quarantine options that Mirapoint offers.

An important security tool, Junk Mail Manager is discussed in detail in [Chapter 10, “Using Junk Mail Manager \(JMM\).”](#)

Using Security Features

Security implementation tasks are presented in this section. There are four areas of security to consider: network security, inbound message handling, message content control, and outbound message handling.

Network Security

Figure 66 summarizes the network security layer.

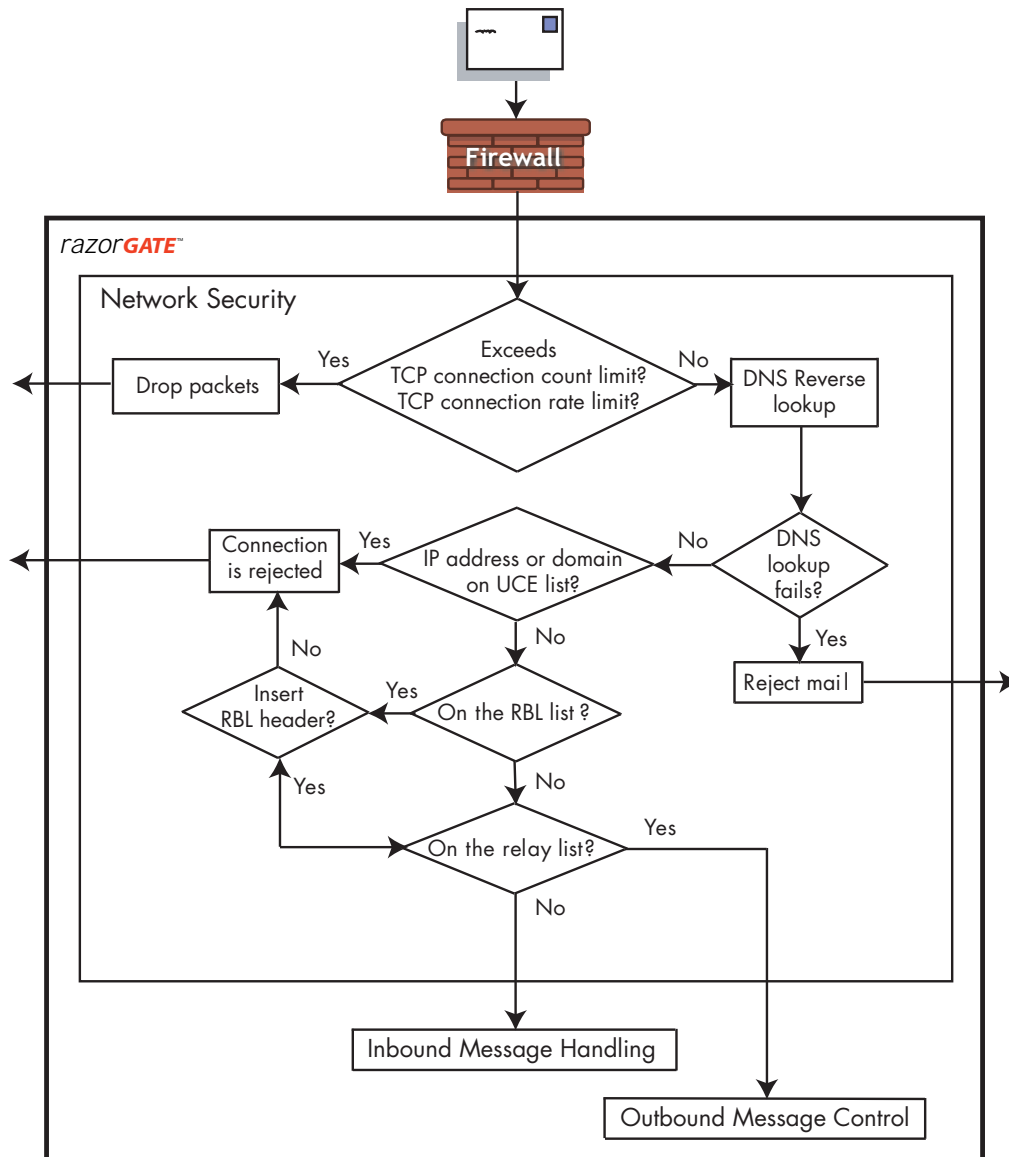


Figure 66 Network Security Layer

The network security layer is the first line of defense against attacks on your messaging system. Reverse DNS Verification can be performed without any custom configuration. Blocklist and RBL checking need to be configured for your particular deployment. You can also configure relay domains if you need to permit selected IP addresses or domains to relay messages through your network.

You can use the Administration Suite to configure the following network security functions:

- ◆ **Blocked domains:** You can automatically reject all mail from certain IP addresses or domains; see [“Updating Blocked Domains \(Reject List\)” on page 435](#) for details.
- ◆ **Relay domains:** To prevent open relaying (unwanted use of your network), specify which IP addresses or domains can use your network; see [“Updating Relay Domains \(Relay List\)” on page 434](#) for details.
- ◆ **Realtime Blackhole List (RBL):** You can make use of various services on the Internet keeping track of spamming domains; see [“Updating Your Realtime Blackhole List \(RBL\)” on page 437](#) for details.

Inbound Message Handling

Figure 67 summarizes the inbound message handling layer.

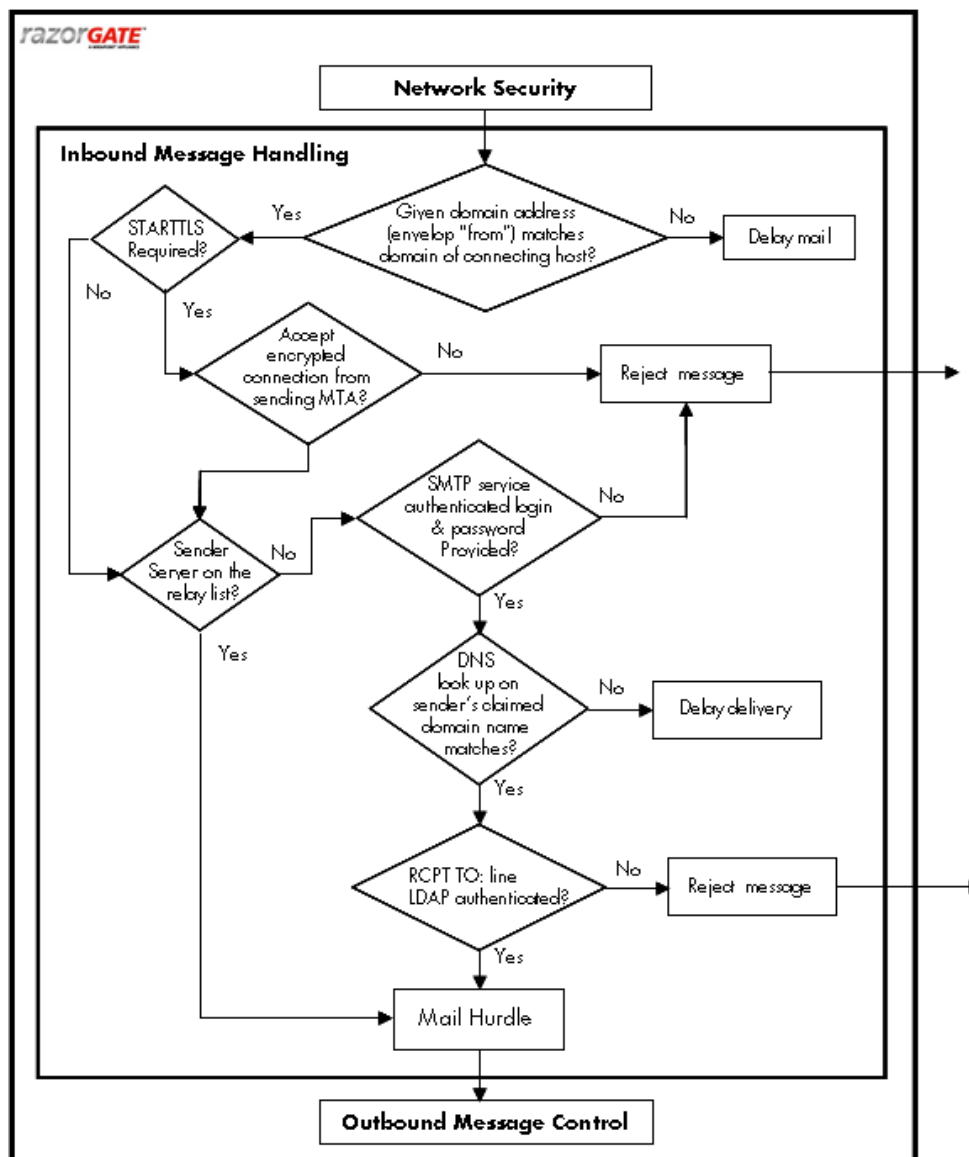


Figure 67 Inbound Traffic Handling Layer

Security features for inbound message handling include the following:

- ◆ **TLS encryption:** Uses encryption for added privacy of messages. This is set using the **System > Services > SMTP > Main Configuration** “Allow STARTTLS (Inbound Connections)” option.
- ◆ **SMTP authentication:** Requires that all users connecting to the mail service must be authenticated. This is set using the **System > Services > SMTP > Main Configuration** “Require Secure Authentication (SSL)” option
- ◆ **SMTP sender check:** Requires that the sender has a valid domain. This is set using the **System > Services > SMTP > Main Configuration** “Reject Messages from Unknown Senders” option.
- ◆ **Sender Address Rewrite:** With LDAP masquerade enabled, the **From** address can be rewritten to match the authenticated sender, and a policy requiring that the sender be the same as the authenticated user can be enforced to prevent outbound spamming. This is set using the **System > Services > SMTP > Main Configuration** “Re-write From Address based on Authentication” option.
- ◆ **SMTP recipient check:** Requires that mail recipients be valid users. This is set using the **System > Services > SMTP > Main Configuration** “Reject Messages for Unknown Recipients” option.
- ◆ **MailHurdle:** Uses an antispam technique that automatically weeds out likely spam mail. See [“Working with MailHurdle” on page 388](#) for more information.
- ◆ **Wire Taps:** Sends a copy of all mail to or from a certain sender to a mailbox where it can be examined; see [“Using Wire Taps” on page 349](#) for details.
- ◆ **User and Admin Audit:** Displays all activity (mail traffic, filters, logins, and commands) on a per-user or per-administrator basis. See [“Viewing User and/or Administrator Activity” on page 251](#) for details.

Message Content Handling

Figure 68 summarizes the message content control layer.

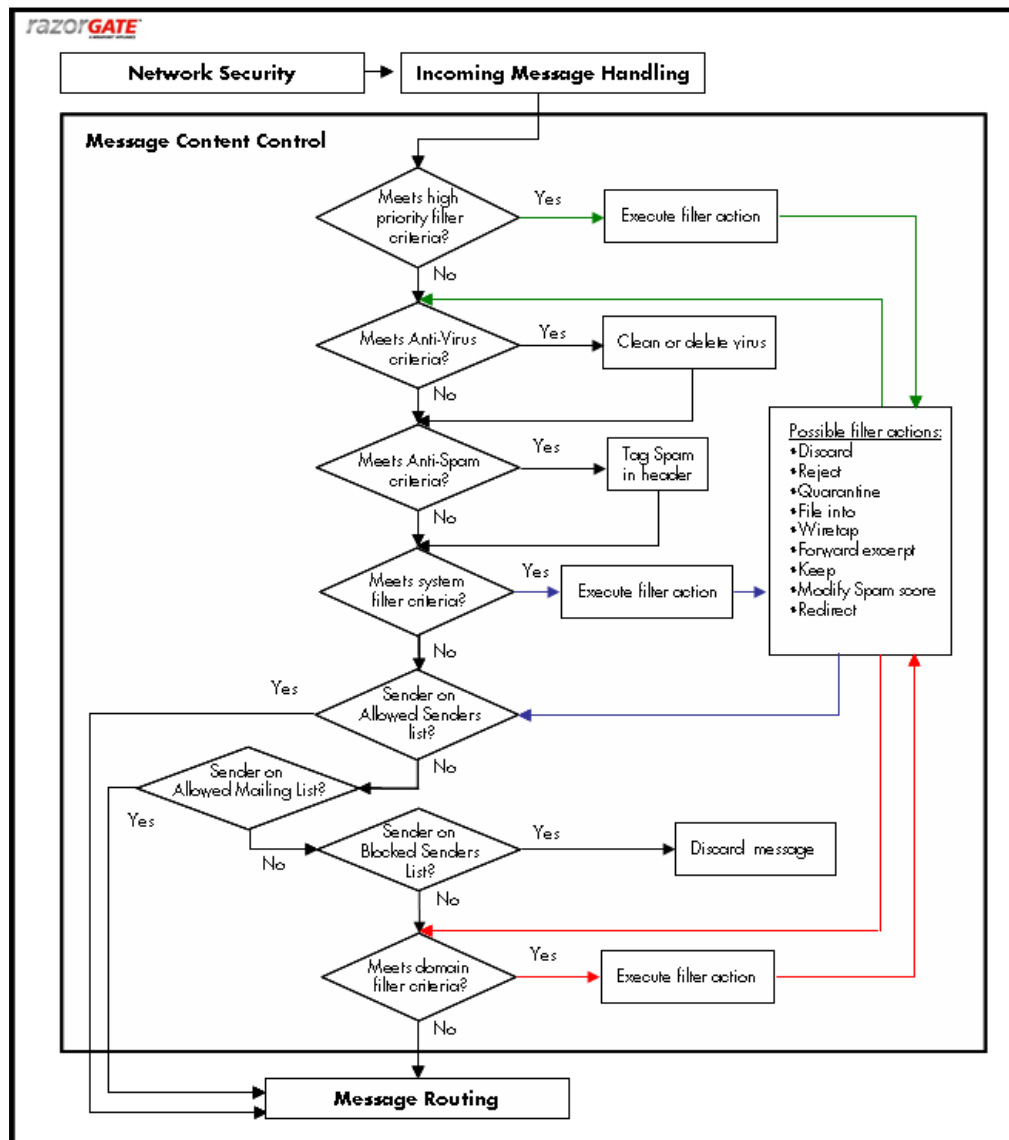


Figure 68 Message Content Control

There are many facilities that you can use to control message content; these include the following:

- ◆ **High Priority Message Filters:** These filters are performed before antivirus or antispam scanning; see [“About Filter Priorities and Ordering” on page 333](#) for details.
- ◆ **Antivirus scanning:** Configure up to three antivirus engines to keep viruses out; see [“Using Antivirus Scanning” on page 396](#) for details.
- ◆ **Antispam scanning:** Configure basic antispam scanning and additional antispam facilities such as
 - ❖ **Allowed Senders:** Senders, users or entire domains whose mail should not be subject to antispam scanning.
 - ❖ **Blocked Senders:** Users or entire domains whose mail should always be categorized as spam.
 - ❖ **Allowed Mailing Lists:** Recipients, users or entire domains, whose mail should not be subject to antispam scanning.
- ◆ **Domain Message filters:** These filters operate on all mail incoming to a particular domain or set of domains; see [“Managing Content Policies \(Domain Filters\)” on page 332](#) for details.
- ◆ **WebMail Session IDs:** In WebMail and Calendar, the HTTP session ID is exposed in the URL by default. Users sometimes copy and paste the URLs with their session IDs into email, unintentionally enabling recipients to access their mail folders and account. To prevent this, set the **Cookies: Required** option on the **System > Services > HTTP > Main Configuration** page. This secures user information by requiring cookies for all sessions.

Outbound Message Handling

Figure 69 summarizes the outbound message control layer.

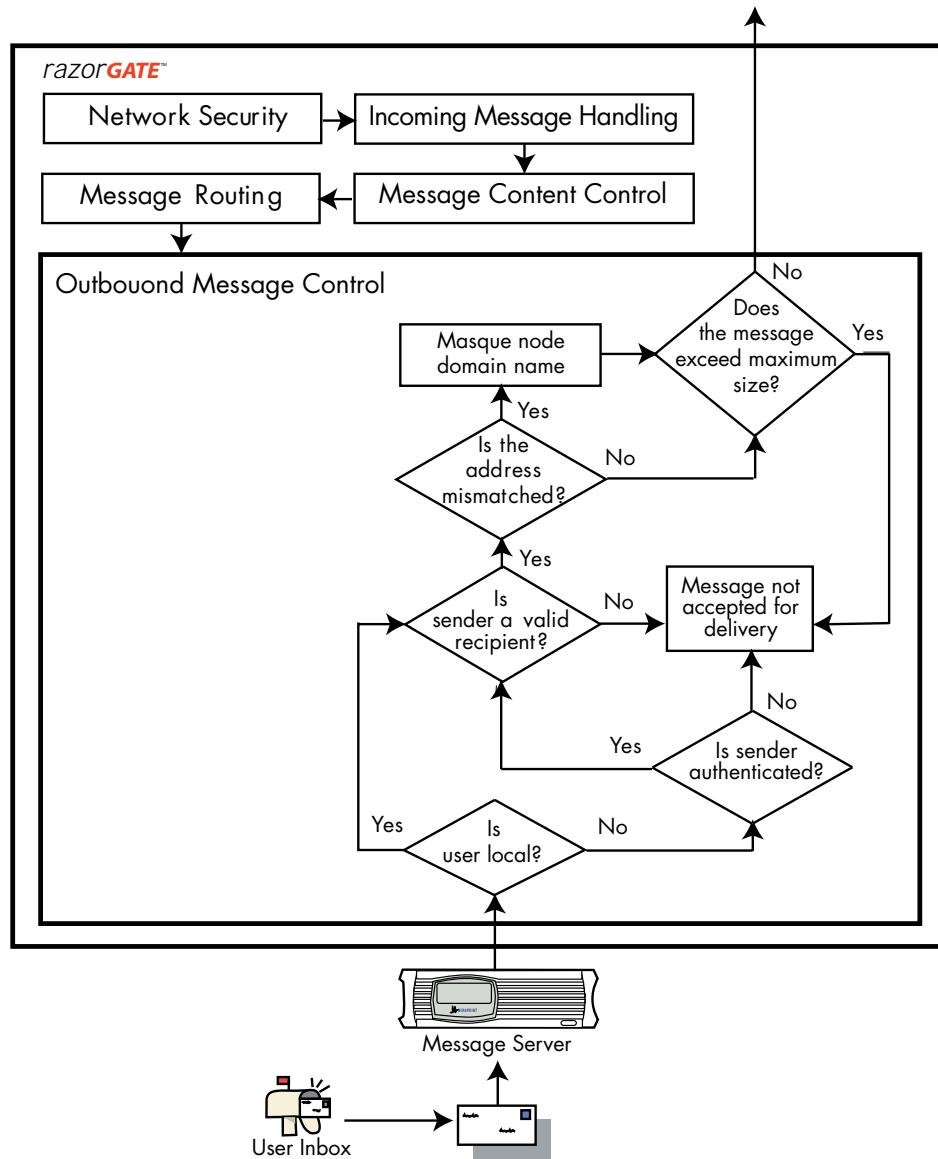


Figure 69 Outbound Message Control Layer

Outbound Message Control includes the following:

- ◆ **User Authentication for SMTP:** The outbound router can require that users be authenticated, often by a prior mail-reading connection, before being permitted to send messages; this is set using the **System > Services > SMTP > Main Configuration** “Require Secure Authentication (SSL)” option.
- ◆ **Sender Normalization to Smtpath:** To reduce the likelihood of forged headers being sent from inside your organization, it is best to normalize user names in the **From** header to the login name as verified by Smtpath; this is set using the **System > Services > SMTP > Main Configuration** “Re-write From Address based on Authentication” option.
- ◆ **SMTP recipient check:** To reduce the likelihood of forged email being sent from inside your organization, some sites like to check that the sender is a valid recipient with an LDAP lookup; this is set using the **System > Services > SMTP > Main Configuration** “Reject Messages for Unknown Recipients” option.
- ◆ **Sender Masquerade Address:** Most large organizations have users scattered over multiple computers with different hostnames. Some users transmit email from systems on a totally unrelated network. For reasons of security and compatibility, it is best for outgoing mail to appear as if it originates from a single organization. This is often done by setting a “masquerade” for the **From** domain, the address part after @ (at-sign). **Senderisauth** normalizes the user name, while **masquerade** normalizes the domain name. You set masquerade with the **System > Services > SMTP > Main Configuration** “Masquerade all messages as this domain” option.
- ◆ **Maximum Message Size:** If network load is too high, or users complain, you can control the maximum message size that SMTP service allows. Larger messages are rejected. The default maximum is 30 MB (31,457,280 bytes) but you can set this limit lower, or higher up to 128 MB (134,217,728 bytes). Do this using the **System > Services > SMTP > Main Configuration** “Maximum Message Size” option.

Working with MailHurdle

MailHurdle sits at the edge of the messaging network and screens messages from unrecognized senders. When messages are received, MailHurdle caches three pieces of mail data:

- ◆ Remote Server Peer (IP) Address
- ◆ Sender (Envelope From) Address
- ◆ Recipient (Envelope To) Address

This *triplet* is used to determine whether or not the sender is recognized (has sent messages to the recipient before). If not, MailHurdle sends a standard SMTP error code that means “you should retry this address later.” Properly configured mail servers do just that—but most spam sources don’t retry failed messages. Figure 70 summarizes MailHurdle processing during inbound message handling.

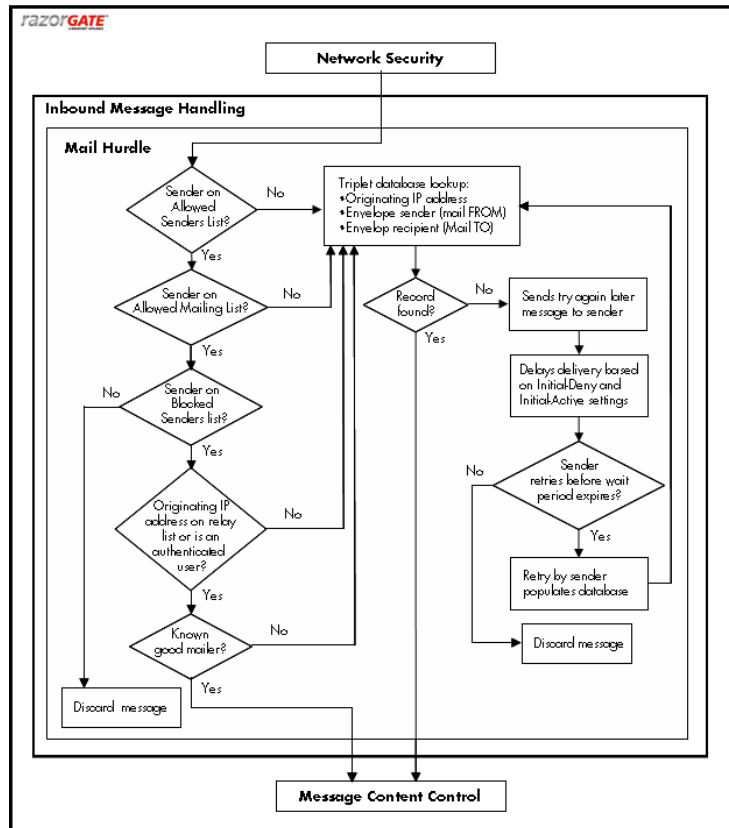


Figure 70 MailHurdle Processing for Inbound Messages

Modifying MailHurdle

Use the **Anti-Spam > MailHurdle > Configuration** page (shown in Figure 71) to modify your MailHurdle utility. You can change the server specified to perform the function, and the default time-outs for the three phases of caching triplets.

Configuration

Use this page to configure MailHurdle servers, timeout periods, and server cache.

MailHurdle is currently **enabled**. [Disable It](#)
 (Warning: Enabling MailHurdle may cause occasional mail delays to critical e-mail. [MailHurdle FAQ](#))

MailHurdle Server:
[Add](#)

No items in list

Set Triplet Timeouts

Triplets are the three pieces of mail data; **Remote Server Peer (IP) Address**, **Sender (Envelope From) Address**, and **Recipient (Envelope To) Address**, that MailHurdle caches while waiting for a retry after it "tempfailed" the message. Use the timeout options to set how long MailHurdle waits during the three stages of the process.

Initial-Deny:

An **Initial-Deny** triplet is one that has been "tempfailed" (an error code has been returned to the sender). No retries or new mail from this triplet may be accepted until after the time period you specify (then the triplet becomes **Initial-Active**).

Initial-Active:

An **Initial-Active** triplet is one that may now change status; either to **Active** (a retry is accepted) or **Initial-Expired** (no retry is accepted) before the time period you specify ends. If a retry for an **Initial-Expired** triplet arrives, the triplet is returned to an **Initial-Deny** state.

Active:

An **Active** triplet is one that has had a retry accepted by the system; during this time period all mail from that triplet is accepted. Each new accepted message resets the **Active** timeout counter; otherwise, the triplet is **Expired** after the time period you specify. If a retry for an **Expired** triplet arrives, the triplet is returned to an **Initial-Deny** state.

[Set](#)

Figure 71 MailHurdle Configuration Page

To modify basic MailHurdle settings, follow these steps on the **MailHurdle > Configuration** page; see Figure 71 for an example.

1. Specify a **MailHurdle server** and click **Add**. This is the machine that performs the MailHurdle caching. Default is the local host.
2. Set **Triplet Timeout** options (Note: These options do not display if MailHurdle is not enabled):
 - ❖ **Initial Deny** (default is 5 minutes): An **Initial-Deny** triplet is one that has been "tempfailed" (an error code has been returned to the sender). No retries or new mail from this triplet can be

accepted until after the time period you specify (then the triplet becomes **Initial-Active**).

- ❖ **Initial Active** (default is 1 day): An **Initial-Active** triplet is one that can now change status; either to **Active** (a retry is accepted) or **Initial-Expired** (no retry is accepted) before the time period you specify ends. If a retry for an **Initial-Expired** triplet arrives, the triplet is returned to an **Initial-Deny** state.
- ❖ **Active** (default is 36 days): An **Active** triplet is one that has had a retry accepted by the system; during this time period all mail from that triplet is accepted. Each new accepted message resets the **Active** timeout counter; otherwise, the triplet is **Expired** after the time period you specify. If a retry for an **Expired** triplet arrives, the triplet is returned to an **Initial-Deny** state.

3. Click **Set**.

Result: MailHurdle caches the received triplets as specified, beginning immediately. As MailHurdle begins to cache triplets, there is an initial slow-down in mail delivery that should diminish over time.

MailHurdle and SMTP Authentication

MailHurdle is not enforced for mail from an authenticated SMTP connection to a local user, such mail is treated as local-local.

MailHurdle is enforced for mail from a non-authenticated SMTP connection to a local user.

MailHurdle is enforced for mail from an authenticated SMTP connection to a remote user (relaying), depending on the status of the **Inbound Mail Only** option on the **MailHurdle > Advanced** page. If this option is selected (default), authentication is not enforced. If this option is de-selected, authentication is enforced.

Adding and Deleting MailHurdle Allowed Hosts

Use the **Anti-Spam > MailHurdle > Allowed Host** page (see Figure 72) to specify which machines can query the MailHurdle server; each machine with the MailHurdle service should be an Allowed Host.

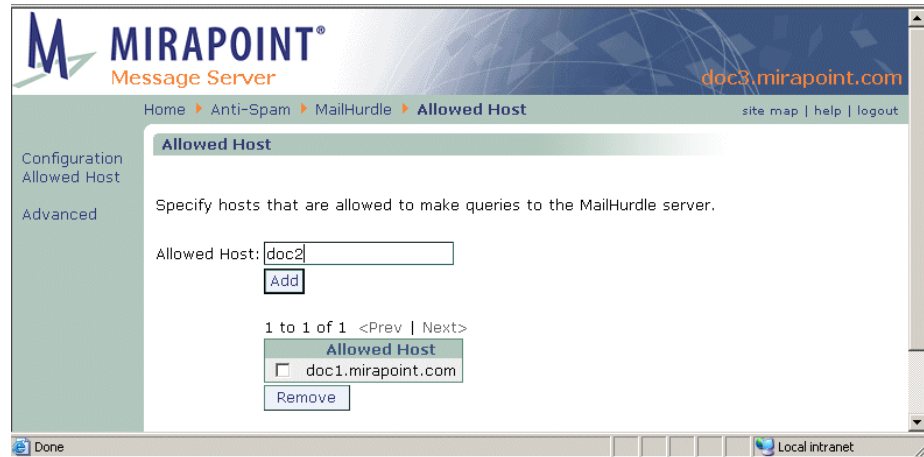


Figure 72 MailHurdle Allowed Hosts Page

To add or delete MailHurdle allowed hosts, enter the hostname of all your machines that need to communicate with your MailHurdle server; click **Add** for each entry. The local host is allowed by default.

Result: A table displays your list of allowed hosts. Use the checkbox and **Remove** button to delete hosts from the list.

Setting Advanced MailHurdle Configuration Options

Use the **Anti-Spam > MailHurdle > Advanced** page (see Figure 73) to set filtering prioritization and other options, and also to search for triplets or manually flush the triplet cache.

Advanced

Set Advanced Options

Prioritize Allowed Senders
Immediately pass mail through if the sender is on the primary domain's Allowed Senders List.

Prioritize Blocked Senders
Immediately classify the message as junkmail if the sender is on the primary domain's Blocked Senders List.

Prioritize Allowed Mailing Lists
Immediately pass mail through if the recipient is on the primary domain's Allowed Mailing List.

Prioritize Relay List
Immediately pass mail through if the remote server is on the relay list.

Allow Known Good Mailers
Immediately pass mail through if the sender is on the MailHurdle (system-maintained) known good mailers list.

Allow Null Sender
Immediately pass mail through if the sender is <>.

Inbound Mail Only
Apply MailHurdle to inbound mail only.

Cache MX record
Cache MX record (if available) instead of triplet IP address.

Accept All Triplets Based on "Active" IP Address
Once a triplet is **Active**, pass through all mail from that **Remote Server Peer (IP) Address**. To have all triplets checked always, deselect this option on each MailHurdle server and client.

Apply

Check Mail Delivery Triplets for Message

Remote Server Peer (IP) Address:

Sender (Envelope From) Address:

Recipient (Envelope To) Address:

Check

Flush Delivery Triplets

Manually flush the mail delivery triplets in MailHurdle server cache.

Warning! Flushing all triplets removes currently active triplets and restarts the MailHurdle process for all incoming mail. This will result in mail delivery delays.

Flush Expired Triplets Flush All Triplets

Recommend selecting this option

Leave this option deselected if any of your users use POP

Recommend selecting this option

Recommend leaving these settings at default

Monitor the affect of this option

Figure 73 MailHurdle Advanced Page, Detail

Select from these MailHurdle message handling options:

- ◆ **Prioritize Allowed Senders** (deselected by default). Ensures that mail from a sender on your Allowed Senders list does not get delayed by MailHurdle. Selecting this option is recommended.

- ◆ **Prioritize Blocked Senders** (deselected by default). Applies your set Blocked Senders list action immediately to mail from those senders without utilizing MailHurdle. Leaving this option deselected is recommended if any of your users can use POP.
- ◆ **Prioritize Allowed Mailing Lists** (deselected by default). Ensures that mail addressed to recipients on your Allowed Mailing Lists list is delivered without MailHurdle delays. Recommend selecting this option.

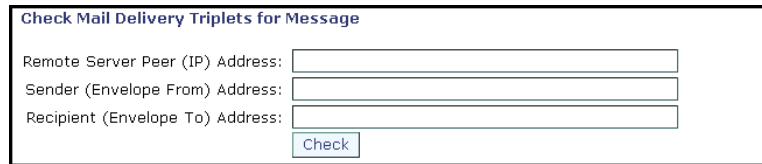
It is recommended that the remaining options be left in their default state.

- ◆ **Prioritize Relay List** (selected by default). Ensures that mail being routed through the system from servers on your relay list is not subject to MailHurdle delays.
- ◆ **Allow Known Good Mailers.** (selected by default) Allows delivery of messages sent from known “good-mailers” who don’t respond correctly to the MailHurdle “try me later” message. The list of good-mailers is maintained by the antispam community at large and is periodically updated. You can schedule automatic updates of this list using the Anti-Spam Updates page, for details see [“Scheduling Updates for Anti-Spam Scanning” on page 422](#).
- ◆ **Allow Null Sender** (selected by default). Provides for the corner case where mail is sent with no information for the **Sender** header.
- ◆ **Inbound Mail Only** (selected by default). Specifies that MailHurdle should only process inbound mail. When this option is selected, delivery of outbound mail is not affected by MailHurdle processing.
- ◆ **Cache MX record** (selected by default). Caches the MX record instead of the IP address. This is useful to avoid delaying mail from senders that send mail through multiple systems (with different IP addresses).
- ◆ **The Accept All Triplets Based on “Active” IP Address** option cuts down on MailHurdle delays. Once a triplet achieves the “Active” state, all mail coming from the IP address of that triplet is accepted (the Sender and Recipient addresses are ignored).

Click **Apply** to enter your settings.

Checking Mail Delivery Triplets for Messages

You can use the **MailHurdle > Advanced** page to search for particular triplets in the triplet cache (see Figure 74). This can be useful if you're trying to diagnose what happened to a message that a user was expecting, but did not receive.



Check Mail Delivery Triplets for Message

Remote Server Peer (IP) Address:

Sender (Envelope From) Address:

Recipient (Envelope To) Address:

Figure 74 MailHurdle Check for Message Advanced Page Detail

To search the triplet cache:

1. Enter the following information (all three parts of the triplet are required):
 - ❖ **Remote Server Peer (IP) Address:** The IP address of the sender's mail server.
 - ❖ **Sender (Envelope From) Address:** The envelope from sender header.
 - ❖ **Recipient (Envelope To) Address:** The envelope to recipient header.
2. Click **Check** to scan the triplet cache for a corresponding entry.

Result: If the information matches a triplet in the cache, the triplet information is displayed, including its state and expiration time.

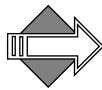
For information about message headers, see [“Reading Message Envelopes and Headers” on page 235](#).

Flushing Mail Delivery Triplets

You can manually flush the triplet cache from the **MailHurdle > Advanced** page, shown in Figure 75.



Figure 75 MailHurdle Flush Triplets Advanced Page Detail



It is not normally necessary or desirable to manually flush the cache in a production environment. Flushing the entire cache causes the MailHurdle process to start over with new incoming mail and can cause delays in mail delivery while the cache is repopulated.

There are two options for flushing the cache:

- ◆ **Flush Expired Triplets:** Only those triplets that are not in an **Initial Deny**, **Initial Active**, or **Active** state are flushed. All triplets still being processed are left in the MailHurdle queue.
- ◆ **Flush All Triplets:** All triplets regardless of state are flushed. The MailHurdle process begins again with new incoming mail; triplets that had been passed to an **Active** state return to **Initial Deny** until passed again.

Using Antivirus Scanning

The Anti-Virus scanning utility can search for viruses in incoming and outgoing messages. Messages are scanned before leaving the mail queue. Anti-Virus scanning is done after 100 level filters are applied and before 450 level filters.

Antivirus scanning must be licensed for each appliance in the message stream that needs to search for viruses. For example, to scan outbound messages as well as inbound messages, the Outbound Message Router must have an Antivirus license.

The scanner can use three different engines to search for viruses: Sophos™, or F-Secure™, and RAPID™. Which antivirus scanners are available to you depends on which licenses you have applied. Each engine has its own configuration pages. Task procedures are given in [“Modifying Signature-based Anti-Virus” on page 399](#) and [“Modifying Predictive-based \(RAPID\) Anti-Virus” on page 409](#).



Mirapoint recommends using RAPID along with one of the signature-based antivirus engines (Sophos or F-Secure).

About the Anti-Virus Engines

How many Anti-Virus engines are available to you depends on your licensing. Mirapoint offers three antivirus solutions; two, Sophos and F-Secure, use a signature-based method, one, RAPID®, uses a predictive-base method. These methods are discussed in this section.

About Signature-Based Anti-Virus

Both Sophos and F-Secure use a “signature” based methodology. When a virus appears on the Internet, it is observed and classified as such as rapidly as possible; in general, it takes between 4 to 24 hours for a new virus to be classified. Once the virus is classified, it is added to the pattern files (databases) of the service. This is why it is important to schedule pattern file updates to occur as frequently as possible.

About Predictive-Based Anti-Virus

RAPID Anti-Virus uses an entirely different methodology called “predictive.” RAPID does not attempt to identify viruses that appear on the Internet as do Sophos and F-Secure. Instead, RAPID identifies suspicious activity, based on sending IP addresses, that might indicate a virus outbreak. This identification usually takes place in 30 seconds to 2 minutes after a virus appears. RAPID AV does not use a pattern file but requires a periodic engine update to counter emerging threats.

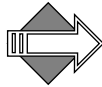
Because RAPID does not attempt to verify that potential virus outbreaks are, in fact, viruses, the only action option for RAPID AV is quarantine. An administrator with the Quarantine Administrator role,

may those messages quarantined by RAPID to make sure that they are truly viruses.

About Cleanable vs. Non-cleanable Viruses

Anti-Virus scanning configuration requires making specifications for actions to be taken on infected attachments, non-cleanable infected attachments, and selecting a **Quarantine E-mail Address**.

Virus scanning software distinguishes between two major types of viruses: **cleanable** and **non-cleanable**. A cleanable virus is one that can be removed from an attachment, document, or program without damaging the attachment, document, or program. Examples of this type are the macro viruses written in Microsoft Word or Excel macro language. Some other viruses such as W32/Magistr-A, and some old DOS viruses also are considered cleanable. If a virus is not one of the above, it is considered non-cleanable. In this case, the only way that the message can be made safe is to remove the virus, whether it is the entire attachment or the message body itself. The virus scanner uses pattern files that classify viruses as cleanable or non-cleanable. The system tries to automatically clean cleanable viruses if you select one of the **Auto Clean** options.



Cleaning a virus also invalidates any digital signature attached to the message.

How Antivirus Quarantine Works

The antivirus quarantine typically works differently than the content filtering quarantine. The address you specify as the **Anti-Virus Quarantine E-mail Address** receives messages that potentially contain live viruses. Messages quarantined by the signature-based scanners contain live viruses. They can be examined and deleted, but should not be released from the quarantine. Messages quarantined by RAPID antivirus potentially contain live viruses and can be released for re-scanning by one of the signature-based scanners. The **Anti-Virus Quarantine E-Mail Address** should either be a local address or an address that does not subject the message to more antivirus scanning.

For signature-based antivirus engines, the Quarantine E-Mail Address does not need to be for an account with the **Quarantine Administrator** role. You never want to release an infected message back to the mail queue.

For RAPID antivirus (a predictive-based engine) it is essential that you quarantine messages to an account that has the **Quarantine Administrator** role. A quarantine administrator may examine all messages quarantined by the RAPID antivirus scanner and possibly return selected messages to the mail stream via the Quarantine Administrator's WebMail **Deliver** and/or **Virus Scan** actions; this should be done after a time period that allows for the updates of your signature-based antivirus engines. For example, if your signature-based antivirus engine(s) are set to update every hour, to allow for the updates to install (and include relevant new virus data), releasing RAPID-quarantined messages should be done no earlier than six hours after the message was first quarantined. In this way, the signature-based engines have time to discover the virus, add it to their database, and your system has time to install the update. Automatic release of RAPID-quarantined messages occurs eight hours after quarantining; this can be changed using the CLI. See **Help About Antivirus**.

Any WebMail user can be assigned the **Quarantine Administrator** role and log in to the Quarantine Administrator's WebMail. For more information about Quarantine Administration, see [“About the Quarantine Administrator User” on page 289](#).



When using the quarantine filter action, it is best to use a local address to prevent the mail from getting re-scanned.

Modifying Signature-based Anti-Virus

Use the Anti-Virus **Sophos™** and **F-Secure™** pages to modify your configured signature antivirus engines, including setting up notifications and updates. To better understand how Sophos and F-Secure AV work see [“About Signature-Based Anti-Virus” on page 397](#).



It is recommended that RAPID and one signature-based antivirus engine run at the edge and one signature-based engine run at the core.

Sophos and F-Secure antivirus scanning configuration require making specifications for actions to be taken on infected attachments, non-cleanable infected attachments, and specifying a **Quarantine E-mail Address**.

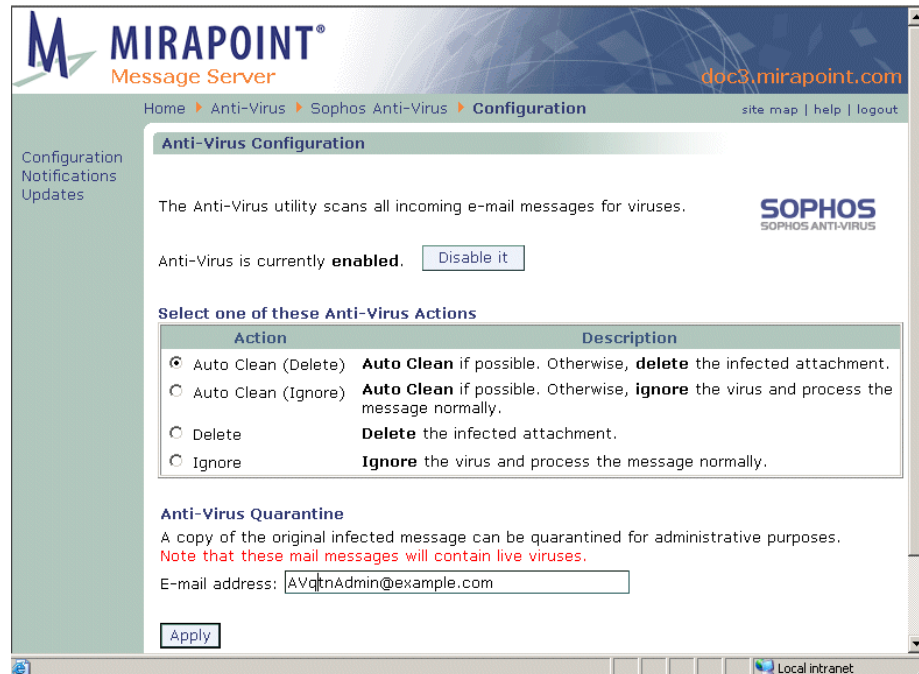


Figure 76 Anti-Virus Signature Engine Configuration Page

To configure Sophos or F-Secure antivirus scanning, follow these steps on the **Anti-Virus > Sophos > Configuration** or **Anti-Virus > F-Secure > Configuration** page.

1. Make sure the antivirus scanner is enabled. (If it is currently disabled, click the **Enable it** button.)
2. In the **Select one of these Anti-Virus Actions** area, choose one of the following settings:
 - ❖ **Auto Clean (Delete)** (default) (recommended): The system attempts to clean the attachment of the virus; if the attachment cannot be cleaned, it is deleted. The system logs that a virus was

found and sends the message with the attachment either cleaned or deleted, to the intended recipient(s).

- ❖ **Auto Clean (Ignore):** The system attempts to clean the attachment of the virus; if the attachment cannot be cleaned, it is ignored. The system logs that a virus was found and sends the message with the attachment either cleaned or unchanged, to the intended recipient(s). This option is not recommended.
- ❖ **Delete:** The system logs that a virus was found and sends the message with the attachment deleted, even if cleanable, to the intended recipient(s).
- ❖ **Ignore:** The system logs that a virus was found and sends the message with the attachment unchanged to the intended recipient(s). This option is not recommended.

Optionally, you can specify an antivirus quarantine **E-mail Address** of an administrator account local to the system. See [“How Antivirus Quarantine Works” on page 398](#) for information. If you use this option, a copy of the infected message is sent to the specified address, regardless of which **Anti-Virus Action** you specify.

3. Click **Apply**.

Result: The system acts as specified when viruses are found. In all cases, the original message is modified with a header (**X-Mirapoint-Virus**) and a warning banner indicating that a virus was found and what action was taken (“cleaned”, “ignored”, or “deleted”); the message includes the virus name, you can go to <http://www.sophos.com> or <http://www.f-secure.com> to learn more about that virus. See [“About Cleanable vs. Non-cleanable Viruses” on page 398](#) for information on cleanable viruses. If you specified a **Quarantine E-mail Address**, your selected actions are taken and any message found to contain a virus is forwarded to the specified address.

Setting Notifications for Sophos and F-Secure Anti-Virus



Anti-Virus notifications must be specified for notices to be sent to the correct parties.

For signature-based antivirus engines, notifications are not recommended on the grounds that the viruses found are proven viruses.

This is not the case with RAPID antivirus where setting notifications is highly recommended.

Configuration
Notifications
Updates

Home ▸ Anti-Virus ▸ Sophos Anti-Virus ▸ Notifications site map | help | logout

Anti-Virus Notifications

Choose a notification message to edit
 Virus-alerts | Sender | Recipient(s) | Summary | Deleted

Send this notification to the virus-alerts distribution list when a virus is found.
 This notification is currently **disabled**.

From: administrator

Subject: Virus Warning

Message: The %v virus was detected in attachment (%F) in email from %f to %t.
 Action taken: %a

Unicode (UTF-8)

%aa=Action taken %od=Date %of=Sender
 %oF=Attachment file name %oh=Mail server hostname
 %oi=Attachment index %op=Attachment problem %ot=Recipient
 %ov=Virus name

Powered By Local intranet

Click here to set which type of notification you want

This text changes depending on which type of notification you choose

Figure 77 Anti-Virus Signature Engine Notifications Page

The following graphics depict the various notification messages that can be configured.

Send this notification to the message sender when a virus is found.

This notification is currently **disabled**.

From:

Subject:

Message:

Unicode (UTF-8)

%a=Action taken %d=Date %f=Sender
 %F=Attachment file name %h=Mail server hostname
 %i=Attachment index %p=Attachment problem %t=Recipient
 %v=Virus name

Figure 78 Anti-Virus SENDER Message, Notification Page Detail

Insert this summary at the top of the infected e-mail when a virus is found.

Message:
 The following message attachments were flagged by the antivirus scanner:
 Attachment [%i] %F, %p: %v. Action taken: %a"/>

Unicode (UTF-8)

%a=Action taken %d=Date %f=Sender
 %F=Attachment file name %h=Mail server hostname
 %i=Attachment index %p=Attachment problem %t=Recipient
 %v=Virus name

Figure 79 Anti-Virus SUMMARY Message, Notification Page Detail

Insert this warning message in place of a deleted infected attachment.

Message: VIRUS WARNING Message (from %h)

The virus %v was detected in email attachment [%i] %f. The infected attachment has been deleted.

Unicode (UTF-8)

%a=Action taken %d=Date %f=Sender
 %F=Attachment file name %h=Mail server hostname
 %i=Attachment index %p=Attachment problem %t=Recipient
 %v=Virus name

Apply Restore to Default

Figure 80 Anti-Virus DELETED Message, Notification Page Detail

To specify antivirus scanning notifications follow these steps on the **Anti-Virus > Sophos > Notifications** OR **Anti-Virus > F-Secure > Notifications** page, respectively.

1. Choose which notification message to edit by clicking one of the links at the top of the page (detail shown above in Figure 78):
 - ❖ **Virus Alerts** (default): When a virus is detected, this notification is sent to the **virus-alerts** distribution list. See Figure 77 for an example. This messages might look like this:
 “The Sobig virus was detected in attachment “Something.vbs.” in email from Sender@viruscity.com to User@example.com.
 Action taken: Deleted.”
 - ❖ **Sender**: When a virus is detected, this notification is sent to the message sender (“From” header). See Figure 78 for an example. This message might look like this:
 “The message you emailed to User@example.com, dated 04/21/2006, contains the Sobig virus in the “Something.vbs” attachment.
 Action taken: Deleted.”
 - ❖ **Recipient(s)**: When a virus is detected, this notification is sent to the message recipient(s). The default for this message is identical to the default for the **Virus Alerts** message. This message might look like this:
 “The Sobig virus was detected in attachment “Something.vbs” in email from Sender@viruscity.com (04/21/2006).
 Action taken: Deleted.”

Use the last two options to customize what's inserted in the message for the filter actions:

- ❖ **Summary:** When a message containing a virus is delivered with the virus cleaned or passed (either **Auto Clean (Ignore)** or **Ignore** was the action) this notification is inserted at the top of the body of the message. See Figure 79 for an example. This message might look like this:

“WARNING!!! (from mirapoint.com)

The following message attachments were flagged by the antivirus scanner:

Attachment [125634] “Something.vbs”, Infected: Sobig.
Action taken: Deleted”

- ❖ **Deleted:** When a message containing a virus is delivered with either the **Auto Clean (Delete)** or **Delete** was action taken, this notification is inserted in place of the deleted attachment. See Figure 80 for an example. This message might look like this:

“VIRUS WARNING Message (from mirapoint.com)

The virus Sobig was detected in email attachment [125634] “Something.vbs”. The infected attachment has been deleted.”

Result: The page changes slightly depending on which notification type you choose.

2. Enable each of the notification types you want to send. (Click **Enable it** to turn on a notification; click **Disable it** to turn it off.)
3. You can modify the **From** line, the **Subject** line, and the **Message** text for any of the notification messages. When modifying the text, use these variables in conjunction with any of the options:
 - ❖ **%a** (action taken): The words used in a message for this variable are “cleaned”, “deleted”, or “passed”.
 - ❖ **%d** (date): The date that the virus was detected.
 - ❖ **%f** (sender): The **From** header of the sender of the virus.
 - ❖ **%F** (attachment file name): The name of the attachment containing the virus.
 - ❖ **%h** (mail server hostname): The name of the mail server that routed the virus.
 - ❖ **%t** (envelope recipient): The envelope-to data (can include **Bcc** recipients). **Important!** Use the **%t** code with the administrator

notification message; do not add it to sender or recipient notifications, because doing so might expose confidential information about DL memberships or Bcc recipients.

❖ %v (virus name): The virus name and number.

4. Click **Apply** or **Restore to Default**.

Result: If you click **Apply**, the system uses the specified notifications. If you click **Restore to Default**, your changes to the selected notification message go away and the factory set message re-displays. **Note:** Clearing the text box resets the default message.

Scheduling Updates for Sophos and F-Secure Anti-Virus

Anti-Virus updates ensure optimal performance over time. Use the **Anti-Virus > Sophos > Updates** OR the **Anti-Virus > F-Secure > Updates** page, respectively, to set up a schedule of automatic updates. This is important as new viruses are discovered each day, sometimes hourly, and added to the pattern file against which the scanning is done.



You should update the virus scanning pattern on an hourly basis. Scheduling hourly updates ensures that the scanning utility operates at maximum protection. Updating the pattern file does not inhibit system performance. How to do schedule automatic updates is described in [“Getting Automatic Updates & Setting a Proxy Server,”](#) next.

MIRAPPOINT®
Message Server

doc3.mirapoint.com

Home ▶ Anti-Virus ▶ Sophos Anti-Virus ▶ Updates

site map | help | logout

Configuration
Notifications
Updates

Anti-Virus Updates

About Sophos Anti-Virus
Sophos Anti-Virus SAVI3 3.2.07.127
Pattern file: 4.02
Incremental patterns: agobo-vi alcra-e backurl bagdl-bi bagdl-bl bagle-cf bagle-cj bagle-cm bagle-co bagle-cu bagle-cy bagledbj bagledbk baglezip bancb-nq bancbaoe banco-pz banco-qg bank-akw bankas-m bankd-aj banksn-g banlo-ij banlo-rt bckdr-qf bdoor-qd bdoor-vk bnksafam bombka-d bombka-e bront-w brospy-k byteve-q cimuz-t cimuz-u clagge-d clagge-f clagge-h clckr-w codbot-l coldfu-g crybot-b danmec-g datom-b dloa-ada dload-hr dload-li dloadacy dloadrlm dnsch-bd doxpar-f drop-eb dropp-eh drsmar-e drsmar-l emdoor-a fasong-i feebdl-a feebdl-g feebds-e feebds-g fiat-g forbo-gr forbotgn goldu-bx grayb-bn haxdo-as haxdo-at haxdo-gn hookie-b hupig-ci inqtan-a kelvirbe kookoo-a leap-a look-ae look-aw loosky-v maslan-i mdrop-kz mrcgirib mytob-go mytob-gw nyxem-d ooj-b opank-aj paymit-b prosti-a pws-em qqrob-cy qqrob-dg rbot-bka rbot-blc rbot-bmg rbot-bsc rbot-bwt rbot-bwu rbot-bya rbot-bym rbot-ccy rbot-cgc rbot-lt remlo-b ruindl-k sality-i sdbo-aop sdbo-aqh sdbo-axp sdbo-dja sdbotaos sdbt-azl sdbt-amf sdbt-avz shredl-j smldlr-b spammita spywa-ae stinx-f stinx-n stinx-o stinx-p stinx-q stinx-r stinx-s stinx-t stinx-u swizz-aw telemo-b teros-a tileb-cx tileb-cz tileb-dl torpi-ai vb-tc vixup-bh wowpws-a wowpws-c yahoo-b zlob-bc zlob-cn zlob-co zlob-fv zotob-k zotob-l

Mirapoint MIME engine: 051029
Mirapoint scan engine: 051029
Mirapoint AV updater: 2.1.1
Last updated: Fri Feb 24 15:56:05 PST 2006
Last checked: Fri Feb 24 15:56:05 PST 2006

Automatic Update and Proxy Server
 Automatically update:

*Hourly: 56 (on the minute)
 Daily: 00:00 (on the hour)
 Weekly: Sunday (day of week)
 Monthly: 1 (on the day)
*Strongly Recommended

Use Proxy Server:
Host: doc2.mirapoint.com
Port: 25
User ID: administrator
Password: ●●●●

Apply Update Now

Figure 81 Anti-Virus Signature Engine Updates Page

Getting Automatic Updates & Setting a Proxy Server

To setup automatic updates and/or a proxy server, follow these steps on the **Anti-Virus > Sophos > Updates** OR **Anti-Virus > F-Secure > Updates** page, respectively.

1. Check the **Automatically update** checkbox and specify one of the following:
 - ❖ **Hourly:** Choose a minute from the drop-down list, on that minute, every hour, the utility retrieves new virus information.
 - ❖ **Daily:** Choose an hour from the drop-down list, on that hour, every day, the utility retrieves new virus information.
 - ❖ **Weekly:** Choose a day from the drop-down list, on that day (at midnight), every week, the utility retrieves new virus information.
 - ❖ **Monthly:** Choose a day from the drop-down list, on that day (at midnight), every month, the utility retrieves new virus information.
2. If you use a proxy server to reach the Internet, select the **Use Proxy Server** option. Enter the **Host** name, the **Port** number, the **User ID**, and **Password** required by your proxy for access to the Internet. Click **Apply**.
Result: The utility retrieves an updated pattern file via the specified proxy.



Use the **Hourly** option to ensure that the utility operates at maximum protection.

Getting an Immediate Antivirus Update

To get an immediate update, follow these steps on the **Anti-Virus > Sophos > Updates** OR **Anti-Virus F-Secure > Updates** page:

1. If you use a proxy server to reach the Internet, select the **Use Proxy Server** option. Enter the **Host** name, the **Port** number, the **User ID**, and **Password** required by your proxy for access to the Internet. Click **Apply**.
2. Click **Update Now**.

Result: The utility immediately accesses and updates itself with the latest virus pattern file. When the update is complete, the page refreshes and displays an update complete message.



Perform an immediate update as soon as you complete the initial configuration of the system.

Checking Current Version Information

Check for updates on the **Anti-Virus > Sophos > Updates** OR **Anti-Virus > F-Secure > Updates** page, respectively; see Figure 81 for an example. The following information, as well as the version number of that antivirus pattern file, displays. Note: *Scanner*, below, refers to either “Sophos” or “FSAV” for F-Secure.

- ◆ **Pattern file:** The pattern (virus definition) file number.
- ◆ **Incremental patterns:** The viruses that have been added to the utility with each update it has performed since the last version and pattern file was obtained. **Note:** This value only displays when applicable.
- ◆ **Mirapoint *Scanner* MIME engine:** The version of the current Multipurpose Internet Mail Extension interpreter.
- ◆ **Mirapoint scan engine:** The version of the current scan engine.
- ◆ **Mirapoint *Scanner* AV updater:** The version of the current updater.
- ◆ **Last updated:** The date of the utility's last update.

Modifying Predictive-based (RAPID) Anti-Virus

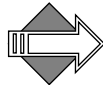
Use the **Anti-Virus > RAPID™** pages to configure the RAPID antivirus scanner, including setting up notifications and updates. See [“About Predictive-Based Anti-Virus” on page 397](#) for important details.



Because RAPID AV uses IP Addresses to determine a potential virus outbreak, it is important that your Relay List of acceptable IP Addresses (those that you want to accept mail from for relay; should include all your internal servers) be up-to-date so as not to incur any unnecessary delays.

Before you can configure **RAPID Anti-Virus** scanning, you'll need to:

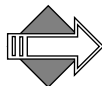
1. Identify a *quarantine administrator* to manage the virus quarantine.
2. If this user does not already have an account, create an account and assign the user the *quarantine administrator* role. For more information about quarantine administrators, see [“About the Quarantine Administrator User” on page 289](#).
3. Create a folder for this user called *RapidAv* (or a name of your choosing). You configure RAPID AV to send quarantined messages to this folder. For more information about creating folders, see [“Adding Folders” on page 303](#)



The default quarantine folder is a sub-folder of the *administrator* account: **user.administrator.RapidAv**.



Figure 82 Anti-Virus Predictive Engine (RAPID) Configuration Page



There are some file extensions that always trigger the RAPID antivirus quarantine action; those extensions are:

- ❖ .scr
- ❖ .pif

- ❖ .com
- ❖ .exe
- ❖ .vbs
- ❖ .bat
- ❖ .cmd
- ❖ .d11
- ❖ .cpl

In addition, any zip file containing an .exe file is always quarantined.

To modify RAPID antivirus scanning, follow these steps on the **Anti-Virus > RAPID > Configuration** page; see Figure 82 for an example.

1. Make sure the RAPID antivirus scanner is enabled. (If it is currently disabled, click the **Enable it** button.)
2. Specify your quarantine administrator's RapidAv folder in the Quarantine Folder field, for example *user.qadmin.RapidAv*. The administrator must be registered in the same domain and be assigned the Quarantine Administrator role.
3. Click **Apply**.
Result: All messages potentially containing a virus are automatically quarantined to the specified email address; all others are delivered normally. In both cases, the original message is modified with a header (**X-Mirapoint-RAPID**) and a warning banner indicating that a virus was found and what action was taken. Automatic release of RAPID-quarantined messages occurs eight hours after quarantining; this can be changed using the CLI. See **Help About Antivirus**.

Setting Notifications for RAPID Anti-Virus

It is highly recommended that **RAPID Anti-Virus** notifications be configured to let users know that their mail is being quarantined due to a potential virus.

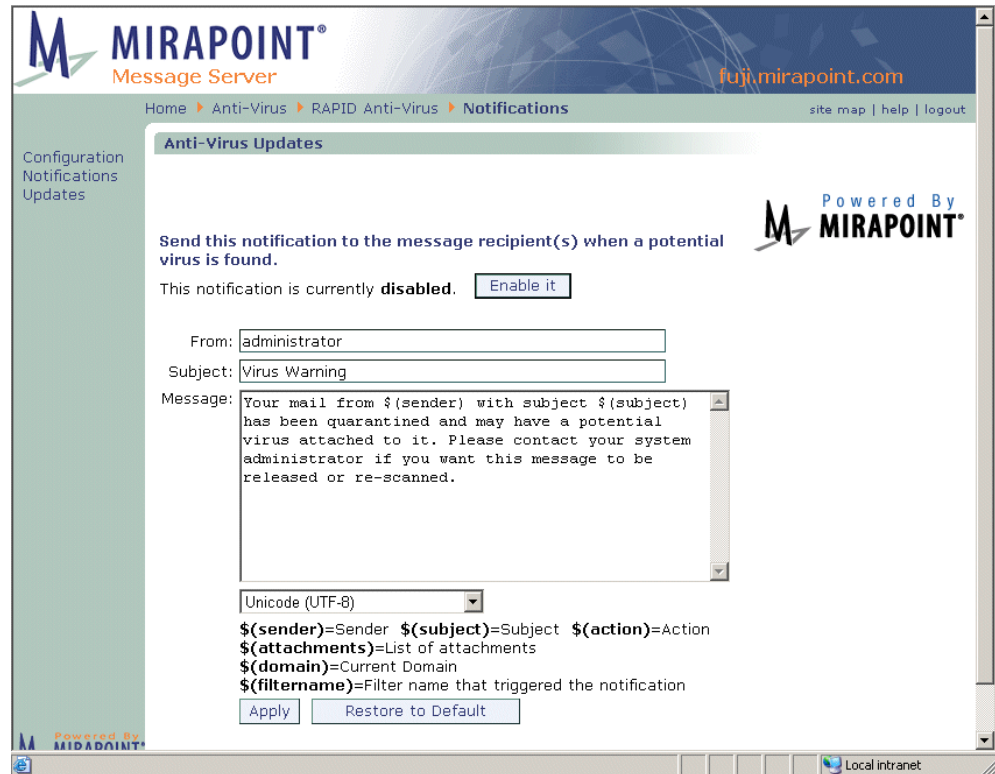


Figure 83 Anti-Virus Predictive Engine (RAPID) Notifications Page

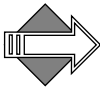
To specify antivirus scanning notifications follow these steps on the **Anti-Virus > RAPID > Notifications** page; see Figure 83 for an example.

1. Use the **Enable it** button to turn on the notification; use the **Disable it** button to turn it off. You can modify the **From** line, the **Subject** line, and the **Message** text for any of the notification messages.

Result: Depending on your action, the notification is enabled or disabled; the notification must be enabled before it can be sent.

2. When modifying the notifications text, use these variables in conjunction with any of the options:
 - ❖ **\$(recipientlist)** Recipient(s): The **To** header of the recipient(s) of the message.
 - ❖ **\$(sender)** Sender: The **From** header of the sender of the message.
 - ❖ **\$(subject)** Subject: The **Subject** line of the message.
 - ❖ **\$(action)** Action: Currently, this is always “Quarantined”.
 - ❖ **\$(attachments)** List of attachments: The names of any attachments to the message.
 - ❖ **\$(domain)** Current Domain: The domain in which the RAPID scanning was done.
 - ❖ **\$(filtername)** Filter name that triggered the notification.
3. Click **Apply** or **Restore to Default**.

Result: If you click **Apply**, the system uses the specified notification. If you click **Restore to Default**, your changes to the selected notification message go away and the factory set message re-displays. **Note:** Clearing the text box resets the default message.



An important step in configuration is setting the updates schedule. See [“Scheduling Updates for RAPID Anti-Virus” on page 413](#) for details.

Scheduling Updates for RAPID Anti-Virus

Anti-Virus updates ensure optimal performance over time. Use the **Anti-Virus > RAPID > Updates** page to set up a schedule; see Figure 84 for an example. **Note:** RAPID updates differ from Sophos and F-Secure updates in that there is no “pattern file,” instead, there is a “Ruleset”

that comprises the filter that RAPID uses to quarantine messages with potential viruses. Occasionally this should be updated.

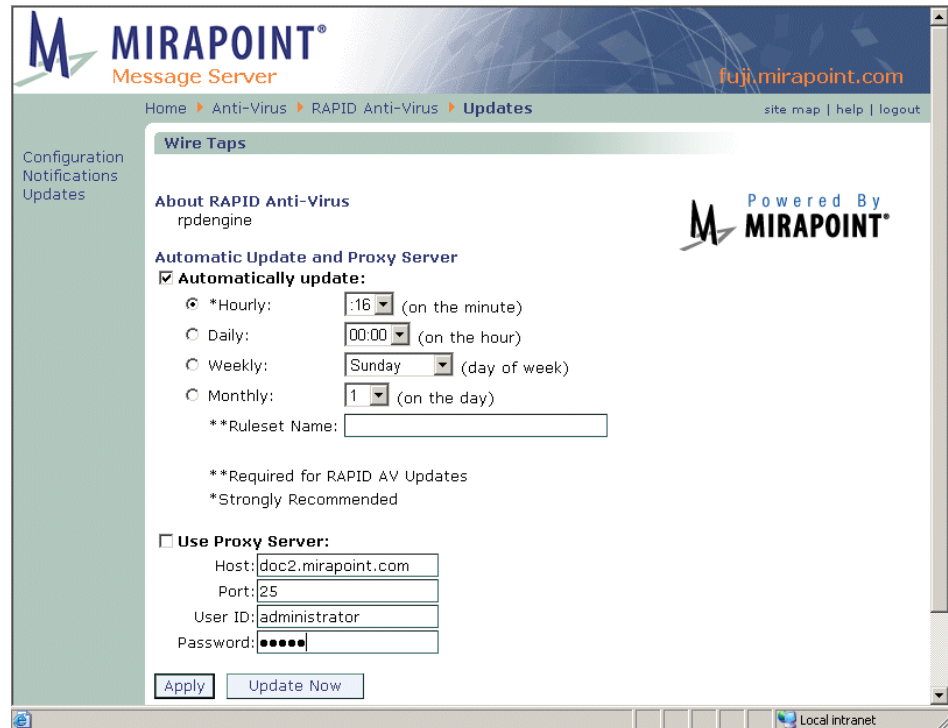



Figure 84 Anti-Virus Predictive Engine (RAPID) Updates Page

Getting Automatic Updates & Setting a Proxy Server

To set up automatic updates or a proxy server, follow these steps on the **Anti-Virus > RAPID > Updates** page, which is shown in Figure 84.

1. Check the **Automatically update** checkbox and specify one:
 - ❖ **Hourly:** Choose a minute from the drop-down list. On that minute, every hour, the utility retrieves new virus information.
 - ❖ **Daily:** Choose an hour from the drop-down list. On that hour, every day, the utility retrieves new virus information.
 - ❖ **Weekly:** Choose a day from the drop-down list. At midnight on that day, every week, the utility retrieves new virus information.

- ❖ **Monthly:** Choose a day from the drop-down list. At midnight on that day, every month, the utility retrieves new virus information.
2. Specify a **Ruleset Name** if no ruleset is selected. **Note:** As they are developed, Mirapoint adds named Rulesets to the Mirapoint Support site at <http://support.mirapoint.com>.
Result: The new ruleset displays in a list. Click the ruleset's **Delete** icon  to remove it.
 3. If you use a proxy, select the **Use Proxy Server** option. Enter the **Host** name, **Port** number, **User ID**, and **Password** required by your proxy for access to the Internet.
 4. Result: The system retrieves ruleset updates through the specified proxy.
 5. Click **Apply** to save your changes.

Result: The system automatically retrieves updated Ruleset files for the RAPID antivirus scanner.



Use the **Hourly** option for maximum protection against viruses.

Getting an Immediate Ruleset Update

To manually update the ruleset, go to the **RAPID Anti-Virus > Updates** page, select the ruleset that you want to update, and click **Update Now**.

Result: The system immediately retrieves and applies the latest ruleset. The page refreshes and displays a message to indicate that the update is complete.

Checking Current Version Information

Click **Updates** in the left page menu to display the **Anti-Virus > RAPID > Updates** page. This page is shown in Figure 84. Information about the current ruleset is shown below the **About RAPID Anti-Virus** heading.

Using Antispam Scanning



The Anti-Spam scanner is a licensed software option. If other Anti-Spam scanning is done upstream, the anti-spam scanner re-writes previous UCE scores or lists. Anti-Spam scanning is performed after high-priority (level 100) filters are applied and before level 450 filters.



Set up antispam scanning as soon as you complete your initial configuration. Antispam scanning should always be configured on your edge device.

Managing your antispam scanning can involve the following tasks:

- ◆ **Modifying Anti-Spam Scanning:** Enable/disable Anti-Spam scanning, specify how severely the utility should judge incoming mail for spam, and set other defaults.
- ◆ **Scheduling Updates for Anti-Spam Scanning:** Specify how often the utility should update spam information. You can also choose to perform a manual update that causes an immediate update.
- ◆ **Setting the Allowed Senders List:** Specify certain senders from whom mail should never be marked as spam.
- ◆ **Setting the Blocked Senders List:** Specify certain senders from whom mail should always receive the configured **Junk Mail** filter action.
- ◆ **Setting the Allowed Mailing Lists List:** Specify certain recipient addresses whose mail should never receive the configured **Junk Mail** filter action.
- ◆ **Updating Relay Domains (Relay List):** Specify IP networks or DNS domains for which the SMTP service is to accept messages for relay to remote hosts. Does not require an Anti-Spam license.
- ◆ **Updating Blocked Domains (Reject List):** Specify networks from which messages should be rejected. Does not require an Anti-Spam license.
- ◆ **Updating Your Realtime Blackhole List (RBL):** Specify that all incoming messages be checked against the Real Time Blackhole List (RBL) internet service. Does not require an Anti-Spam license.

Anti-Spam Scanning Options

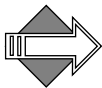
There are many options to choose from when configuring antispam scanning; this section describes options that you should understand beforehand. The step-by-step procedure is given in [“Modifying Anti-Spam Scanning” on page 419](#).

Principal Edition vs. Signature Edition

The antivirus scanner uses one of two mutually exclusive techniques to categorize mail as junkmail (spam): **Principal Edition** or **Signature Edition**. Which scanner you use depends on which licenses you have applied. The licenses are separate and cannot be applied simultaneously.

Principal Edition antispam compares all incoming email messages to a set of rules. The more rules the message matches, the higher the junkmail UCE (unsolicited commercial email) score it is assigned. Any UCE score over the junkmail **Threshold** (50, by default) categorizes the mail as spam and triggers the **Junk Mail** filter. The rule group updates for Principal Edition are named “default” and are automatically installed.

Signature Edition antispam uses an external pattern detection method that scans Internet email traffic to create a database of email signatures against which incoming mail is compared. Mail is thereby categorized as spam, bulk, suspicious, unknown, or not spam. Like the **Principal Edition**, any UCE score over the junkmail **Threshold** (50, by default) categorizes the mail as spam and triggers the **Junk Mail** filter. Signature Edition updates are named “rpdengine” and need to be added manually.



Signature Edition’s predictive-based scanning is faster than the rules-based scanning performed by the Principal Edition.

Both antispam techniques score messages and insert a message header, **X-Junkmail**, to indicate junkmail. This header is inserted when a message is scored above the junkmail **Threshold**; by default, this threshold is set to 50 for both techniques. The X-Junkmail header can be used as a search parameter in a message filter on a domain-wide or per-user basis. The junkmail **Threshold** can be adjusted on the **Configuration** page for any of the antivirus engines. For a list of

Mirapoint X-Junkmail headers, see [“Reading Message Envelopes and Headers” on page 235](#).

To learn more about the antisпам threshold, see [“About the Antisпам Scanning Rules and Threshold” on page 336](#).

About the Junk Mail Filter



The **Junk Mail** filter, when ON, tells the Anti-Spam scanner what to do with mail categorized as junkmail (spam). The default action, **Move to the Junk Mail folder**, allows users to check their junkmail for false-positives. The **Junk Mail** filter is visible on the **Options > Message Filters** (Corporate Edition WebMail) or **Options > Junk Mail Control > Junk Mail Filter** page (Standard Edition WebMail), respectively, for end-users.

The user’s **Junk Mail** filter **Condition** must be **Normal** or **Exclusive** for their **Allowed Senders**, **Blocked Senders** and **Allowed Mailing Lists** WebMail options to work. The system-created **Junk Mail** filter defaults to **Off** because non-WebMail, POP users would not be able to see the Junk Mail folder. Users must go to **Options > Junk Mail Control > Junk Mail Filter** (Standard Edition) or **Options > Message Filters** (Corporate Edition) and explicitly turn ON the **Junk Mail** filter.

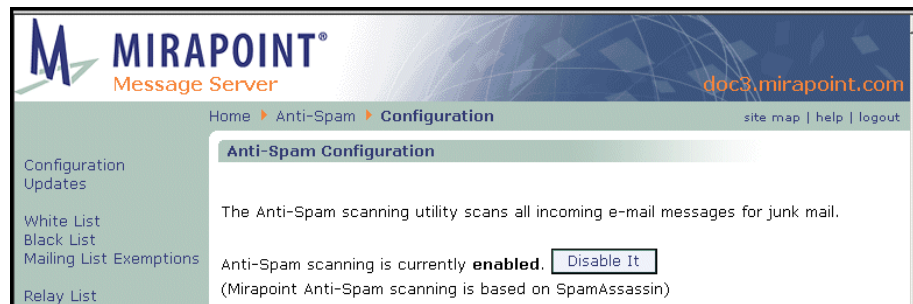
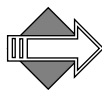


Figure 85 Anti-Spam Configuration Page Detail



The Junk Mail Filter is only used when Junk Mail Manager is *not* used to manage junk mail messages. Users must turn the Junk Mail Filter OFF to use JMM.

Modifying Anti-Spam Scanning

On the **Anti-Spam > Configuration** page (see Figure 86 for an example), a message displays in **red** if you do not have a valid license. You must obtain a valid license before you can configure the antispam scanning utility. If you have a valid license, the page displays a **Disable it** button so you can turn the utility off; if you turn the utility off, it displays an **Enable it** button. Antispam **Configuration** requires making specifications for an antispam scanning threshold, and setting warning, explanation, reporting, and scan recipient options.

Set Threshold [Show Junk Mail Statistics](#)
 Set a threshold for qualifying messages as junk mail (spam). The lower the threshold, the more likely messages will qualify as junk mail. The higher the threshold, the less likely messages will qualify as junk mail.

Threshold Number: (0 - 300, increment by 1)

Set Anti-Spam Warning Flag
 The Anti-Spam warning flag is added to the Subject line of all messages that qualify as junk mail (spam).

Add Warning Flag
 Flag Text:

Set Junk Mail Explanation
 Junk Mail Explanation inserts an "X-Junkmail-Info:" header to the message with an explanation of why it did (or did not) qualify as junk mail. The explanation includes the spam score, per rule; the name of each spam rule that was matched; and a simple description of the rule. If the total of all the spam scores received exceeds the **Threshold** (see **Set Threshold** section on this page), the message qualifies as junk mail.

Insert Junk Mail Explanation

Set Junk Mail Reporting
 Junk Mail Reporting provides a user option, **Report to system support**, for spam that the filter missed and false spam that accidentally triggered the filter. System folders for each are created when the options are used and Mirapoint is periodically sent samples from each folder; this can help Mirapoint make junk mail scanning improvements.

Enable Junk Mail Reporting

Disable Local Recipient Check
 The Anti-Spam local recipient check, ON by default, causes only mail to addresses in the local routing table to be scanned. This may be inappropriate for routers. Select the option below to disable this check, causing every message being routed to get scanned regardless of recipient address.

Scan messages for any recipient

Figure 86 Anti-Spam Configuration Page Detail, Options

To modify antispam scanning, follow these steps on the **Anti-Spam > Configuration** page; see Figure 86 for an example.

1. Make sure antispam scanning is enabled. (If it is currently disabled, click the **Enable it** button.)

Result: Enabling the utility creates the end-user Junk Mail filter. Scanning is done only on local; select Scan messages for any recipient (below) to enable outbound scanning. If COS is not

enabled, antispam works for all users. If COS is enabled and antispam services are under COS control, antispam works only for users with **antispam** listed in their **miService** LDAP attribute.

2. Click **Show Junk Mail Statistics** to see your system's current **Incoming Mail vs Junk Mail** performance graph; for details on reading the graph, see [“Junk Mail Graphs” on page 212](#). Click **Hide Junk Mail Statistics** to make the graph go away.
3. Set these antispam scanning options:
 - ❖ **Threshold Number**, text box option: Adjust the anti-spam scoring severity by incrementing or decrementing the **Threshold** by 1 (one), and then testing the results. **Important!** In most cases, the default of 50 is optimal and should not be changed. Increasing the default **Threshold** causes the Junk Mail scanning utility to mark less incoming mail as spam. Decreasing the default **Threshold** causes the utility to mark more mail as spam. See [“About the Antispam Scanning Rules and Threshold” on page 336](#) for more details.
 - ❖ **Add Warning Flag**, checkbox and text box options: Customize the warning inserted in the message **Subject** to identify it as spam. This is useful for POP client users, since POP lacks multiple folder support; spam mail for POP users must be configured to go to their Inbox.
 - ❖ **Insert Junk Mail Explanation**, checkbox option selected by default: Adds a special header, **X-Junkmail-Info**, to the message header that contains the results of the antispam scan. This option only applies to the **Principal Edition** anti-spam scanner. For details on this header, see [“Reading Message Envelopes and Headers” on page 235](#).
 - ❖ **Enable Junk Mail Reporting**, checkbox option selected by default: Places an extra option, **Report this spam to system support** or **Report this false spam to system support**, on the **This is Spam** and **This is Not Spam** pages, respectively, in WebMail. These pages open when a user clicks the **This is Spam** or **This is Not Spam** link on messages in their **Inbox** or **Junk Mail** folder. If users elect to report the spam/false spam to Mirapoint, two system folders are created (**junkmail.junkmail** and **junkmail.notjunkmail**) to receive those messages. Samples

from the two folders are sent to Mirapoint daily to assist in scanning improvements.

- ❖ **Scan messages for any recipient**, checkbox option selected by default: The otherwise-automatic local recipient check might not be desirable in all cases. Selecting this checkbox enables anti-spam scanning on outbound mail as well as inbound mail.

4. Click **Apply**.

Result: Your configuration options are recorded by the system and acted on as specified. A header line **X-Junkmail: UCE(score)** (Principle Edition) or **X-Junkmail-SD-Raw (score)** (Signature Edition), is added to all messages identified as spam. For details on these headers, see [“Reading Message Envelopes and Headers” on page 235](#).

Scheduling Updates for Anti-Spam Scanning

Anti-Spam Updates are an important step in the configuration process as rulegroup updates optimize the utility. In addition to rulegroup updates, which do not apply to **Signature Edition** anti-spam scanning; exception files for **MailHurdle** listing (“known good mailers”) are included in updates.



Use the **Update all rule groups every week** option to ensure that the utility operates at maximum protection.

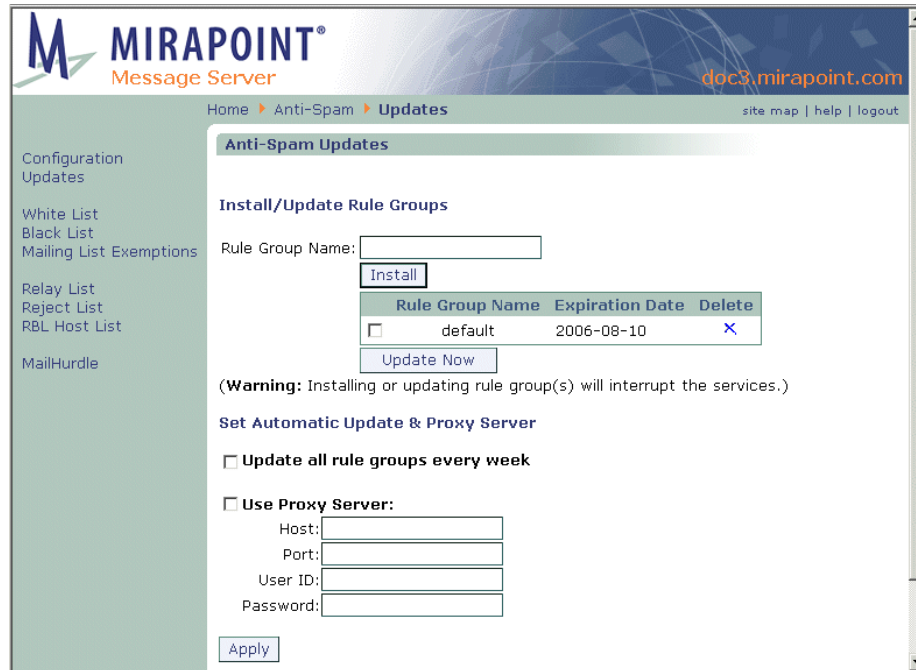


Figure 87 Anti-Spam Updates Page


Installing/Updating Anti-Spam Rule Groups

As spammers evolve new spamming techniques, new methods to battle them are added.

To install or update a rule group or exception file (known good mailers) for your antispam scanning utility, follow these steps on the **Anti-Spam > Updates** page (see Figure 87 for an example).

1. Enter the Rule Group Name and click **Install**. **Note:** As they are developed, Mirapoint adds named Rule Groups to the Mirapoint Support site at <http://support.mirapoint.com/>.

Result: The new rule group displays in the list below with the following information:

- ❖ **Rule Group Name:** The name of the rule group. The initial name is always **default**, the rule group that shipped with the product.
 - ❖ **Expiration Date:** The date after which the rule group is no longer valid and must be updated.
2. To update an already installed rule group, select the rule group and click **Update Now**.
Result: Any updates to that rule group are downloaded.
 3. Click the rule group's **Delete** icon  to remove it from the antispam scanning utility.
Result: A confirmation page displays, click **Ok** to complete the removal or **Cancel** to stop and keep the rule group.

Getting an Immediate Rule Group Update

To get an immediate rule group update, on the **Anti-Spam Updates** page, select the rule group that you want to update and click **Update Now**.

Result: The utility immediately accesses and updates itself with the latest junkmail rule group. The page re-displays with a message indicating that the update is complete.

Setting Up Automatic Rule Group Updates and Proxy Server

You can set your antispam scanning utility to updates its rule groups and/or MailHurdle exception files (known good mailers) automatically every week. To do this, follow these steps on the **Anti-Spam > Updates** page.

1. Select the **Update all rule groups every week** checkbox.
2. If you use a proxy when accessing the Internet, select the **Use Proxy Server** option and enter the **Host** name, the **Port** number, the **User ID**, and **Password** required by your proxy for access to the Internet.

3. Click **Apply**.

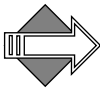
Result: The utility retrieves an updated file with additional spam rules and, MailHurdle known good mailers, for it to use when scanning messages.

Setting the Allowed Senders List

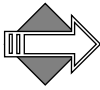
Use the **Allowed Senders** page to ensure that mail from certain senders is always sent to recipients and never tagged as junkmail. Please note: domain and user filters can override this safelist. Administrators can use the CLI to set up logging of domain mail from Allowed and Blocked senders; for information see the CLI online help command **Help About Log**.



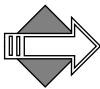
This link only displays if you have Anti-Spam licensed and configured for your system.



If you want to set an Allowed Senders list for a delegated domain, select the current domain, as described in [“Selecting a Domain” on page 265](#). If you do not select a delegated domain, the safelist applies to all traffic through the primary domain.



The user’s **Junk Mail** filter condition must be **Normal** or **Exclusive** for the user-level **Allowed Senders** list in WebMail to work; the filter must not be set to **Off**. For more information, see [“About the Junk Mail Filter” on page 418](#). This **Note** does not apply to Junk Mail Manager, or non-WebMail, users!



The Allowed Senders filter does not do period-to-underbar mapping so it might be necessary to create both a period (.) and an underbar (_) entry for the same sender to ensure that the sender is safelisted. For example, to make sure that user.ab@example.com is always safelisted, enter **user.ab@example.com** and **user_ab@example.com**.

See [“Using Patterns” on page 323](#) for details on using wildcards with filters.

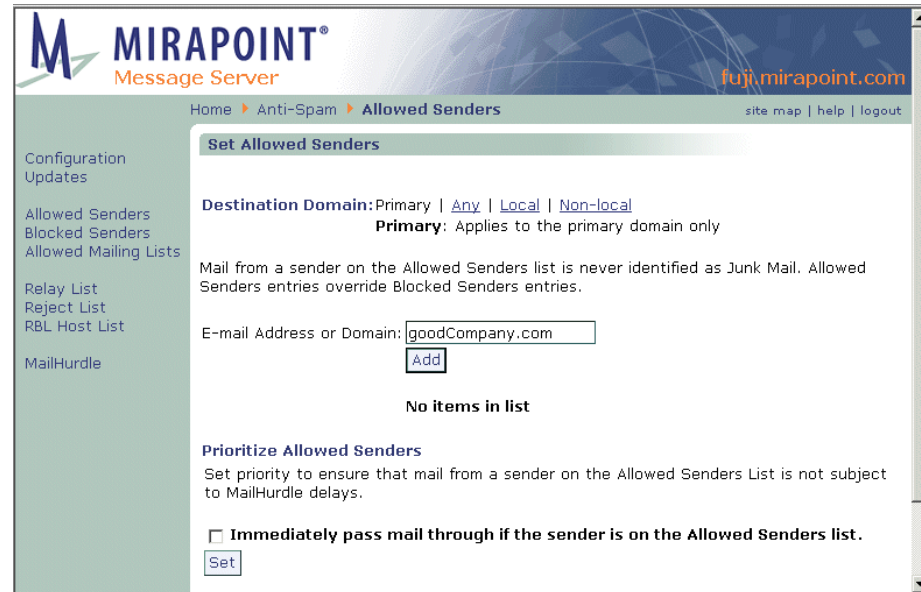


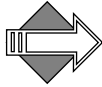
Figure 88 Anti-Spam Allowed Senders Page

To create an Allowed Senders filter follow these steps on the **Anti-Spam > Allowed Senders** page; see Figure 88 for an example.

1. In the **Destination Domain** area specify the scope for the filter.
Note!: If you select a delegated domain before coming to this page or if you log in as a domain administrator, or if this is for a Junk Mail Manager domain, these options do not display.
 Select one:
 - ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
 - ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
 - ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
 - ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.

Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. To find a previously created Allowed Senders entry, enter a name in the **E-mail Address or Domain** name text box, and click **Find**. **Note:** See [“Using Patterns” on page 323](#) for details on using wildcards. Click **Clear** to empty the text box and re-display the entire list (ten names display at a time). To find an entry in a delegated domain’s Allowed Senders list, remember to select the domain first
Result: The list box displays the results.
3. Enter an **E-mail Address or Domain** name in the text box and click **Add**. If you enter a domain name, the at sign (@) is automatically prefixed.
Result: The address or domain name appears in the **Allowed Senders** list box and the Allowed Senders status is updated to reflect the new number of entries. Mail sent from Allowed Senders is forwarded to the specified recipients with a header, **X-Junkmail-Whitelist: YES (by domain whitelist at hostname)**, added; such mail is not subject to antispam scanning; however, it can be acted on by content filters. The header is added whether the safelist was at the primary level, the delegated domain level, or user level.
4. Select the **Prioritize Allowed Senders** option and click **Set** to prevent mail from your allowed senders from being delayed by MailHurdle. If you leave the checkbox unselected, mail from senders on your Allowed Senders list is processed by MailHurdle. Messages should still be delivered successfully, but there will be an initial delay for each sender. (If the mail fails to pass MailHurdle, then it is never delivered.)



The sender is derived from the **From** header of the message.

Removing Allowed Senders Entries

To remove a sender from the Allowed Senders list, select the checkbox for the sender you want to remove and click **Remove**.

Result: The address or domain you selected goes away from the **Allowed Senders** list box and the status updates to reflect the new number of entries.

About the Whitelist Header

The header for domain safelisted mail and user safelisted mail is slightly different. A domain level safelist generates this header:

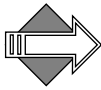
X-Junkmail: Whitelist (by domain whitelist at *hostname*). A user level safelist generates this header: **X-Junkmail: Whitelist (by *username* at *hostname*)**. Neither header is visible unless the recipients view all of the headers; this can be done in WebMail by clicking the **Open** (Standard Edition) or **Source** (Corporate Edition) button when viewing a message.

Setting the Blocked Senders List

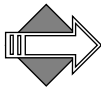
Use the **Blocked Senders** page to ensure that mail from certain senders is always sent to recipients tagged as junkmail. Administrators can use the CLI (command line interface) to set up logging of domain mail from Allowed and Blocked senders; for information see the CLI online help command **Help About Log**.



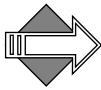
This link only displays if you have Anti-Spam licensed and configured for your system.



If you want to set a Blocked Senders for a delegated domain, select the domain, as described in [“Selecting a Domain” on page 265](#). Otherwise, this blockedlist applies to all traffic through the primary domain.



The user’s **Junk Mail** filter condition must be **Normal** or **Exclusive** for the user-level **Blocked Senders** in WebMail to work; the filter must not be set to **Off**. For more information, see [“About the Junk Mail Filter” on page 418](#). This Note does not apply to Junk Mail Manager, or non-WebMail, users!



The Blocked Senders filter does not do period-to-underbar mapping so it might be necessary to create both a period (.) and an underbar (_) entry for the same sender to ensure that the sender is blocklisted. For example, to make sure that user.ab@example.com is always blocklisted, enter **user.ab@example.com** and **user_ab@example.com**.

See [“Using Patterns” on page 323](#) for details on using wildcards with filters.

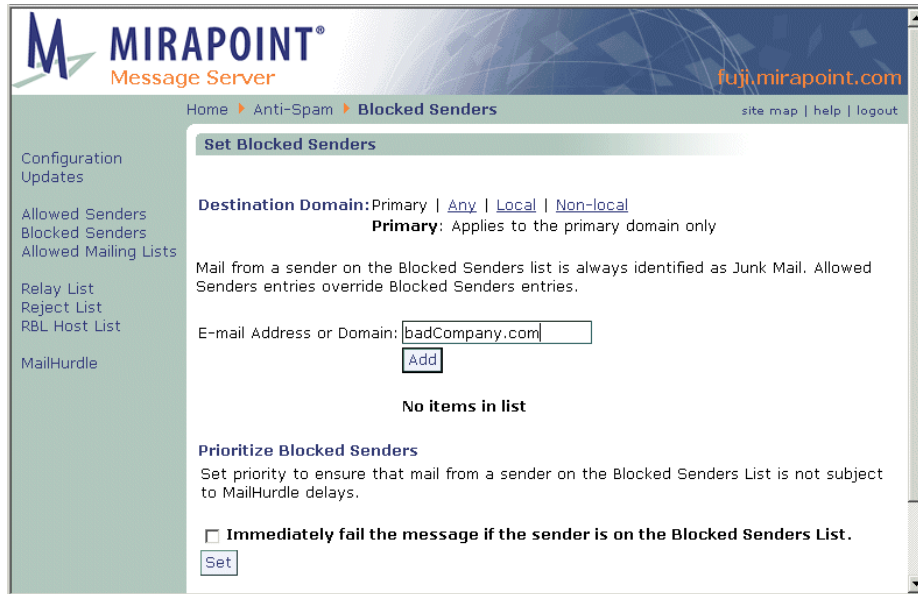


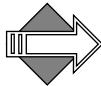
Figure 89 Anti-Spam Blocked Senders Page

To create a Blocked Senders filter follow these steps on the **Anti-Spam > Blocked Senders** page.

1. In the **Destination Domain** area specify the scope for the filter.
Note!: If you select a delegated domain before coming to this page or if you log in as a domain administrator, or if this is for a Junk Mail Manager domain, these options do not display.
 Select one:
 - ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
 - ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
 - ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
 - ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.

Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. To find a previously created Blocked Senders entry, enter a name in the **E-mail Address or Domain** name text box, and click **Find**. **Note:** See [“Using Patterns” on page 323](#) for details on using wildcards. Click **Clear** to empty the text box and re-display the entire list (ten names display at a time). To find an entry in a delegated domain’s Blocked Senders list, remember to select the domain first
Result: The list box displays the results.
3. Enter an **E-mail Address or Domain** name in the text box and click **Add**. If you enter a domain name, the at sign (@) is automatically prefixed.
Result: The address or domain name appears in the **Blocked Senders** list box and the Blocked Senders status is updated to reflect the new number of entries. Mail sent from senders on your Blocked Senders list is forwarded to the specified recipients with a header added (**X-Junkmail: Blacklisted**) and processed by the **Junk Mail** filter if the recipients have turned it on. **Important!** If the sender is on the user’s personal Allowed Senders list, the header is inserted but the mail is still delivered.
4. Select the **Prioritize Blocked Senders** option and click **Set** to prevent mail from your Blocked Senders from getting processed by MailHurdle. If you leave this option unselected, mail from senders on your Blocked Senders list is processed by MailHurdle. If the mail passes MailHurdle, it is then subject to the selected **Junk Mail** filter action.



The sender is derived from the **From** header of the message.

Removing Blocked Senders Entries

To remove a sender from the Blocked Senders list, select the checkbox for the sender you want to remove and click **Remove**.

Result: The address or domain you selected goes away from the **Blocked Senders** list box.

About the Blacklist Header

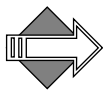
The header for domain blocklisted mail and user blocklisted mail is slightly different. A domain level blocklist generates this header:

X-Junkmail: Blacklisted. A user level blocklist generates this header:

X-Junkmail: Blacklisted (by *username at hostname*). Neither header is visible unless the recipients view all of the headers; this can be done in WebMail by clicking the **Open** (Standard Edition) or **Source** (Corporate Edition) button when viewing a message.

Setting the Allowed Mailing Lists List

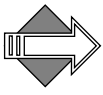
Use the **Allowed Mailing Lists** page to ensure that mail addressed to certain recipients never receives the configured **Junk Mail** filter action. This is primarily used to safelist mailing lists that you are on, to avoid that mail coming in to you being accidentally categorized as spam. This can also be used for mailing lists to which you want to send mail without Anti-Spam filtering delays. This feature is also known as the “recipient whitelist” or “whitelisto.”



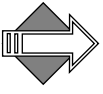
To scan outbound messages for spam, you must have the **Scan messages for any recipient** option selected on the **Anti-Spam > Configuration** page. Administrators can use the CLI (command line interface) to set up logging of domain mail from Allowed and Blocked senders; for information see the CLI online help command **Help About Log**.



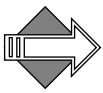
This link only displays if you have Anti-Spam licensed and configured for your system.



If you want to set an Allowed Mailing List for a delegated domain, select the current domain, as described in [“Selecting a Domain” on page 265](#). Otherwise, this Allowed Mailing List list applies to all traffic through the primary domain.



The user’s **Junk Mail** filter condition must be **Normal** or **Exclusive** for the user-level **Allowed Mailing Lists** in WebMail to work; the filter must not be set to **Off**. For more information, see [“About the Junk Mail Filter” on page 418](#). This **Note** does not apply to Junk Mail Manager, or non-WebMail, users!



The Allowed Mailing Lists filter does not do period-to-underbar mapping so it might be necessary to create both a period (.) and an underbar (_) entry for the same recipient to ensure that the recipient is safelisted. For example, to make sure that user.ab@example.com is always safelisted, enter **user.ab@example.com** and **user_ab@example.com**.

See [“Using Patterns” on page 323](#) for details on using wildcards with filters.

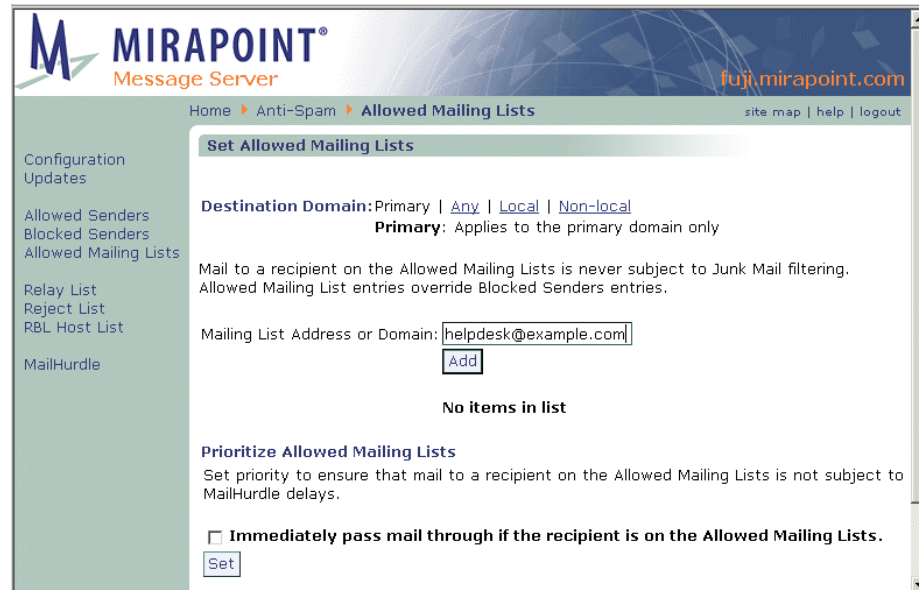


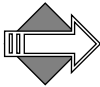
Figure 90 Anti-Spam Allowed Mailing Lists Page

To create an Allowed Mailing List filter follow these steps on the **Anti-Spam > Allowed Mailing Lists** page.

1. In the **Destination Domain** area specify the scope for the filter.
Note!: If you select a delegated domain before coming to this page or if you log in as a domain administrator, or if this is for a Junk Mail Manager domain, these options do not display.
Select one:
 - ❖ **Primary:** Only filter messages addressed to users on the primary domain of the machine on which the filter is created.
 - ❖ **Any:** Filter any messages routed to or through the machine on which the filter is created.
 - ❖ **Local:** Only filter messages addressed to users (all domains) on the machine on which the filter is created.
 - ❖ **Non-local:** Only filter messages addressed to users not on the machine on which the filter is created.

Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.

2. To find a previously created Allowed Mailing Lists entry, enter a name in the **E-mail Address or Domain** name text box, and click **Find**. **Note:** See [“Using Patterns” on page 323](#) for details on using wildcards. Click **Clear** to empty the text box and re-display the entire list (ten names display at a time). To find an entry in a delegated domain remember to select the domain first.
Result: The list box displays the results.
3. Enter a mailing list email address in the text box and click **Add**.
Result: The address appears in the **Allowed Mailing Lists** list box and the Allowed Mailing Lists status is updated to reflect the new number of entries. Mail sent to recipients on your Allowed Mailing Lists list is forwarded to the specified recipients with a header, **X-Junkmail-Recipient-Whitelist: YES (by domain whitelist at hostname)**, added; such mail is not scanned by the Anti-Spam scanning utility. The header is added whether the exempting was at the primary level or at the delegated domain level.
4. Select the **Prioritize Allowed Mailing Lists** option and click **Set** to prevent mail to your exempted mailing list recipients from being processed by MailHurdle. If you leave this option unselected, MailHurdle processes mail sent to recipients in your Allowed Mailing Lists list. The mail should still be delivered, but there will be an initial delay the first time mail is received from each sender. (If the mail fails to pass MailHurdle, it is never delivered.)



The recipient is derived from the **To** header of the message.



Allowed Mailing Lists is effective in preventing mail addressed to recipients on a mailing list (such as helpdesk@example.com) from being delayed by MailHurdle. However, for this to work, the Allowed Mailing Lists list must reside on the same machine that executes MailHurdle. If the Allowed Mailing Lists filter is configured on a machine that receives mail after MailHurdle processing, it cannot prevent MailHurdle delays.

Removing Allowed Mailing Lists Entries

To remove a mailing list from the Allowed Mailing Lists, select the checkbox for the mailing list you want to remove and click **Remove**.
Result: The address you selected goes away from the **Allowed Mailing Lists** list box and the status updates to reflect the new number of entries.

About the Recipient-Whitelist (Allowed Mailing Lists) Header

The header for domain exempted mail and user exempted mail is slightly different. A domain level mailing list exemption generates this header: **X-Junkmail: Recipient-Whitelist (by domain whitelist at *hostname*)**. A user level mailing list exemption generates this header: **X-Junkmail: Recipient-Whitelist (by *username* at *hostname*)**. Neither header is visible unless the recipients view all of the headers; this can be done in WebMail by clicking the **Open** button when viewing a message.
Note: These headers are identical to the headers inserted for regular safelisting.

Updating Relay Domains (Relay List)

The **Set Relay List** page lets you specify IP networks or DNS domains from (and to) which the SMTP service is to accept messages for relay to remote hosts. A message is relayed if it is from a network or domain on the relay list, or addressed to a domain on the relay list. This has no affect on messages accepted for delivery to local mailboxes.

Relay lists prevent your systems from being high-jacked to send junk mail. Unless a relay address is explicitly added, the system does not relay messages from other networks or domains. You do not need to have an Anti-Spam license to configure a relay list.

To accept mail relay from a specific network, enter a partial IP address. For example, if you specify 10.128, the SMTP service accepts relays from 10.128.0.1 or 10.128.3.1, but not from 10.129.0.1. By default Mirapoint systems relay mail from the mail domain you set, but many administrators add the mail domain to the relay list anyway.



You should only specify IP addresses in the Relay List. To prevent accidental exposure, keep the list as short as possible and use SMTP auth wherever possible.

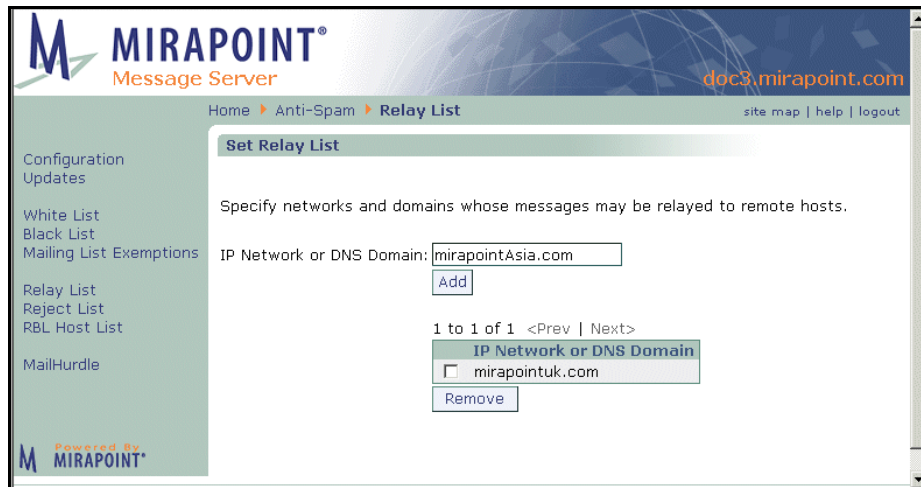


Figure 91 Anti-Spam Relay List Page

To configure a Relay List follow these steps on the **Anti-Spam > Relay List** page. See Figure 91 for an example.

1. Enter an **IP Network or DNS Domain** name and click **Add**. You can use a partial IP address, a full IP address, or a domain name.
Result: The new relay network displays in a list with a **Remove** button; use it to remove networks from your list. Mail sent from those networks is relayed out to its destination.
2. To remove a sender from the relay list, select the checkbox for the sender you want to remove and click **Remove**.
Result: The address or domain you selected goes away from the **Relay List** list box.

Updating Blocked Domains (Reject List)

Use the **Anti-Spam Reject List** page to specify networks from which your system will not accept messages. Maintaining a reject list helps

minimize the amount of unsolicited commercial email (UCE), or spam, that your system receives.



For optimum safety, specify blocked domains using IP Network addresses rather than DNS domain names—DNS domain names are easily spoofed by spammers. However, when adding domains to the reject list, keep in mind that hackers often use “zombies” to distribute spam and viruses and mount denial of service attacks. (A zombie is a PC that has been compromised by a hacker unbeknownst to its owner.)

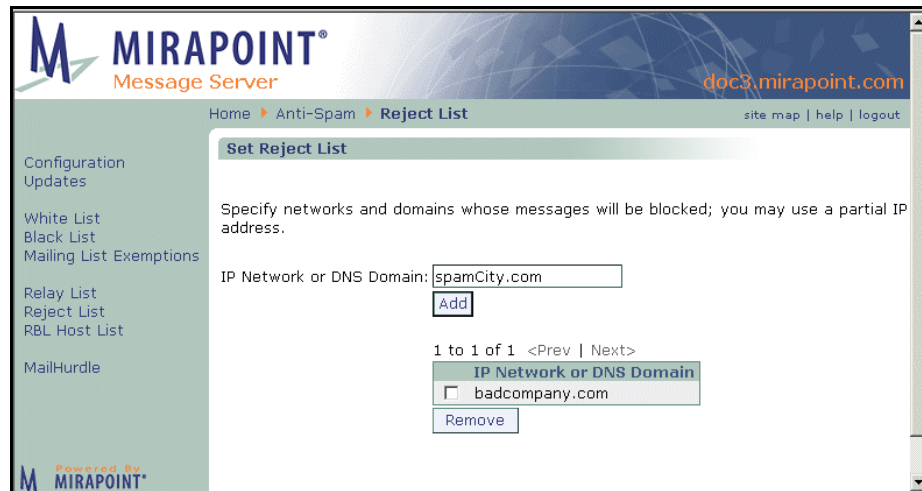
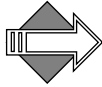


Figure 92 Anti-Spam Reject List Page

To configure a Reject List follow these steps on the **Anti-Spam > Reject List** page. See Figure 92 for an example.

1. Enter a **DNS Domain** name in the text box and click **Add**. (You can also add partial or full IP addresses to the reject list, but Mirapoint recommends that you use domain names instead.)
Result: The new reject network displays in a list with a **Remove** button; use it to remove networks from your list. Mail sent from those networks is bounced back to the sender.
2. To remove a sender from the reject list, select the checkbox for the sender you want to remove and click **Remove**.
Result: The address or domain you selected goes away from the **Reject List** list box.

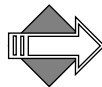


This feature does not require an Anti-Spam license.

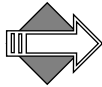
Updating Your Realtime Blackhole List (RBL)

The **Anti-Spam RBL Host List** page allows you to specify that all incoming messages be checked against the Real Time Blackhole List (RBL) internet services you specify (you can add up to eight). RBLs are lists of IP addresses known to transmit junk mail; various free and commercial services are available, with different policies. You must visit the service's websites, and subscribe in order to use this option.

Use the **RBL Check Action** option to specify whether qualifying messages are bounced back to the sender or sent to the intended recipient with an **X-Junkmail: RBL** header. **Note:** Other antispam functions can remove this header.



The effect of setting RBL Host checking depends on your antispam settings. If antispam scanning is enabled, RBL checking is used to calculate the UCE score (for information on the UCE score, see [“About the Antispam Scanning Rules and Threshold” on page 336](#)), and an appropriate **X-Junkmail** header is added based on that score and any safelist or blocklist settings. If antispam scanning is unlicensed or not enabled, messages are categorized as junk mail based on RBL checking alone, and the **X-Junkmail: RBL** header is added. If you are using Signature Edition antispam scanning, this setting has no effect on the UCE score.



This feature does not require an Anti-Spam license.

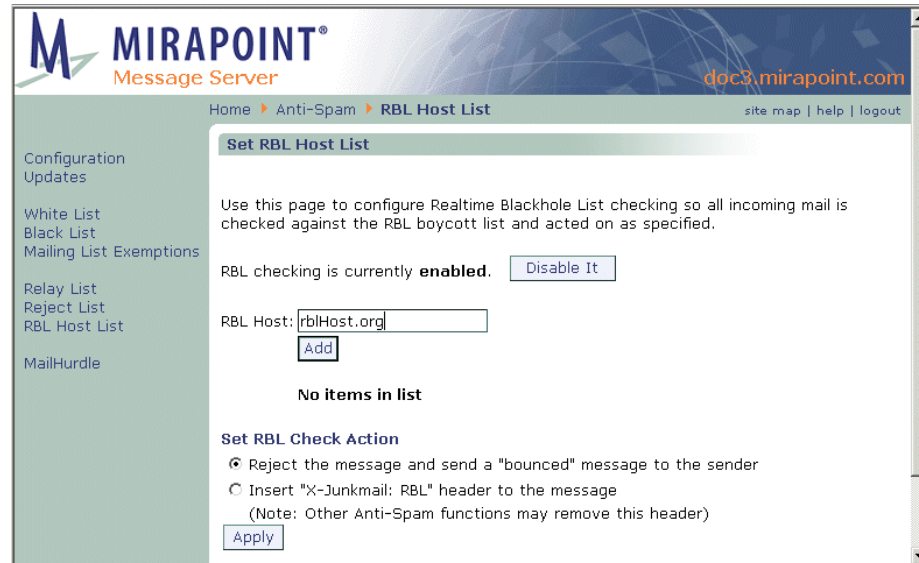


Figure 93 Anti-Spam RBL Host Page

To configure an RBL Host List (you can add up to eight) follow these steps on the **Anti-Spam > RBL Host List** page. See Figure 93 for an example.

1. Make sure RBL checking is enabled. (If it is currently disabled, click the **Enable it** button.)
2. Enter the hostname for an RBL service in the **RBL Host** option and click **Add**. For subscription information, see Knowledge Base article “RBL Hosting” #45 at support.mirapoint.com.
Result: The new RBL Host displays in a list with a **Remove** button; use it to remove hosts from your list. You can add up to 8 RBL hosts.
3. To remove a host from the RBL List, select the checkbox for the host you want to remove and click **Remove**.
Result: The host you selected goes away from the **RBL List** list box, the status updates to reflect the new number of entries.
4. To specify an action, use the **Set RBL Check Action** option, choose either:

- ❖ **Reject the message and send a “bounced” message to the sender:** The message is returned to the boycotted host with a 5xx permanent error message informing them that they have been rejected by the RBL.
- ❖ **Insert “X-Junkmail: RBL” header to the message:** The message is sent on to the recipients with the X-Junkmail header.

Note: Filters can be created that act on the X-Junkmail header. For details see [“Creating a Message Filter” on page 339](#).

Click **Apply**.

Result: All incoming mail is checked against the RBL boycotted hosts list. If a match is found, the specified action is taken. If **Reject the message and send a “bounced” message to the sender** is selected, the detailed SMTP log indicates the action, and whether the action taken was associated with RBL. If **Insert “X-Junkmail: RBL” header to the message** is selected, there is no trace of any RBL activity in the logs unless you set up a filter on the X-Junkmail: RBL header; filtering is logged.

For more information about RBLs, see <http://en.wikipedia.org/wiki/DNSBL>.



In addition to the antispam options discussed here, there are several filters that can be set up to help with antispam. For details, see [“Filter Examples” on page 374](#).

Configuring NIC Failover

NIC failover allows an appliance to switch seamlessly to a second network connection if the first one fails (supported in Release 3.7.1 and later).

To configure NIC failover on a Mirapoint appliance, follow these steps:

1. Obtain a second drop from the same advertised network and attach the cable to Port1 on the appliance back panel (assuming the first network drop is connected to Port0). Note: The second drop can be to a different switch, but both routes must have the same netmask

and use the same IP address for both connections. When NIC failover occurs, the IP address does not change.

2. Create a logical port interface (failover NIC) on the appliance:

```
Netif Addlogical "" Failover
OK Completed
```

With null-string argument, the appliance automatically manages the name space for logical ports, usually creating **logical0** to start, but you will need to run the **Netif Listlogical** command to see the actual port assignment if you let the appliance manage the name space.

3. Check the network bindings, and starting with the primary port, bind the connected physical ports to the newly created logical port:

```
Netif Bindings
Port0 10.0.11.8/16 00:d0:b7:a9:52:f8 AUTO:AUTO(100:FULL)
Port1 unassigned/0 00:d0:b7:b9:f9:6a AUTO:AUTO(100:FULL)
Port2 unassigned/0 00:d0:b7:b9:f9:6b AUTO:AUTO(100:FULL)
OK Completed
```

```
Netif Bindlogical logical0 port0
OK Completed
```

```
Netif Bindlogical logical0 port1
OK Completed
```

The first port added to the logical port becomes the primary port. Once bound, you cannot change primary port using **Netif Set**. There is currently a limit of two physical ports per logical port.

4. Was the first-bound port previously associated with an IP address?
 - a. If so, the logical port was automatically bound to its IP address.
 - b. If not, associate the logical port with its assigned IP address:

```
Netif Bind logical0 10.0.11.18/16
```

The physical port that was bound second (port1) should not have an IP address assigned to it.

5. The **Netif Setlogical** command controls parameters of operation. For instance, you can select whether NIC failover continues to use the standby port after active port failure (**Activebackup**, the default) or whether the appliance switches back to the original active port when it becomes available again:

```
Netif Setlogical Mode logical0 Activefailback
```


Port failover can be forced by a `Netif Setlogical "" Failover` command.

A NIC failover event results in an “ALERT!” message being written to the System Log, which can be examined from the Logs & Reports page in the GUI. Currently the `Log` command in the CLI (and Administration protocol) does not support any identifiers related to NIC failover.

To test NIC failover, find a lightly-loaded or undeployed appliance. Follow the configuration instructions above. On the appliance back panel, disconnect the port1 Ethernet connector. Access the appliance with `telnet`, and observe messages in the System Log.

Using Security Quarantine

All content filters and the antispam scanning Allowed Senders, Blocked Senders, and Allowed Mailing Lists features offer a **Send to Quarantine folder** option. This option allows you to review any messages meeting those filter conditions using the Quarantine Administrator’s WebMail.

The Quarantine Administrator’s WebMail differs from the end-user WebMail in the addition of a **Deliver** button. The **Deliver** button releases back to the mail stream any selected messages that were quarantined by one of the filters. This button does NOT work on regular messages sent to the account. Messages that receive a **Send to Quarantine folder** filter action are specially handled so they can be released back to the mail stream and delivered to the intended recipients without any indication that they were ever quarantined.

If RAPID antivirus is licensed, the Quarantine Administrator’s WebMail also displays a **Virus Rescan** button. This button operates only on messages receiving the RAPID antivirus **Quarantine folder** action. The **Virus Rescan** button allows those selected messages to be released back to the mail stream and re-scanned by one of the signature-based antivirus engines.

Assigning the Quarantine Administrator Role

To use the **Send to Quarantine folder** filter action, the quarantine destination must belong to a user with the Quarantine Administrator role. The Quarantine Administrator periodically checks the specified

folder for quarantined messages and decides whether or not to release them for **Delivery**.

You can create any number of Quarantine Administrator accounts by creating an account and assigning the Quarantine Administrator role to it. See [“Managing User Accounts” on page 288](#) for details. To quarantine messages, you designate a folder that belongs to one of the Quarantine Administrator accounts in the **Send to Quarantine folder** (antispam) or **Quarantine folder** (RAPID antivirus) option. For example, if you have a Blocked Addresses Quarantine Administrator account named **BAQ**, entering **user.BAQ** in the **Send to Quarantine folder** option on the **Blocked Addresses** page will quarantine messages from blocked addresses to the Inbox of the BAQ account.

Educating Quarantine Managers

Which messages should a Quarantine Administrator release? It depends on which filter quarantined the message. For example, if the message is quarantined by the **Blocked Addresses** filter, the Quarantine Administrator probably shouldn't release it unless specifically requested to do so by a user.

Messages quarantined by RAPID antivirus should remain in quarantine long enough for your signature-based engines to update and those updates to get installed (by default, eight hours). Automatic release of RAPID-quarantined messages occurs eight hours after quarantining; this can be changed using the CLI. See **Help About Antivirus**. Messages quarantined by the signature-based antivirus scanners contain live viruses and should never be released to the mail stream.

Using Junk Mail Manager (JMM)



The Junk Mail Manager (JMM) feature is a licensed software option that quarantines mail categorized as junkmail, and allows non-WebMail users to access and manage their quarantined junkmail. If Junk Mail Manager is not licensed and enabled; this link does not display. Junk Mail Manager is only licensed on RazorGates. This chapter provides details on JMM administration; the following topics are included:

- ◆ [Modifying Junk Mail Manager](#): How to make changes to your JMM configuration.
- ◆ [Administering Junk Mail Domains](#): How to add and administer JMM domains.
- ◆ [Bulk Account Provisioning for JMM](#): How to create a file for use with JMM Bulk Create Accounts.

Full details on initial setup of JMM, including important background information, are given in the [Chapter 4, “RazorGate with Junk Mail Manager Security Deployment for Exchange.”](#) Please read that chapter for set up information.

About Junk Mail Manager

Junk Mail Manager can reside on the same machine that performs mail security functions (MailHurdle and antispam scanning) and acts as the IMR, split off from the IMR with the mail security functions, or split into a completely separate JMM tier. The functions that a JMM host

performs is an important factor in determining where filters and lists should be configured.

For example, **Allowed Mailing Lists** should always be configured on the machine that acts as the MailHurdle. Safelists on a JMM that only receives messages already categorized as junkmail are not very useful.

Junk Mail Manager sends users a summary email of their quarantined junkmail with functions that allow them to act directly on the junkmail without logging in to Junk Mail Manager itself. Most users manage their junkmail through these summary messages instead of logging in to Junk Mail Manager.

Junk Mail Manager provides an interface, `http://hostname/spam`, for users to access and manage their quarantined junkmail. Once configuration is complete, users receive a **Welcome** email message, that you can configure, that includes an option to opt-out of JMM; if they do so, all of their junkmail is delivered directly to them.

Users who use Junk Mail Manager to manage their junkmail receive summary reports of all quarantined messages by default. While they can choose to not receive these emails, it should be highly discouraged—users should regularly check their quarantined junkmail for mis-categorized messages (false positives). For information about using Junk Mail Manager, see the Junk Mail Manager online Help.

What is a Junk Mail domain?

A JMM domain is an Internet domain name for which Junk Mail Manager stores and manages spam messages. It is always associated with a JMM host and a mail host. The name should match your mail domain names; for example, mail domain **example.com** would be entered as JMM domain **example.com**. One important difference between regular mail or delegated domains and Junk Mail domains is the default system junkmail filter or “rule”; this filter on JMM domains always sends junkmail to JMM instead of using the user-configured Junk Mail filter.

What's the difference between a local Junk Mail domain and a remote Junk Mail domain?

A local Junk Mail domain is one configured on the machine; a remote Junk Mail domain is configured on a different machine. You can administer local Junk Mail domains on the **Junk Mail Manager > Junk Mail Domains** pages. You must go to the Junk Mail Manager host for a remote domain to administer it.

Why does JMM configuration change with routing options?

If you are using LDAP routing, the LDAP attributes (discussed in [“Junk Mail Manager LDAP Records” on page 446](#)) provide the **Account Default** settings, so they are not available on the **Configuration** page. If you are using Local Routing Table, you cannot configure Remote Junk Mail domains, so those options are not available on the **Configuration** page. Only the options necessary for the selected routing method display.

In what order are JMM filters and lists applied?

Junk Mail Manager only applies filters and lists to configured Junk Mail domains—but it does apply those filters and lists for ALL mail coming to those domains through it (not just junkmail). If other antispam scanning is done upstream, JMM antispam scanning overrides previous spam scores. Messages that once receive a quarantine filter action are no longer subject to further quarantine actions.

How Junk Mail Manager Quarantine Works

Junk Mail Manager uses the Quarantine filter action in its system default Junk Mail filter. The default system junkmail filter cannot be modified at this time. In this special, system default junkmail filter, the Quarantine action is set to send matching messages (those categorized by the antispam scanner as junkmail) to the Junk Mail Manager interface.

For information on the Content Filtering quarantine action, see [“How the Content Filtering Quarantine Works” on page 337](#).

For information on the Anti-Virus quarantine, see [“How Antivirus Quarantine Works” on page 398](#).

Junk Mail Manager LDAP Records

These are the Mirapoint schema LDAP records that are required for Junk Mail Manager to work correctly. If you do not use Mirapoint schema, you must enter equivalent records into your LDAP.

These are the mandatory records:

- ❖ mailhost
- ❖ mi quarantinehost
- ❖ micosdn: cn=Junkmail_Manager_default_cos
- ❖ miservice: msgexpiration
- ❖ miservice: quota
- ❖ miservice: antispam
- ❖ miservice: junkmailmanager
- ❖ mimailquota
- ❖ mimailexpirepolicy: QTNBOX.* 14 I
- ❖ midefaultjunkmailfilter::
I0BNaXJhcG9pbmQtRmlsdGVyLTEuMA0KZmlsdGVyICJTeX
N0ZW0g
SnVuayBnYWlsIFJ1bGUiIFF1YXJhbWUgIlFUTkJPWC5
KdW5rIE1haWwiIGFsbG9mIHN0b3ANC
jpVQ0UgaXMgIm5vcmlhbCINCg==

Note: In the CLI, the filter would look like this:

```
#@Mirapoint-Filter-1.0
filter "System Junk Mail Rule" Quarantine "QTNBOX.Junk Mail"
allof stop
:UCE is "normal")
```

After generating the rule, use any base64 encoding program to encode it and then add it to the **midefaultjunkmailfilter** LDAP attribute.

The following is an example.

```
dn: o=mira_route_top
objectclass: Organization
o: mira_route_top

dn: ou=domains,o=mira_route_top
```

```

objectclass: OrganizationalUnit
ou: domains

dn: miDomainName=primary,ou=domains,o=mira_route_top
objectclass: miDomain
midomainname: primary

dn: miDomainName=demo.com, ou=domains, o=mira_route_top
objectclass: miDomain
midomainname: demo.com

dn: mail=@demo.com, miDomainName=demo.com, ou=domains, o=mira_route_top
cn: domain entry
objectclass: mirapointUser
objectclass: mirapointMailUser
mail: @demo.com
mailhost: example0.mirapoint.com
miquarantinehost: example.mirapoint.com
micosdn: cn=Junkmail_Manager_default_cos, miDomainName=primary, ou=cos,
o=mira_route_top

dn: ou=cos,o=mira_route_top
objectclass: OrganizationalUnit
ou: cos

dn: miDomainName=primary,ou=cos,o=mira_route_top
objectclass: miDomain
midomainname: primary

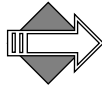
dn:
cn=Junkmail_Manager_default_cos,miDomainName=primary,ou=cos,o=mira_route_top
miservice: msgexpiration
miservice: quota
miservice: antispam
miservice: junkmailmanager
objectclass: miClassOfService
cn: Junkmail_Manager_default_cos
mimailquota: 0
mimailexpirepolicy: QTNBOX.* 14 I
midefaultjunkmailfilter:: I0BNaXJhcG9pbmQtRm1sdGVyLTEuMAOKZm1sdGVyICJTeXN0ZW0g
SnVuayBNYW1sIFJ1bGUiIFF1YXJhbnRpbmUgI1FUTkJPWC5KdW5rIE1haWwiIGFsbG9mIHN0b3
ANC jpvQ0UgaXMgIm5vcmlhbCINCg==

```

Modifying Junk Mail Manager

Use the **Junk Mail Manager > Configuration** page to enable/disable Junk Mail Manager and enable/disable the summary emails. If you are using Local Routing Table for routing, you can also set basic mail store defaults for the quarantining of junkmail here. If you are using LDAP

for routing, you can set remote Junk Mail Domains (those not local to the machine) here; however, you can only administer Junk Mail Domains local to the machine on the **Junk Mail Domains** pages.



Before you begin configuring Junk Mail Manger, you should have the following information:

- ◆ The names of any remote Junk Mail domains and, if any, the Junk Mail Manager enabled hosts for each. Enter this information on the **Junk Mail Manager Configuration** page.
- ◆ The names of all the mail domains, and their hosts, whose junkmail you want Junk Mail Manager to quarantine. Each mail domain must be entered to Junk Mail Manager as a Junk Mail domain; for example, for mail domain “example.com” enter **Junk Mail Domain** “example.com” on the **Administer Local Junk Mail Domains** page.
- ◆ A text file to bulk-import user accounts for Junk Mail Manager; details on the syntax required for this file and how to import it are given on [“Bulk Account Provisioning for JMM” on page 461](#).

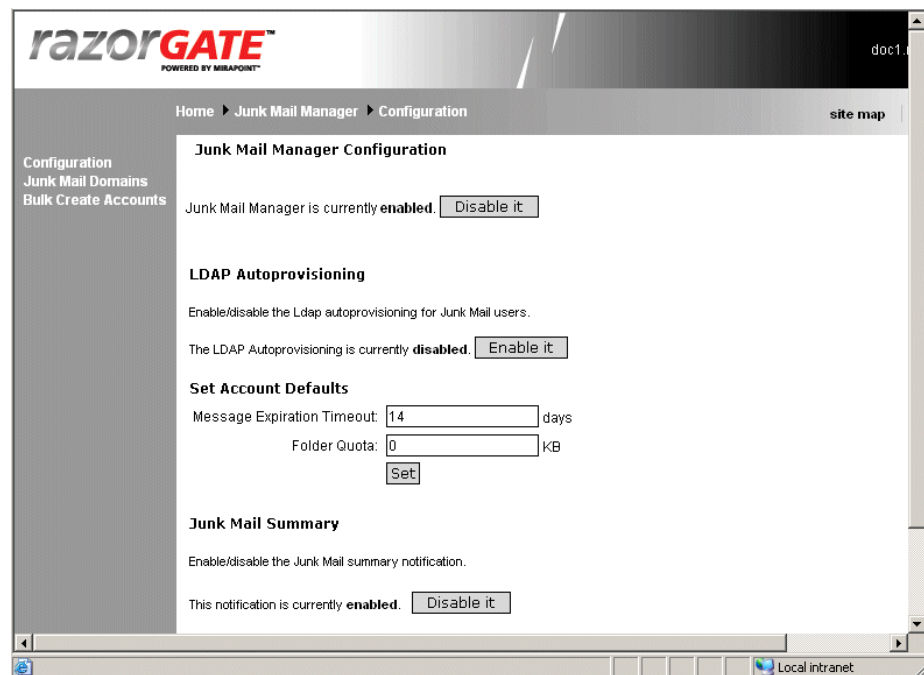


Figure 94 RazorGate Junk Mail Manager > Configuration Page

To configure Junk Mail Manager, follow these steps on the **Junk Mail Manager > Configuration** page. See Figure 94 for an example.

1. If the utility is not already enabled, an **Enable it** button displays; click it to enable the utility. If the utility is enabled, a **Disable it** button displays, click it to disable the utility.
Result: Depending on your action, the utility is enabled or disabled; the utility must be enabled before configuration can begin.
2. Set **Account Defaults for Local Routing Table** routing (**Note:** These options do NOT display if you are using LDAP routing):
 - ❖ **Message Expiration Timeout:** Enter an integer for the amount of time a message can be quarantined in a single user's Junk Mail Manager account. The default timeout is 14 days; it is recommended that this be set to no less than 10 days (the equivalent of a week plus two weekends).
 - ❖ **Folder Quota:** Enter an integer for the amount of megabytes that can accumulate in a single user's Junk Mail Manager account quarantine folder, or leave blank for no quota (recommended). Set to -1 to remove a quota.
3. Set **Remote Junk Mail Domain to Host Mapping** for LDAP routing: For each Junk Mail Manager domain located on a different Junk Mail Manager, enter the following:
 - ❖ **Remote Junk Mail Domain:** The mail domain whose junkmail the remote Junk Mail Manager is to handle. These should be first configured on the remote Junk Mail Manager.
 - ❖ **Junk Mail Manager Host:** The name of the Junk Mail Manager machine for that remote Junk Mail domain.
 - ❖ **Mail Host:** The machine that receives the non-junkmail for that remote Junk Mail domain. **Note:** This option only displays when Active Directory routing is being used.
4. Enable or disable the **Junk Mail Summary**: The summary notification emails are enabled by default. If you disable the summaries, users must log in to Junk Mail Manager to manage their junkmail.
5. In the **Junk Mail Summary Custom Schedule** area, select hours and click **Add** or **Remove** to create a custom schedule that end-users can select on the **Junk Mail Manager Summaries** page.

Administering Junk Mail Domains

Use the **Junk Mail Domains** page to tell Junk Mail Manager what domains have accounts for which Junk Mail Manager is to quarantine junkmail; in other words, any mail domain. Also, select Junk Mail domains for administration, including antispam scanning options.



This page also allows you to select a Junk Mail domain for administration. You must select a domain and click **Select Domain** before you can administer it.

Configuring **Junk Mail Domains** involves the following tasks:

- ◆ **Administering Junk Mail Domains:** Add, find, select, or delete Junk Mail Manager domains. You must select a domain (click **Select Domain**) to administer it.
- ◆ **Managing Junk Mail Domain Accounts:** Add, find, edit, or delete Junk Mail Manager accounts.
- ◆ **Setting the JMM Welcome Message:** Customize the Welcome message for new Junk Mail Manager accounts.
- ◆ **Setting the JMM Over-Quota Message:** Customize the Over-Quota message for Junk Mail Manager accounts that have exceeded their quota.
- ◆ **Setting the JMM Allowed Senders List:** Create or edit Junk Mail domain safelists. Messages sent from addresses on the Allowed Senders List are never categorized as junkmail.
- ◆ **Setting the JMM Blocked Senders List:** Create or edit Junk Mail domain blocklist. Messages sent from addresses on the Blocked Senders List are always categorized as junkmail.
- ◆ **Setting the JMM Allowed Mailing Lists List:** Create or edit Junk Mail domain allowed mailing lists. Messages sent to recipients on the Allowed Mailing Lists list are never categorized as junkmail).
- ◆ **Creating JMM Message Filters:** Create or edit Junk Mail domain message filters.

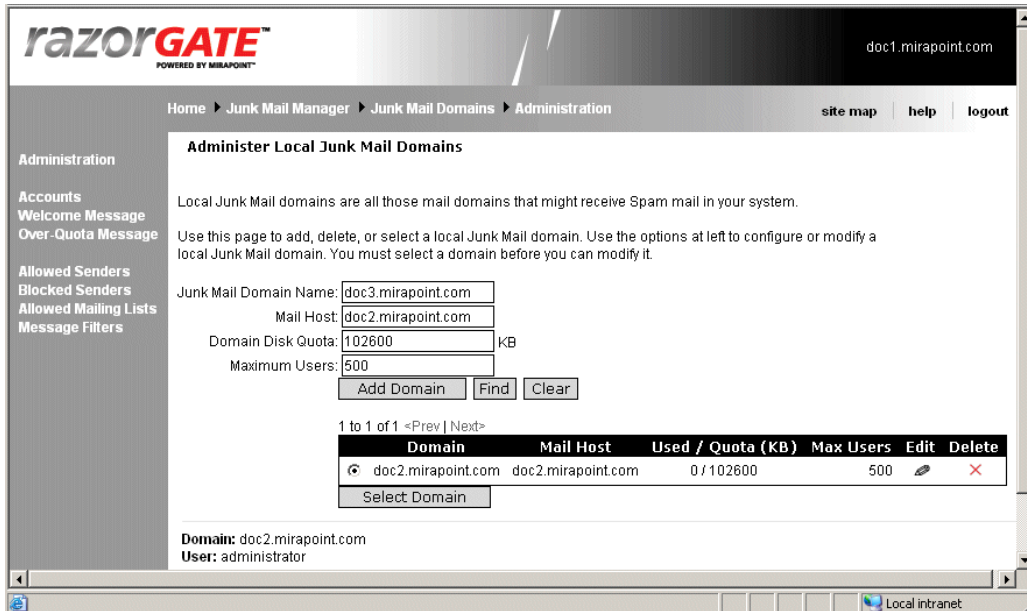


Figure 95 RazorGate Junk Mail Manager Domains Page

Adding Junk Mail Domains

To add a Junk Mail domain follow these steps on the **Junk Mail Manager > Administer Local Junk Mail Domains** page; see Figure 95 for an example.


1. Enter into the **Junk Mail Domain Name** option the domain name of each mail domain in your system and click **Add Domain**
Result: The filter looks only at the mail addressed to the selected domain. See [“About the Destination Domain Options” on page 332](#) for details on this option.
2. To find a Junk Mail domain, enter the entire domain name or use the wildcard asterisk (*) to match any sequence of zero or more characters into the **Junk Mail Domain Name** text box. For example, **fo*** finds domain **foo.com**, domain **foods.com**, domain **folly.com**, and so forth. Click **Find**.
Result: The specified name appears in the domain list. Enter the asterisk (*) wildcard in the **Find Domain** text box and click **Find** to display all of the Spam domain names on the system.

Selecting a Junk Mail Domain

To modify or administer a Junk Mail domain, you must first select it by selecting the radio button for the domain and clicking **Select Domain**. When you do this, the **Domain** *domain name* indicator in the bottom left corner of the all of the **Junk Mail Domains** pages is updated to show the currently selected domain. Once you've selected a Junk Mail domain, any changes you make using the **Junk Mail Domains** pages act only on that domain. For example, if you select the Junk Mail domain **qtn.example.com** and then create a user, **george@example.com**, you create a Quarantine folder on the **qtn.example.com** Junk Mail domain that receives junkmail sent to **george@example.com**. To manage his junkmail, George accesses his **qtn.example.com/spam** folder.

Deleting Junk Mail Domains

Use the **Junk Mail Manager > Administer Local Junk Mail Domains** page (see Figure 95 for an example) to delete JMM domains.

Click the **Delete** icon  for any domain you want to remove from the system; click **Prev** and **Next** to page through the list of domains.

Click **OK** to enter your changes.

Managing Junk Mail Domain Accounts

Use the **Junk Mail Domains > Accounts** page to add or modify Junk Mail Manager accounts, or to add, find, rename, or delete an account. Be sure to click **Select Domain** before you begin.

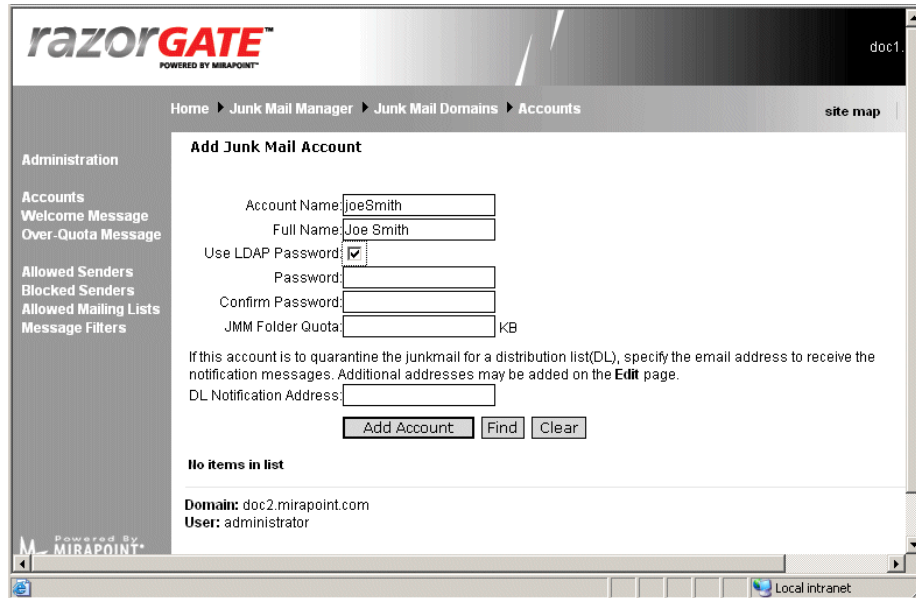


Figure 96 RazorGate Junk Mail Manager Accounts Page

A Junk Mail Manager **account** consists of a login—name and password, and a main folder—quarantine.*username*. The user’s login name is used as the address for their Quarantine folder. By default, Junk Mail Manager user folders reside in the system folder called **quarantine**.

When a user logs in to the Junk Mail Manager, they see only their **Quarantine** account folder (**My Junkmail**). Users can perform the following junkmail management tasks using the Junk Mail Manager:

- ◆ Change their own Junk Mail Manager account password
- ◆ Set message filters and some Junk Mail Manager options

About Junk Mail Accounts for Distribution Lists

Junk Mail Manager can also manage the junkmail for a distribution list (DL); in this case, a DL is treated as an account. The expansion of the

DL to member's email addresses happens after Junk Mail Manager processing.

To add a DL account, enter the name of the DL in the **Account Name** field (see [“Adding Junk Mail Domain Accounts” on page 454](#) for details); then enter an email address for the DL owner in the **DL Notification Address** field; you can add multiple DL owners. The Welcome message, with login information, goes to all the DL owners. The junkmail summaries go to all the DL owners. If a DL owner clicks **Deliver**, the message is sent to all members of the DL. If a DL owner clicks **Approve**, the message is sent to all members of the DL and the sender is added to the DL account's Allowed Senders list. All of the DL owners can log in and manage the account.

Adding Junk Mail Domain Accounts

Use the **Add Junk Mail Account** page (see Figure 96 for an example) to add, find, or modify Junk Mail Manager users, including setting folder quotas, and assigning a notification message when appropriate. Follow these steps.

1. To add a Junk Mail Manager user, select the Junk Mail Domain first (click **Select Domain**) and enter the following data:
 - ❖ **Account Name:** This name becomes the name of that user's folder under the **qtn** system directory, the first part of their Junk Mail Manager quarantine email address, and their login name. If the account is for a DL, enter the DL name here.
 - ❖ **Full Name:** This name is displayed in messages alongside the user name.
 - ❖ **Password:** A password for the user. A password is a secret text string (numbers and letters) that is case sensitive and up to 80 characters long.
 - ❖ **Confirm Password:** Enter the password again.
 - ❖ **Folder Quota:** A quota for that user's Quarantine folder; all of their subfolders are included in the total set quota. You can completely remove a quota from a folder by entering **-1**.
 - ❖ **DL Notification Address:** The email address where notifications of junkmail quarantined for a distribution list should go. This

address receives a Welcome message with a login to manage this Junk Mail Manager account.

2. To find an existing Junk Mail Manager user account, enter a name in the **Account Name** text box, and click **Find**. **Note:** You can use the asterisk (*) wildcard, for any kind of character including the folder hierarchy separator dot (.), or the percent sign (%) wildcard, for any kind of character NOT including the folder hierarchy separator dot (.). Click **Clear** to empty the options of any text that you have entered and re-display the entire user list (ten names display at a time).

Result: The list box below displays the find results.

3. Click **Add Account**.

Result: The system creates an account in Junk Mail Manager for that user, and the name moves to the list box. Incoming mail for that user that is categorized as junkmail is sent to this account.

Repeat step 2 as necessary to add more users.




Important! Be sure to set up your mail accounts on the mail hosts before creating JMM accounts as the Welcome Message is sent the instant each account is created.

Editing Junk Mail Domain Accounts

Use the **Add Junk Mail Account** page (see Figure 96 for an example) to change a Junk Mail Manager user password, folder quota, or distribution list owner notification. Follow these steps.

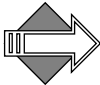
1. Click **Prev** and **Next** to page through the list of names, as needed.

Or enter an account name and click **Find**. Click the **Edit** icon  for the account you want to modify.

Result: The **Edit Junk Mail Account** page displays with that user's data.

2. Make the changes you want and click **OK** or **Cancel**.


Result: If you click **OK**, the page displays a message confirming the modification. If you click **Cancel**, the **Add Junk Mail Account** page re-displays, your changes to that user are not made.



You can completely remove a quota from a folder by entering -1.

Deleting Junk Mail Domain Accounts

Use the **Add Junk Mail Account** page (see Figure 96 for an example) to delete a Junk Mail Manager user account. Follow these steps.

1. Click **Prev** and **Next** to page through the list of names, as needed. Select the name in the user list you want to remove. Click the **Delete** icon  next to it.
Result: A **Confirmation** page displays.
2. Click **Delete** or **Cancel**.
Result: If you click **Delete**, the name disappears from the list. If you click **Cancel**, you are returned to the **Add Users** page, your deletion is terminated.

Setting Up Junk Mail Manager Content Filtering

Junk Mail Manager typically runs on a separate machine from the mail server. Content filters can be set up to work with Junk Mail Manager.

Setting the JMM Allowed Senders List

Once you have added a new, or selected an existing, Junk Mail domain; use the Junk Mail Manager **Allowed Senders** page to ensure that mail from certain senders is always sent to recipients and never classified as junkmail.

This page works in an identical manner to the **Anti-Spam > Allowed Senders** page, see [“Setting the Allowed Senders List” on page 425](#) for details.

Setting the JMM Blocked Senders List

Once you have added a new, or selected an existing, Junk Mail domain; use the **Blocked Senders** page to specify certain addresses that should never have mail received at that Junk Mail domain.

This page works in an identical manner to the **Anti-Spam > Blocked Senders** page, see [“Setting the Blocked Senders List” on page 428](#) for details.

Setting the JMM Allowed Mailing Lists List

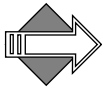
Once you have added a new, or selected an existing, Junk Mail domain; use the **Allowed Mailing Lists** page to ensure that mail from certain senders is always sent to recipients and never classified as junkmail.

This page works in an identical manner to the **Anti-Spam > Allowed Mailing Lists** page, see [“Setting the Allowed Mailing Lists List” on page 431](#) for details.

Creating JMM Message Filters

Once you have added a new, or selected an existing, Junk Mail domain; use the **Add Message Filters** page to create custom filters and manage your existing filters.

This page works in a similar manner to the **Content Filtering > Advanced Content Filtering** page, see [“Creating a Message Filter” on page 339](#) for details.



The difference between the two pages is that for **Junk Mail Domains > Message Filters** you do not have the option of directing the filter towards a Destination Domain because the filter you create here applies only to the Junk Mail domain that you have selected or logged in to. To create a system-wide filter, use the **Content Filtering > Advanced** page, not the **Junk Mail Domains > Message Filters** page.

Setting JMM Notification Messages

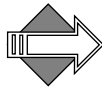
Junk Mail Manager Welcome Message and Over-Quota Message should be customized before deployment.

The Junk Mail Manager Welcome message announces to your users that their junk mail is being managed in a new way. It includes a default password for each user and links to Junk Mail Manager, and explains the Summary messages.

The Over-Quota message warns Junk Mail Manager users that their junk mail account is getting full and some messages must be deleted.

Setting the JMM Welcome Message

You use the **Junk Mail Domains > Welcome Message** page to customize the message that is delivered when a user's Junk Mail Manager account has been created. You can also select the character set used to encode the message. For example, if you select ISO-2022-JP and Japanese characters are used, the message is encoded in the ISO-2022-JP character set.



The Welcome message you customize here is associated with the domain that you select in **Junk Mail Domains > Administration**.

razorGATE™
POWERED BY MIBAPPOINT™

Home ▶ Junk Mail Manager ▶ Junk Mail Domains ▶ Welcome Message site

Administration

Accounts
Welcome Message
Over-Quota Message

Allowed Senders
Blocked Senders
Allowed Mailing Lists
Message Filters

Set Welcome Message

For the selected domain, create a custom welcome message that users will receive when their accounts are created. If a brand with a custom message is used by that domain.

This notification is currently **enabled**.

From: Administrator@\$(host)

Subject: Welcome to your new Junk Mail Manager account

Message:

```
<html>
<body>
Welcome to Junk Mail Manager and the new junkmail
management
services that are now being provided for your
email account.
Junk Mail Manager scans incoming messages and
quarantines
those categorized as spam (junkmail).<br><br>
Periodically, Junk Mail Manager will send you a
summary log with
links to the quarantined messages. A junkmail
account has been set up
for you on Junk Mail Manager to access those
messages and control
```

Charset: Western European (ISO-8859-1)

Local intranet

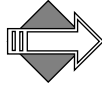
Figure 97 RazorGate Junk Mail Manager Welcome Message Page

To customize a Junk Mail domain's welcome message follow these steps.

1. Select the Junk Mail domain, as described in [“Selecting a Junk Mail Domain” on page 452](#).
Result: The selected JMM domain is available for modifications.
2. Click **Welcome Message**.
Result: The **Set Welcome Message** page displays; see Figure 97.
3. If the welcome message is not already enabled, an **Enable it** button displays; click it to enable the welcome message. If the welcome message is enabled, a **Disable it** button displays, click it to disable the welcome message.
Result: Depending on your action, the message is enabled or disabled; the message must be enabled before customizing.
4. Customize the text in the **From**, **Subject**, and **Message** text fields as desired. You can also select a character set for the message from the drop-down list. The default is UTF-8.
5. Click **Apply**.
Result: The message you entered, along with the character set you specified (if any), is sent to users when their Junk Mail Manager account is created.
6. To revert to the default welcome message, click **Restore Default**.
Result: The default system welcome message and character set is sent to users when their account is created. **Note:** if the domain is assigned to a named brand, clicking **Default Message** causes that named brand's welcome message to be sent to users when their quota is reached.

Setting the JMM Over-Quota Message

Use the Junk Mail Manager **Over-Quota Message** page to customize the warning message that is delivered when a user's folder has gone over its allocated size limit. You can also specify the **From** field and select the character set used to encode the message. For example, if you select ISO-2022-JP and Japanese characters are used, the message is encoded in the ISO-2022-JP character set.



The over-quota message you customize here is associated with the Junk Mail domain that you select on the **Junk Mail Domains > Administration** page.

Figure 98 RazorGate Junk Mail Manager Over-Quota Message Page

To customize a JMM domain's over quota message, follow these steps.

1. Select the current domain, as described in [“Selecting a Junk Mail Domain” on page 452](#).
Result: The selected JMM domain is available for modifications.
2. Click **Over-Quota Message**.
Result: The **Set Over-Quota Message** page displays; see Figure 98.
3. Customize the text in the **From**, **Subject**, and **Message** text fields as desired. You can also select a character set for the message from the drop-down list. The default is UTF-8.

4. Click **Apply**.
Result: The message you entered, along with the character set you specified (if any), is sent to Junk Mail Manager accounts when their quota is exceeded.
5. To revert to the default over-quota message, click **Restore Default**.
Result: The default Junk Mail Manager over-quota message and character set is sent to users when their quota is reached.

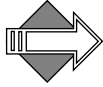
Bulk Account Provisioning for JMM

The **Bulk Create Accounts** page lets you import a text file containing information about your existing user accounts. For information on creating an acceptable accounts file, see [“Converting LDAP for JMM Accounts Bulk Import”](#).



Figure 99 RazorGate Junk Mail Manager Bulk Create Accounts Page

The format of the file is a newline separated text file containing the fully qualified email address of each account. Additionally, for each account, you can include the fullname and password. If you do not include the fullname, the system uses the fully qualified email address to derive a name. If you do not include the password, the system creates a random password for the account and includes that password in the **Welcome** message. For information on Welcome messages, see [“Setting the JMM Welcome Message” on page 458](#).



Note: You must have already created your Junk Mail domains before bulk creating accounts. For details on creating Junk Mail domains, see [“Adding Junk Mail Domains” on page 451](#).



Important! Be sure to set up your mail accounts on the mail hosts before creating JMM accounts as the Welcome Message is sent the instant each account is created.

Bulk Creating JMM Accounts

Use the **Bulk Create Accounts** page (see Figure 99 for an example) to bulk create Junk Mail Manager accounts. First, ensure that the format of the text file you have with account information uses the correct syntax:

The format of the input file for **Bulk Create Accounts** (see annotated examples, below), must be:

```
fully qualified email address [fullname "password"]
```

where:

- ❖ *fully qualified email address* is the host name plus the domain name; for example, user@demo.com
- ❖ [] the brackets indicate where you can include optional arguments--do not include the bracket characters
- ❖ *fullname* is the user's first and last names, enclosed in quotes to allow for spaces
- ❖ *password* is the user's password; if left empty ("") the system generates a random password.

Note: The *password* argument can be used to specify whether the authentication for these accounts is via non-local or local passwords. If authentication is via a non-local password, the *password* argument should contain one of the valid authentication schemes; for example, PLAINTEXT:LDAP. Please refer to Mirapoint [Administration Protocol Reference](#) AUTH chapter for the rest of the schemes.

Here are some annotated examples of the lines you can specify in the input file:

joe@example.com

There is no password included; Junk Mail Manager generates a random password for this user.

joe@example.com "" ""

There are empty strings (" " ") instead of the AUTH type and password, Junk Mail Manager generates a random password for this user.

joe@example.com "Joe Smith" "joepassword"

Junk Mail Manager uses the specified full name and password for this user.

joe@example.com "" "joepassword"

Junk Mail Manager uses the specified password for this user; the account has no full name.

joe@example.com "Joe Smith" ""

Junk Mail Manager uses the specified full name and generates a random password for this user.

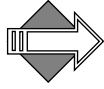
joe@example.com "Joe Smith" "PLAINTEXT:LDAP"

Junk Mail Manager uses the specified full name and password AUTH type and database for this user.

Once the accounts file is set up properly, on the **Bulk Create Accounts** page, enter the **Filename** of the file that contains the user account data, in the format described above, that you want to import, or use the **Browse** button to find the file, and click **Create Accounts**.

Result: A message displays indicating the completion or any problems.

You must create domains in Junk Mail Manager before attempting to bulk create accounts. Once you specify the bulk create accounts file and click **Create Accounts**, the system parses your input file and creates accounts based on the **user name**, **domain name**, **fullname** and **password** scanned from each line. If the domain doesn't exist, the system stops the process and displays an error on the page. If the user or folder already exists, the system skips to the next line. If the password field is "" (empty string) or **PLAINTEXT:LOCAL**, the system generates a password for the user and that is included in their Welcome message. For the non-local password, the system displays in their Welcome message a note that their password is, "Their regular password."



Note: Double quotes are not allowed in the fields. For example, the following entry creates an account with the fullname "A \"

```
user1@dom1.com "A \"Test\" account" ""
```


Using the Operations Console

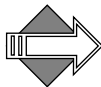
Use the Mirapoint Operations Console (OC) to create groups of machines, assign a master, and replicate the configuration of the master throughout the group.



The OC is a licensed feature that is generally run on the master directory server, if one exists. In large-scale deployments, it can be run on a separate appliance. In smaller deployments, it can run on the Message Server. It should not be run on an edge device unless no other option exists. Only one OC is needed within the messaging infrastructure regardless of the size of the deployment.

The following topics are included:

- ◆ [Managing Operations Console Groups](#): How to create and administer groups.
- ◆ [Using the Operations Console Dashboard](#): How to use the dashboard to monitor and act on existing groups.
- ◆ [Using Operations Console Alerts](#): Operations Console alerts you might see and what to do.



Enable HTTP SSL (see [“Adjusting Administration Security” on page 50](#)) to ensure that the **OC Dashboard** uses SSL when accessing the managed hosts. This is because each time data is retrieved from a host, the login and password are transmitted.



The master of any group must be configured using the Administration Suite or CLI before being made a group master. The master's configuration can then be synchronized to the rest of the group. The master's configuration can be modified through the OC and the other

members of that group re-synchronized at any time. Those options described in [“Administering Groups” on page 469](#) can be synchronized.

You access the OC through the **ocadmin** login page on the appliance hosting the OC. For example, <http://miServer/ocadmin>.

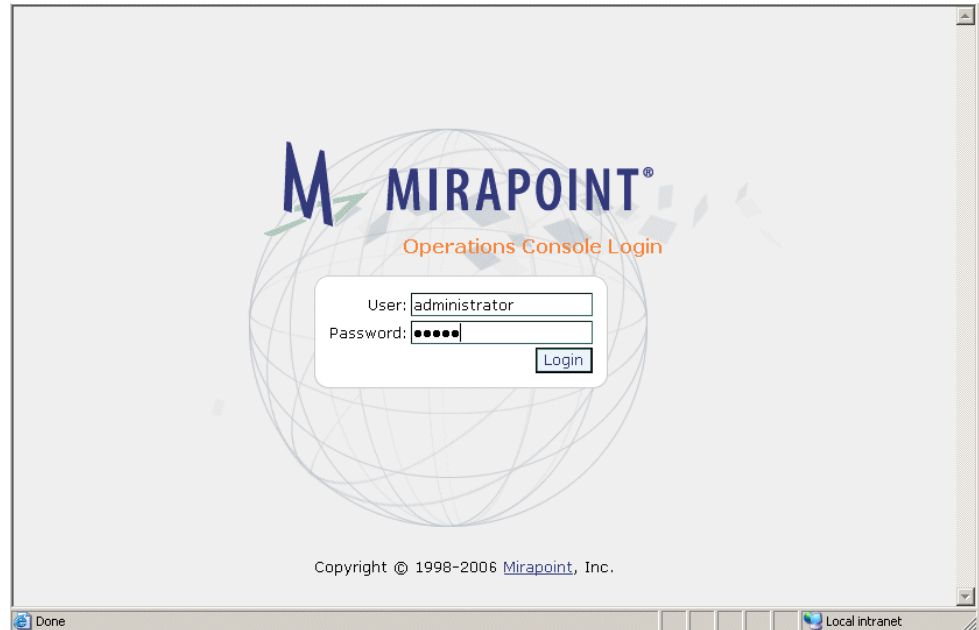



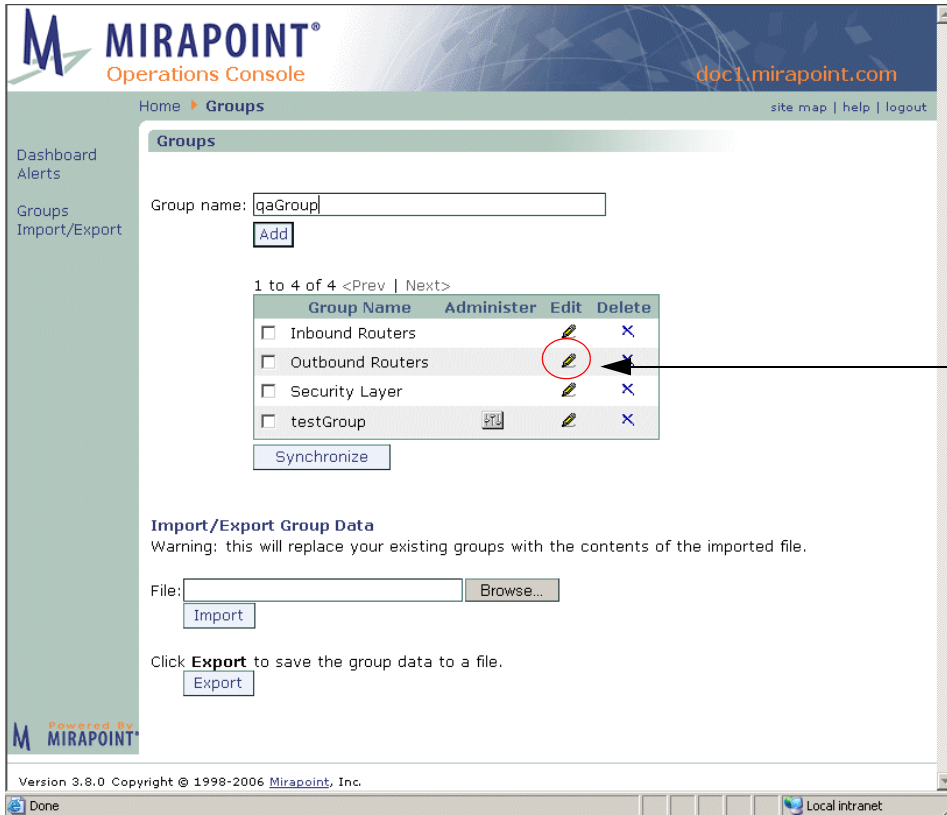
Figure 100 Mirapoint Operations Console Login Page

Managing Operations Console Groups

Use the **Groups** page to add and delete groups of hosts and also to access the **Administer-Home** view for a group member. Using the **Administer-Home** view, you can configure the system **Interface**, **Time**, and **Services**, and the **Anti-Virus**, **Anti-Spam**, and **Content Filtering** options for a group master and then synchronize that configuration to

all of the members of that group; see [“Synchronizing Groups” on page 471](#) for details.

Click the **Administer** icon  to open the **Administer-Home** page for a group’s master. **Note:** The **Administer** icon does not display for groups without members. See [“Administering Groups” on page 469](#) for details.



Click here to edit a group

Figure 101 Operations Console Groups Page

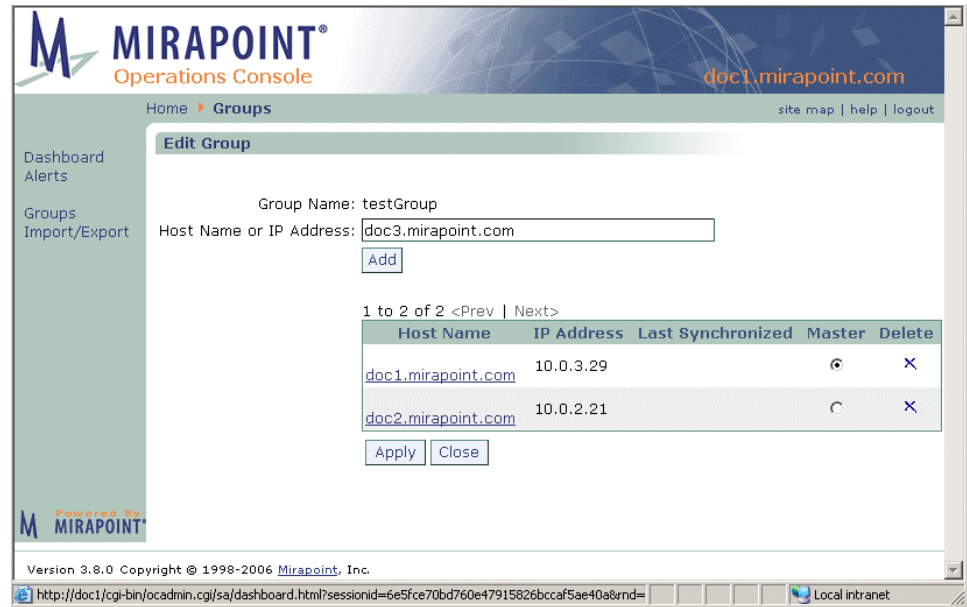


Figure 102 Operations Console Edit Groups Page

Adding, Editing, and Deleting Groups

The groups list is limited to 10 hosts; the number of groups you can create is limited to 5. Each group name must be unique.




The administrator's account name and password for each managed host must be the same as the account name and password used to log into the OC. Only hosts running Messaging Operating System (MOS) 3.4 or later are allowed onto the list. A given host name can only appear in one group (to avoid cyclical synchronization issues).

The Operations Console defines three default group: **Inbound Routers**, **Outbound Routers**, and **Security Layer**. You must edit each group to

add members, including the master—the default groups are initially empty.


To create a group:

1. On the **Groups** page (see Figure 101) enter a name for the new group and click **Add**.
2. Click the **Edit** icon  for the new group to open the **Edit Groups** page to configure the group (see Figure 101 for an example).
3. On the **Edit Groups** page, shown in Figure 102, add the machines that you want in the group. For each machine, enter its host name or IP address and click **Add**.
4. When you are finished adding machines to the group, click **Apply** to save your changes. Click **Close** to return to the **Groups** page.


By default, the first machine you add to a group is the **Master** machine. The master machine's configuration is replicated to the other machines when you synchronize the group. To change the **Master** in a group, go to the **Edit Groups** page, select the **Master** button for the machine that you want to use as the master, and then click **Apply**.

To view the Dashboard page for a particular machine, you can click the **Host Name** link in the hosts list on the **Edit Groups** page.

To copy the configuration from the master machine to the rest of the machines in a group, select the group on the **Groups** page and click the **Synchronize** button. The master configuration is sequentially pushed via HTTPS to each replica in the group.

You can remove a group from the system by going to the **Groups** page and clicking the **Delete** icon  for the group you want to remove.

Administering Groups

Click the **Administer** icon  on the **Groups** page to configure the master of the selected group. This displays the **Administer-Home** pages that enable you to configure the master system through the OC. You use these pages to edit the properties of the master system that you want

to propagate to the replica members of the group when the group is synchronized.

When you're done configuring the master, use the **Synchronize Groups** link to push your changes to the replicas. See [“Synchronizing Groups” on page 471](#) for details.




Important! When you click the **Administer** icon , you enter the **Administer-Home** pages. These pages operate exactly like the regular administration pages, but you must deliberately exit the **Administer-Home** pages to return to the Operations Console. To exit the **Administer-Home** pages, click the **Synchronize Groups** link and click **Synchronize Groups** to propagate your changes to the group and return to the **Groups** page, **Continue** to return to the **Groups** page without synchronizing the group, or **Cancel** to discard your changes and return to the **Groups** page.



Figure 103 Operations Console Administer-Home View of Group Master

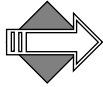
For details on using these administration options, see the following:

- ◆ [“Using Antivirus Scanning” on page 396](#)

- ◆ [“Using Antispam Scanning” on page 416](#)
- ◆ [“Managing Content Policies \(Domain Filters\)” on page 332](#)

Synchronizing Groups

Clicking the **Synchronize** button on the **Groups** page causes the OC to sequentially take the configuration of the master of each selected group, and push that configuration via HTTPs to each of the replicas in that group.



Note: When in the **Administer-Home** view, click the **Synchronize Groups** link on the **Administer-Home** page to open the **Synchronize Groups** page where you can click one of these buttons:

- ◆ **Synchronize Groups:** Instantiates your changes and returns you to the **Groups** page.
- ◆ **Continue:** Rejects your changes and returns you to the **Groups** page.
- ◆ **Cancel:** Returns you to the initial **Administer-Home** page for that group’s master.

Importing and Exporting Groups

The **Groups** page **Import/Export Group Data** facility (see Figure 101) lets you share group data, which consists of the names of your groups and which machines are in each group. You might also want to export the group data to store a backup copy.

When you export a group, the data for all your defined groups is exported to a **.grp** file. When you import a group file, the group data in that file overwrites the existing data for all configured groups with the same names.

To export your group configuration data, click the **Export** button.
Result: Your browser prompts to you save the file.

To import a group file, specify the name of the **.grp** file that contains the group configuration data that you want to import, or use the **Browse** button to find the file, and then click **Import**.

Result: A message displays to indicate that the import process is complete or report problems with the import.

Using the Operations Console Dashboard

The **Dashboard** page shows all the groups, their hosts, the IP address of these hosts, the MOS version and the status. See Figure 104 for an example.

MIRAPPOINT®
Operations Console
doc1.mirapoint.com

Home ▸ Dashboard site map | help | logout

Dashboard Alerts
Groups Import/Export

Refresh
Stop

1 to 3 of 3 <Prev | Next>

	Group	Hostname	IP Address	MOS Version	Status
1	Security Layer	fuji.mirapoint.com	10.0.3.41	3.7.0.62800-randall_r30-200601021136	Alerts
2	testGroup	doc1.mirapoint.com(*)	10.0.3.29	3.7.2-GA-62568	Alerts
3	testGroup	doc2.mirapoint.com(*)	10.0.2.21	3.7.4.5	Alerts

(*) Please enable SSL on these hosts in order to securely administer them from the Operations Console

- Clicking on a group name reduces the view to only the hosts that belong to that group.
- Clicking on a host name brings up a detailed view for that host only.
- Clicking on the MOS Version for a given host has a link that displays the Update page for the selected host.
- Clicking on the Alerts link opens the Alerts page for that host.

Powered By **MIRAPPOINT**

Version 3.8.0 Copyright © 1998-2006 Mirapoint, Inc. Local Intranet

Figure 104 Operations Console Dashboard Page

Use the page options as described:





- ◆ Click the column headers to sort the table by that data.
- ◆ Click a **Group** name to reduce the view to only the hosts belonging to that group; click the **Status Alerts** link (when displayed) to open the Administration Suite for the selected host to the **Alerts** page.
- ◆ Click a **Hostname** in the reduced view to display a detailed view for that host. Information displayed includes:

- ❖ **MOS Version:** Clicking this link opens the Administration Suite for the selected host to the **Update Information** page.
- ❖ **Uptime:** Time since the last boot of the machine.
- ❖ **Status:** Outstanding alerts on that host, see Table 28, “Dashboard Status Colors,” on page 473 for details.
- ❖ **Messages in Queue:** Number of messages in the SMTP queue.
- ❖ **System Load:** 1-minute system load average (the average number of processes in the run queue over 60 seconds).
- ❖ **CPU Usage:** Percentage of the system CPU is use.
- ❖ **Health Monitor:** Clicking this link opens the Administration Suite for the selected host to the **Health Monitor** page.
- ❖ **Performance Monitor:** Clicking this link opens the Administration Suite for the selected host to the **Performance Graphs** page.

All the **Dashboard** pages have a **Refresh** link to manually update the page, and **Start** or **Stop** links to enable or disable automatic update of the page.

The line containing the **Status** information is highlighted with a specific colored as described in Table 28.

Table 28 Dashboard Status Colors

Color	Description
	OK: The selected host has no active alerts.
	Alerts: Link opens the Alerts page for the selected host.
	Permission denied: The host is accessible but the operation is not permitted (for example, because of trusted admin settings).
	Unreachable: The host is currently not accessible

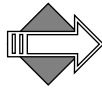
Using Operations Console Alerts

Use the **Alerts** page to view active alerts on the selected host.

Alerts that are received are displayed. The alerts might be for the current host, or, in the case of the Operations Console, for the hosts belonging to the selected group.

Clicking on a column header link sort the table by that factor.


All the **Alerts** pages have a **Refresh** link to manually update the page, and **Start** or **Stop** links to enable or disable automatic update of the page.



The **Logs / Reports > System** report displays **System Alert** messages not related to the persistent conditions shown on this page. To get a more complete picture of system activity, view the **System** report in addition to this page.

Using the Alerts Table

The **Alerts** table shows the name of the alert, the length of time since the alert started, and a description of the alert. Note the following:

- ◆ Click one of the column headers to sort the table by that factor.
- ◆ The **Time Outstanding** indicates how long the alert has been active.
- ◆ Click a **Help** icon  to view suggested corrective actions.

Using Logs and Reports

This chapter describes the reports that can be generated to monitor message traffic, security screening, and system operation.



All of the reports are more valuable when you have developed a good baseline understanding of your system. By monitoring the graphs and reports daily, you can familiarize yourself with the system's normal patterns and will be able to spot unusual activity more easily.

The following topics are included:

- ◆ [Receiving Daily and Weekly Reports](#): How to read the reports that arrive to the administrator's WebMail.
- ◆ [Logs/Reports Overview](#): A summary of all the reports.
- ◆ [Mail Reports](#): How to read the mail reports.
- ◆ [Logins Reports](#): How to read the reports on logins.
- ◆ [Security Reports](#): How to read the antivirus, antispam, and MailHurdle reports.
- ◆ [System Reports](#): How to read the reports on system activity.
- ◆ [Command Report](#): How to read the report on commands issued.
- ◆ [Folders Report](#): How to read the folders report.

Receiving Daily and Weekly Reports

The system automatically generates daily and weekly reports and sends them to the **daily-reports** and **weekly-reports** distribution lists. You can

modify these DLs to send the reports to whoever needs to see them. (For information about how to do this, see [“Editing Distribution Lists” on page 316.](#))

Time Strings

Times are represented in the following format:

yyyymmddhhmm.ss

where:

yyyy is the four-digit year

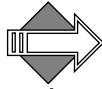
mm is the two-digit month (01 through 12)

dd is the two-digit day of the month (01 through 31)

hh is the two-digit hour (00 through 23)

mm is the two-digit minute (00 through 59)

ss is the two-digit second (00 through 59)



Time is always Greenwich Mean Time (GMT). Minutes and Seconds are often omitted.

Daily Reports

Each day, the system sends the detailed mail and system logs to the **daily-reports** distribution list. The only default member of this list is **Administrator**. You can add list members and send the daily reports to other addresses, including remote addresses if desired.

The following reports are generated each day and sent to the daily-reports distribution list as email attachments:

- ◆ A connection summary: The number of successful and failed connection attempts per user to the IMAP and POP services, and to the administration server. These statistics are sorted by user login name. For details, see [“Summary \(Logins\)” on page 497.](#)
- ◆ A local mail summary: Each message delivered to or received from a local user. For details, see [“Local \(Mail Users\)” on page 498.](#)
- ◆ A remote mail summary: Each message delivered to a remote recipient. For details, see [“Remote \(Mail Users\)” on page 499.](#)

- ◆ Detailed connection logs: All connections and connection attempts to the POP, IMAP, and administration services for the selected day chronologically. For details, see [“Detailed \(Logins\)” on page 507](#).
- ◆ Detailed mail logs: Chronological list of all SMTP transactions for the selected day. For details, see [“Detailed \(Mail Logs\)” on page 501](#).
- ◆ Folder size/quota information: Shows all folders on the system hierarchically and alphabetically, the largest 50 folders, and the 50 folders that are closest to over quota. For details, see [“Folder Size & Quota Information” on page 517](#).

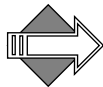
The System Log and security reports are each sent separately. The security reports listed below are sent as attachments to the message titled “Security”:

- ◆ Virus Summary: A summary of viruses found on your system during the selected day. For details, see [“Virus Scanning Summary Report” on page 510](#).
- ◆ Virus Statistics: Detailed information about viruses found. For details, see [“Detailed Virus Scanning Information Report” on page 510](#).
- ◆ Content Filtering Summary: Detailed information about content filtering policies applied to messages on your system. For details, see [“Content Filtering Reports” on page 512](#).
- ◆ SPAM Summary: Detailed information about messages identified as junk mail. For details, see [“Anti-Spam Reports” on page 511](#).
- ◆ Failed Connections by User: The failed login attempts by user for the selected day. For details, see [“Failed by User \(Logins\)” on page 508](#).
- ◆ Failed Connections by IP Address: The failed login attempts by connecting system IP address for the selected day. For details, see [“Failed by IP \(Logins\)” on page 508](#).
- ◆ MailHurdle Host Address Summary: MailHurdle information by host name. It is sorted by the percentage of messages rejected, and then total number of rejections. For details, see [“Host \(MailHurdle\)” on page 513](#).

- ◆ MailHurdle To Address Summary: Information by IP address for recipients; and then each chunk is sorted by the percent of rejections, and then the total number of rejections. For details, see [“To Address \(MailHurdle\)” on page 514](#).
- ◆ MailHurdle From Summary: Information by IP address for senders; and then each chunk is sorted by the percent of rejections, and then the total number of rejections. For details, see [“From Address \(MailHurdle\)” on page 514](#).

Weekly Reports

Each week, the system sends a summary of the week’s email traffic to the **weekly-reports** distribution list. The only default member of this list is **Administrator**. You can add list members and send the weekly reports to other addresses, including remote addresses if desired.



Weekly reports do *not* contain information about user identities or detailed mail traffic. The summary information can safely be sent to remote addresses such as customer care@mirapoint.com without revealing any personal or proprietary user data. Including Mirapoint Customer Care in your weekly-reports distribution list can facilitate troubleshooting if you encounter problems with your system and need to contact support.

The weekly report contains:

- ◆ Appliance configuration information, such as the software version and a list of installed software updates,
- ◆ Hourly summaries for each day, including:
 - ❖ CPU load summary
 - ❖ Local email statistics (messages and bytes sent and received)
 - ❖ Remote email statistics (messages and bytes sent and received)
 - ❖ Network traffic statistics (number of packets sent and received, number of errors encountered)
 - ❖ Disk access statistics

Weekly Report Fields

The following information details the format of weekly reports generated by the Mirapoint or RazorGate appliance. You can refer to this information when writing scripts to extract information from weekly reports.

Depending on the MOS version, your weekly reports may not include all of the field listed below. Mirapoint is constantly adding new fields to help monitor and provide better diagnostics for the system.

Table 29 Report Fields

Field	Description	Example(s)
ADMINSETTINGS	A list of administration settings that have non-default values	security timeout
ANTISPAMSETTINGS	A list of antispam settings that have non-default values	threshold reporting spamprolog headerinfo
ANTISPAMVERSION	A list of installed rulegroups and their version numbers	“mtaverify” “0000” “2005-11-29” “rpdengine” “0000” “2007-07-26”
ANTIVIRUSSETTINGS	A list of antivirus settings that have non-default values	notifyrecipient quarantineaddress
APPTYPE	The application type of the system. MIR=Message Server; SA=RazorGate.	MIR
ARRAYS	The arrays configured on the system; includes the Unix LUN numbers	0.0.0.0 RAID-1 (0.0.0.0. 0.0.1.0) Optimal Inuse 0.0.4.0 Spare (0.0.2.0) Optimal Unused
AUTOREPLYSETTINGS	A list of autoreply settings that have non-default values	autoreplytoall

Table 29 Report Fields (Continued)

Field	Description	Example(s)
BACKUP	A list of backups performed on the system (not available on RazorGate appliances)	NDMP based Dump/Tar Backups: No backup performed NDMP based Image Backups: No backup performed Administration protocol based Backups: No backup performed NetWorker (native client) based Backups: NetWorker Not Enabled
BBWRITETHRU	If On the RAID will switch from caching (normal) to write-through mode, if Off the RAID will not switch. See the CLI Help About Storage for details. (not available on RazorGate 100s)	On
BBWRITETHRUTHRESH	The battery charge in minutes of running time remaining (not available on RazorGate 100s)	2880
BRANDEDDOMAINS	The number of branded domains on the system (does not apply to RazorGate appliances)	7
CALENDARSETTINGS	A list of calendar settings that have non-default values (not available on RazorGate appliances)	timeout maxnumevents
CHASSIS	The system hardware	RG100
CONFENABLED	A list of features enabled on the system or appliance (does not apply to the RazorGate 100)	getmail filtering httpproxy
CONTACT	The name, phone number, address and e-mail of the administrator	Name: Tim Jones Phone: 408-720-3700 Address: 909 Hermosa Court, Sunnyvale, CA 94085 Email: ttjones@mirapoint.com
CONTROLLER	The model/type of SCSI disk controller	2130S

Table 29 Report Fields (Continued)

Field	Description	Example(s)
COSENABLED	A list of features enabled by class of service on the system or appliance (does not apply to the RazorGate 100)	pop imap quota
CPU	The CPU type and speed in megahertz	686 2400
DEFAULTAUTHORIZATION	The authentication type accepted by the system or appliance. See the CLI Help About Auth for details.	plaintext:local
DEFAULTLOCALE	The default locale on the system or appliance	en_US.ISO_8859-1
DIAGSETTINGS	The value(s) of the system diagnostic or tape parameter	changeraddress dataxferelementaddr tapeaddress tapecompression tapecompressionratio
DICTIONARY	Indicates if the dictionary is native (factory installed) or non-native (custom installed) (does not apply to RazorGate appliances)	NonNative
DIRLOGGINSETTINGS	A list of directory logging settings that have non-default values	authentication index protocol replication
DIRSETTINGS	A list of directory settings that have non-default values	password-hash security
DISKS	The configuration of the RAID (not available on RazorGate 100s)	0.0.2.0 70007 Inuse Optimal (ECC no) 0.c2.0.0 0.a2.0.0 0.0.1.0 70007 Inuse Optimal (ECC no) 0.c2.0.0 0.a2.0.0 0.0.0.0 70007 Spare Optimal (ECC no) 0.c2.0.0 0.a2.0.0

Table 29 Report Fields (Continued)

Field	Description	Example(s)
DISKVENDOR	The manufacturer and model numbers of installed disks	0.0.0.0 SEAGATE ST373207LC 0003 0.0.1.0 SEAGATE ST373207LC 0003 0.0.2.0 SEAGATE ST373207LC 0003
DLS	The number of distribution lists on the system	68
DLSMEM	The total number of members in all distribution lists	66
DOMAINS	The number of delegated domains on the system(not available on RazorGate 100s)	9
ENET	The number of available ethernet pots	2
EXCEPTIONAL (format: yyyymmddhhmm)	A list of unusual system events, with a time string, event keyword, and short description for each event. Events are separated by blank lines	200211080812 SYSTEM.REBOOT 200211091458 SYSTEM.REBOOT
FAILOVER	Whether failover is enabled or disabled (not available on RazorGate appliances)	DISABLED
FILTERANY	The number of filters applied to any domain	2
FILTERLOCAL	The number of filters applied to local domains	2
FILTERNONLOCAL	The number of filters applied to non-local domains	1
FILTERPRIMARY	The number of filters applied to the primary domain	1
GETMAILSETTINGS	A list of getmail settings that have non-default values	minpoll
HTTPSETTINGS	A list of HTTP settings that have non-default values	mode root

Table 29 Report Fields (Continued)

Field	Description	Example(s)
HWCPU	CPU type and speed in magahertz	686 2400
HWCPUCOUNT	Number of CPUs installed in the system	1
HWMEMORY	Megabytes of RAM installed in the system	1024
HWMODEL	The hardware model of the appliance	M400 RazorGate 100
HWSTORAGE	The type of disk enclosure on the system	IO4U3206
IMAPSETTINGS	A list of IMAP settings that have non-default values	mode quotawarn
KERB4SETTINGS	A list of KERB4 settings that have non-default values	realm srvtab
KEYSETTINGS	A list of Key (secure log in) settings that have non-default values	mta
LCD	The keypad and LCD panel firmware version number (not available on the M50 or RazorGate 350s or 100s)	3.2
LDAPSETTINGS	LDAP enabled features	autoprovision cachetimeout localcostable
LDAPSETTINGS	A list of LDAP settings that have non-default values	ldif autoprovision

Table 29 Report Fields (Continued)

Field	Description	Example(s)
LICENSES	A list of all applied licenses, user counts where applicable, and expiration dates where applicable	User-limit 750 SSL (strong encryption) SSH Licensed Upgrades Allowed 01/27/2007 Mirapoint Antispam SE 750 users 01/12/2007 Web-mail 300 users POP 750 users IMAP 301 users Directory Server Access 750 users XML unlimited users Sophos virus filtering 750 users 01/27/2007 Message Server
LOCALES	A list of all locales installed on the system or appliance	en_US.ISO_8859-1 en_US.ISO_8859-1_nokia ja_JP.utf-8
LOCALEUNANNOUNCED	Locale Set Unannounced settings that have non-default values. See the CLI Help About Locale for details.	ko_KR.utf-8
LOGINFOOTER (language selection links on the Login page)	Indicates if the login footer is on or off	On
LOGINS	The largest number of logins for a day and the average number of logins over the past 11 days. Logins include: Calendar, POP, IMAP, and Webmail (Calendar, and Webmail are not available on RazorGate appliances)	CLNDR 1 (single day) CLNDR 0 (11 day average) POP 0 (single day) POP 0 (11 day average) IMAP 0 (single day) IMAP 0 (11 day average) WEBML 1 (single day) WEBML 0 (11 day average)
LOGSETTINGS	A list of log settings that have non-default values	history markinterval syncinterval

Table 29 Report Fields (Continued)

Field	Description	Example(s)
MAILBOXES	The number of folders (mailboxes) on the system (not available on RazorGate appliances)	91
MAILBOXSETTINGS	A list of mailbox settings that have non-default values (currently not available on RazorGate appliances)	broadcast
MEM	The megabytes of RAM installed in the system	1024
MNAME	The appliance name which combines the hardware model, report version and software version numbers	Mirapoint M400 3.2 3.2.0.52-EA RazorGate 300 3.4 3.4.0.52-EA
MONSETTINGS	A list of monitoring thresholds that have non-default values	system.admnc system.popc
MTAVERIFYSETTINGS	A list of MailHurdle settings that have non-default values	allowedentrylifetime allowmisbehavingmailers allownullfrom allowrelays inboundonly initialentrylifetime initialtimeout reversemx
NAMEDBRANDS	The number of named brands on the system (does not apply to RazorGate appliances)	7
NDMPSETTINGS	A list of NDMP settings that have non-default values (not available on RazorGate appliances)	port
NETIFSETTINGS	A list of NETIF settings that have non-default values	blackholeduration limittcpconnectcount limittcpconnectrate maxtcpconnectcount maxtcpconnectrate mediaport0 mediaport1

Table 29 Report Fields (Continued)

Field	Description	Example(s)
NETWORKMEDIA	The configuration and status of the Ethernet port 0	autoselect (100baseTX <full-duplex>) status: active
NISSETTINGS	A list of NIS settings that have non-default values	domain server
NTPSETTINGS	A list of NTP settings that have non-default values	zone
PATCHES	A space-separated list of the software updates (patches) installed on the system	R3_8_1_FCS
POPSETTINGS	A list of POP settings that have non-default values	minpoll security
PORTWWN	The port world wide name (WWN) for the Q-logic host bus adapter card (not available on RazorGate appliances)	0X210000e08b056b2
QUOTAPOLICY	Quota Setpolicy settings that have non-default values. See the CLI Help About Quota for details.	defaultsendoverquotamessage overquota sendoverquotamessage
RADIUSSETTINGS	A list of RADIUS settings that have non-default values	secret timeout
RAID	The RAID configuration used by the system	RTR
REBOOTS (format: yyyymmddhhmm)	A list of date & times in the previous week (one on each line) when the system or appliance rebooted	200211080812 200211091458
REPORTVERSION	The report format version number	3.8
SERIAL	The system serial number	ESDW5420201
SERVICEENABLED	A list of the services enabled on the system or appliance	POP IMAP Calendar Webmail

Table 29 Report Fields (Continued)

Field	Description	Example(s)
SERVICESSTARTED	A list of the services started on the system or appliance	POP IMAP Webmail
SMTPSETTINGS	A list of SMTP settings that have non-default values	Omr Ldaprouting
SNMPSETTINGS	A list of SNMP settings that have non-default values	Syscontact Syslocation
SOFTVERSION	The software version number	3.8.1-FCS
SSLCERTIFICATE	Indicates if the SSL certificate is Mirapoint-issued or not	Mirapoint
STANDBY	The presence of the standby appliance and its Ethernet address (not available on RazorGate appliances)	INACTIVE (no standby head is designated for failover)
STORAGE	The type of disk enclosure on the system	IO4U3206
STORAGESPACE	The amount of total storage space in megabytes followed by the amount used	113828 37296
STORETYPE	The type of message storage, either local, NFS or SAN (NFS and SAN are not available on RazorGate appliances)	local
SYSTEMBRAND	Indicates if there is a system brand (does not apply to RazorGate appliances)	Yes
UPTIME	The time in days, minutes, and seconds since the appliance last booted	217 days, 8:22
UPTIMEPERHOUR	The system uptime in seconds, capped at 3600, recorded every hour	3600, 3600, 3600, 256, 3600, 3600, 3600
USERS	The number of user accounts on the system	49

Table 29 Report Fields (Continued)

Field	Description	Example(s)
VIRTDOM	The number of virtual domains on the system; deprecate as of 3.0. (not available on RazorGate appliances)	0
VIRTDOMMEM	The total number of members in all virtual domains. Virtual domains are deprecate as of 3.0. (not available on RazorGate appliances)	0
VIRUSSCAN	The antivirus license on the system or appliance and its configuration	LICENSED SOPHOS VERSION Sophos Anti-Virus SAVI2 2.2.03.098, Pattern file: 3.63, Incremental patterns: netdex-a nethf-c opaservc, Last updated: Sat Apr 300:00:01 2004
WEBMAILSETTINGS	A list of WebMail settings that have non-default values	Timeout
WEBMAILSORT	The number of times WebMail does a sort operation.	12

Weekly Report Time-Based Fields

The **TIMES** field gives a comma-separated list, one for each hour in the past week for which statistics were collected.

The subsequent fields give lists of statistics with the same number of entries, each corresponding to a time in the **TIMES** list. For example, the third number in the **LOCMSGRCV** list is the number of messages delivered locally during the hour ending at the third hour in the **TIMES** list.

The following table explains the meaning of each entry in the comma-separated list for each field.

Table 30 Time-Based Report Fields

Field	Description
LOCBYTRCV	The average number of bytes in all messages delivered locally per hour
LOCMSGRCV	The average number of messages received by the system
MTAVERIFY.INITIALDENY	The Initial Deny setting for MailHurdle
MTAVERIFY.INITIALACTIVE	The Initial Active setting for MailHurdle
MTAVERIFY.ACTIVE	The Active setting for MailHurdle
MTAVERIFY.APASSED	The number of messages passed into the “Active” state by MailHurdle
MTAVERIFY.ANOTRETRIED	The number of messages that never retried MailHurdle’s initial SMTP error code
MTAVERIFY.ATOTAL	The total number of messages processed by MailHurdle
SMTPMSGSENT	The average number of messages sent to remote systems per hour
SMTPBYTSNT	The average number of bytes in all messages sent to remote systems per hour
SMTPMSGRCV	The average number of messages received from remote systems per hour
SMTPBYTRCV	The average number bytes in all messages received from remote systems per hour
LOAD1	The time-decaying average number of runnable processes on the system or appliance over the previous one minute
LOAD5	The time-decaying average number of runnable processes on the system or appliance over the previous five minutes
LOAD15	The time-decaying average number of runnable processes on the system or appliance over the previous 15 minutes
FXPOPKTIN	The average number of network packets received per hour
FXPOPKTOU	The average number of network packets sent per hour
FXPOBYTIN	The average number of bytes in all network packets received per hour
FXPOBYTOU	The average number of bytes in all network packets sent per hour

Table 30 Time-Based Report Fields (Continued)

Field	Description
FXPOERRIN	The average number of errors encountered while receiving network data per hour
FXPOERROU	The average number of errors encountered while sending network data per hour
DISKSYS	Percent full for the system disk partition
DISKLOG	Percent full for the logging disk partition
DISKSTO	Percent full for the mail-store disk partition
POPCONN	Number of POP connections per hour
IMAPCONN	Number of IMAP connections per hour
WEBMAIL.ACTIVE05	Number of active Webmail connections in the last 5 minutes
WEBMAIL.ACTIVE60	Number of active Webmail connections in the last 60 minutes
WEBMAIL.APPEND	Number of times Webmail has appended a message to the Sent or Drafts folder (not available on RazorGate appliances)
WEBMAIL.ATTACHADD	Number of times Webmail has performed the add attachment operation (not available on RazorGate appliances)
WEBMAIL.ATTACHDEL	Number of times Webmail has performed the delete attachment operation (not available on RazorGate appliances)
WEBMAIL.ATTACHREAD	Number of times Webmail has performed the read attachment operation (not available on RazorGate appliances)
WEBMAIL.CHECKMAIL	Number of times Webmail has performed the check mail operation since boot (not available on RazorGate appliances)
WEBMAIL.CHECKMAILMS	Milliseconds to process CheckMails since boot
WEBMAIL.CLEARALL	Number of times Webmail has performed the clear all operation since boot (not available on RazorGate appliances)
WEBMAIL.COMPACT	Number of times Webmail has performed the compact operation since boot (not available on RazorGate appliances)
WEBMAIL.COMPOSE	Number of times Webmail has performed the compose operation since boot (not available on RazorGate appliances)
WEBMAIL.DORMANT	Number of Webmail sessions inactive after an hour (not available on RazorGate appliances)
WEBMAIL.FOLDERADD	Number of times Webmail has performed the folder add operation since boot (not available on RazorGate appliances)

Table 30 Time-Based Report Fields (Continued)

Field	Description
WEBMAIL.FOLDERDEL	Number of times Webmail has performed the folder delete operation since boot (not available on RazorGate appliances)
WEBMAIL.FOLDERPAGE	Number of times Webmail has accessed the folder page since boot (not available on RazorGate appliances)
WEBMAIL.FOLDERPAGEMS	Milliseconds to process WebMail page up/down since boot
WEBMAIL.LOGIN	Number of Webmail logins since boot (available for proxy only on RazorGate appliances)
WEBMAIL.LOGINMS	Milliseconds to process WebMail logins since boot (available for proxy only on RazorGate appliances)
WEBMAIL.LOGOUT	Number of Webmail logouts since boot (available for proxy only on RazorGate appliances)
WEBMAIL.MSGDEL	Number of times Webmail has performed the message delete operation since boot (not available on RazorGate appliances)
WEBMAIL.MSGDELMMS	Milliseconds to process WebMail deletes since boot (not available on RazorGate appliances)
WEBMAIL.MSGGOTO	Number of times Webmail has performed the message go-to operation since boot (not available on RazorGate appliances)
WEBMAIL.MSGMOVE	Number of times Webmail has performed the message move operation since boot (not available on RazorGate appliances)
WEBMAIL.MSGQUOTE	Number of times Webmail has replied in-line to a message since boot (not available on RazorGate appliances)
WEBMAIL.MSGREAD	Number of times Webmail has performed the message read operation since boot (not available on RazorGate appliances)
WEBMAIL.MSGREADMS	Milliseconds to process WebMail reads since boot (not available on RazorGate appliances)
WEBMAIL.MSGREPLY	Number of times Webmail has performed the message reply operation since boot (not available on RazorGate appliances)
WEBMAIL.MSGSENT	Number of times Webmail has performed the message sent operation since boot (not available on RazorGate appliances)
WEBMAIL.MSGSENTMS	Milliseconds to process WebMail replies since boot (not available on RazorGate appliances)
WEBMAIL.SEARCH	Number of times Webmail has performed the search operation since boot (not available on RazorGate appliances)

Table 30 Time-Based Report Fields (Continued)

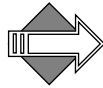
Field	Description
WEBMAIL.SELECT	Number of times Webmail has performed the select operation since boot (not available on RazorGate appliances)
WEBMAIL.SELECTALL	Number of times Webmail has performed the select all operation since boot (not available on RazorGate appliances)
WEBMAIL.SORT	Number of times Webmail performed the sort operation since boot (not available on RazorGate appliances)
WEBMAIL.TOC	Number of times Webmail has listed the table of contents, message list, for a folder since boot (not available on RazorGate appliances)
WEBMAIL.XMLBODYSTRUCT	Number of bodystructure.xml requests since boot.
WEBMAIL.XMLBODYSTRUCTMS	Milliseconds to process bodystructure.xml since boot.
WEBMAIL.XMLEXPUNGE	Number of expunge.xml requests since boot.
WEBMAIL.XMLEXPUNGEMS	Milliseconds to process expunge.xml since boot.
WEBMAIL.XMLGETSID	Number of getsid.xml requests since boot.
WEBMAIL.XMLGETSIDMS	Milliseconds to process getsid.xml since boot.
WEBMAIL.XMLINDEX	Number of index.xml requests since boot.
WEBMAIL.XMLINDEXMS	Milliseconds to process index.xml since boot.
WEBMAIL.XMLRFC822	Number of rfc822.xml requests since boot.
WEBMAIL.XMLRFC822MS	Milliseconds to process rfc822.xml since boot.
WEBMAIL.XMLSEARCH	Number of search.xml requests since boot.
WEBMAIL.XMLSEARCHMS	Milliseconds to process search.xml since boot.
WEBMAIL.XMLSETFLAGS	Number of setflags.xml requests since boot.
WEBMAIL.XMLSETFLAGSMS	Milliseconds to process setflags.xml since boot.
WEBMAIL.XMLSORT	Number of sort.xml requests since boot.
WEBMAIL.XMLSORTMS	Milliseconds to process sort.xml since boot.
WEBMAIL.XMLSTATUS	Number of status.xml requests since boot.
WEBMAIL.XMLSTATUSMS	Milliseconds to process status.xml since boot.
WEBMAIL.XMLVERSID	Number of verifysid.xml requests since boot.
WEBMAIL.XMLVERSIDMS	Milliseconds to process verifysid.xml since boot.
WEBMAIL.XMLBODYSTRUCT	Number of bodystructure.xml requests since boot.
SYSTEM.AMMSGATTACH	Number of messages with attachments since boot time

Table 30 Time-Based Report Fields (Continued)

Field	Description
SYSTEM.AMMSGRECP	Number of message recipients since boot time
SYSTEM.AMMSGVIRUS	Number of e-mail viruses found since boot time
SYSTEM.AMMSGSPAM	Hourly number of Spam Mails (generated by phonestat.pl)
SYSTEM.ASMTPCIN	Number of inbound SMTP connections since boot time
SYSTEM.ASMTPCOUT	Number of outbound SMTP connections since boot time
SYSTEM.MAILQUEUE	Number of messages in the SMTP delivery queue at the top of each hour
DIR.OPS	Number of directory operation (not available on RazorGate appliances)
SYSTEM.UCE1	A count of messages scored 1-10 as junk mail
SYSTEM.UCE2	A count of messages scored 11-20 as junk mail
SYSTEM.UCE3	A count of messages scored 21-30 as junk mail
SYSTEM.UCE4	A count of messages scored 31-40 as junk mail
SYSTEM.UCE5	A count of messages scored 41-50 as junk mail
SYSTEM.UCE6	A count of messages scored 51-60 as junk mail
SYSTEM.UCE7	A count of messages scored 61-70 as junk mail
SYSTEM.UCE8	A count of messages scored 71-80 as junk mail
SYSTEM.UCE9	A count of messages scored 81-90 as junk mail
SYSTEM.UCE10	A count of messages scored 91-100 as junk mail
ADMINREF	A list of which administrator commands have been executed and how many times they have been executed.

Logs/Reports Overview

The Administration Suite enables you to view Mirapoint logs and reports at any time to access detailed information about system usage and mail traffic. This information includes statistics for logins,



commands, CPU, network, and message traffic, as well as audit data for users or administrators.

Select a domain before selecting a **Mail**, **Logins**, or **Folders** report.

The **Logs / Reports** pages provide these reports on system activity:

- ◆ **Mail Reports:** Shows all email traffic going through the system, and other system events.
- ◆ **Logins Reports:** Shows connections to the system through the many access protocols and interfaces that the system offers.
- ◆ **Security Reports:** Shows security-related events, including the identification of junk mail and virus-bearing messages, and content-filtering activity.
- ◆ **System Reports:** Shows all system log events (for that day) in chronological order.
- ◆ **Command Report:** Shows every administration protocol command received by the machine on the selected day and all command responses.
- ◆ **Folders Report:** Shows all folders on the system hierarchically and alphabetically, the largest 50 folders, and the 50 folders that are closest to over quota.

Abbreviations Used in Logs

Table 31 provides definitions for abbreviations used in the logs.

Table 31 Abbreviations Used in Logs

Abbreviation	Description
""	Empty command arguments
ADMIN	Administration service
CLR	Cleartext or nonsecure
INVLD	Bad login
KB	Kilobyte

Table 31 Abbreviations Used in Logs (Continued)

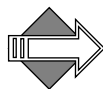
Abbreviation	Description
KERB4 or KERB5	Kerberos authentication
LCL	Local
NTP	Network Time Protocol
PLAIN	Plaintext
RMT	Remote
SSH	Secure Shell authentication
SSL	Secure Sockets Layer authentication
SVC	Service
TLS	Secure connection
WEBML	WebMail

Mail Reports

The Mail Reports show all email traffic going through the system, and other system events. Each day, the system emails detailed mail and system logs to the administrator. Click a **Date** link at the top of each report to look at the information for that day.

These are the available **Mail** reports:

- ◆ **Top (Mail Users):** The most frequent mail users for the selected day.
- ◆ **Local (Mail Users):** Each message delivered to or received from a local user.
- ◆ **Remote (Mail Users):** Each message delivered to a remote recipient.
- ◆ **Traffic Summary:** A summary of the mail traffic.
- ◆ **Detailed (Mail Logs):** Chronological list of all SMTP transactions for the selected day.
- ◆ **Search:** Search the detailed mail logs.



Changing an SMTP setting results in the statistics for that box getting reset to zero. This is because the description for the statistics should match SNMP, and they get reset when you restart sendmail.

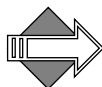
Top (Mail Users)

The **Top Mail Users** report show summaries of the messages sent by each of the top 100 message originators for the selected date. There are several top-100 lists, only some might display:

- ◆ **Sent Message Statistics:** A list of messages sent by each originator.
- ◆ **Received Message Statistics:** A list of messages received by each recipient.
- ◆ **Sent Bytes Statistics:** A list of the total bytes in all messages sent by each originator.
- ◆ **Received Bytes Statistics:** A list of the total bytes in all messages received by each recipient.



Use this report to find out who is sending the most and/or largest size messages. You can then take action through email or blocking/filtering those senders.



Having a null string (< >) at the top of this report is not necessarily cause for concern. The Null Sender is used for bounce messages and non-deliverable responses. If there's high spam through the system, the null string is likely to be at the top of this report.

The **Top Mail Users** report has the following fields. Example report follows in Figure 105 on page 497.

Table 32 Top Mail Users Report

Statistic	Description
Sent Messages	The number of messages sent by the originator or recipient
Number Recipients	The total number of recipients of all messages sent by the originator or received by the recipient
Sent Bytes	The total number of bytes sent by the originator or recipient

Table 32 Top Mail Users Report (Continued)

Statistic	Description
Received Messages	The number of messages received by the originator or recipient
Received Bytes	The total number of bytes received by the originator or recipient

Apr 03, 2006					
Date: 2006 Apr 03 2006 Apr 02 2006 Apr 01 2006 Mar 31 2006 Mar 30 2006 Mar 29 2006 Mar 28 2006 Mar 27					
Sent Messages Statistics (Top Users: 3)					
Originator	Sent Messages	Number Recipients	Sent Bytes	Received Messages	Received Bytes
tmartin@ui0.mirapoint.com	121	121	3702563	0	0
administrator	12	14	337652	12	342988
u	1	1	30	52	2185887
Totals	134	136	4040245	64	2528875
Received Messages Statistics (Top Users: 4)					
Recipient	Sent Messages	Number Recipients	Sent Bytes	Received Messages	Received Bytes
z	0	0	0	70	1594132
u	1	1	30	52	2185887
administrator	12	14	337652	12	342988
customer@mirapoint.com	0	0	0	9	87483
Totals	13	15	337682	143	4210490
Sent Bytes Statistics (Top Users: 3)					
Originator	Sent Messages	Number Recipients	Sent Bytes	Received Messages	Received Bytes
tmartin@ui0.mirapoint.com	121	121	3702563	0	0
administrator	12	14	337652	12	342988
u	1	1	30	52	2185887
Totals	134	136	4040245	64	2528875
Received Bytes Statistics (Top Users: 4)					
Recipient	Sent Messages	Number Recipients	Sent Bytes	Received Messages	Received Bytes
u	1	1	30	52	2185887
z	0	0	0	70	1594132
administrator	12	14	337652	12	342988
customer@mirapoint.com	0	0	0	9	87483
Totals	13	15	337682	143	4210490

Figure 105 Top Mail Users

Summary (Logins)

The **Login Summary** shows the number of successful and failed login attempts per user to the IMAP and POP services, and to the administration server. These statistics are sorted by user login name.

Each summary line contains the same fields described under **Top Login Reports** in Table 40, “Top Logins By User,” on page 505.

Local (Mail Users)

The **Local Mail Traffic** report shows data about the messages sent and received by each local email address on the system.



Use this report to find out who is sending the most and/or largest size local messages. You can then take action through email or blocking/filtering those senders.

The **Local Mail Traffic** report has the following fields. Example report follows in Figure 106 on page 498.

Table 33 Local Mail Traffic Report

Statistic	Description
Sent Messages	The number of messages sent by the local address
Number Recipients	The total number of recipients of all messages sent by the local address
Sent Bytes	The total number of bytes sent by the local address
Received Messages	The number of messages received by the local address
Received Bytes	The total number of bytes received by the local address

Apr 03, 2006					
Date: 2006 Apr 03 2006 Apr 02 2006 Apr 01 2006 Mar 31 2006 Mar 30 2006 Mar 29 2006 Mar 28 2006 Mar 27					
Originator	Sent Messages	Number Recipients	Sent Bytes	Received Messages	Received Bytes
administrator	12	14	337652	12	342988
u	1	1	30	52	2185887
z	0	0	0	70	1594132
Totals	13	15	337682	134	4123007

Figure 106 Local Mail Traffic

Remote (Mail Users)

The **Remote Mail Traffic** report shows data about the messages received from remote email addresses.



Use this report to find out who is sending the most and/or largest size remote messages. You can then take action through email or blocking/filtering those senders.

The **Remote Mail Traffic** report has the following fields. Example report follows in Figure 107 on page 499.

Table 34 Remote Mail Traffic Reports

Statistic	Description
Sent Messages	The number of messages sent to this system by the remote address
Number Recipients	The total number of recipients of all messages sent to this system by the remote address
Sent Bytes	The total number of bytes sent to this system by the remote address
Received Messages	The number of messages received by the remote address from this system
Received Bytes	The total number of bytes received by the remote address from this system

Apr 03, 2006						
Date: 2006 Apr 03 2006 Apr 02 2006 Apr 01 2006 Mar 31 2006 Mar 30 2006 Mar 29 2006 Mar 28 2006 Mar 27						
Originator	Sent Messages	Number Recipients	Sent Bytes	Received Messages	Received Bytes	
customer@mirapoint.com	0	0	0	9	87483	
tmartin@ui0.mirapoint.com	121	121	3702563	0	0	
Totals	121	121	3702563	9	87483	

Figure 107 Remote Mail Traffic

Traffic Summary

The **Mail Traffic Summary** shows three summaries of email traffic:

- ◆ **Message Events by Hour:** The number and rate of messages received, queued, originating locally, and originating from remote hosts

Below this report, are the following two tables of data:

- ◆ **Average Size Summary:** A distribution of messages by message size
- ◆ **Average Number of Recipients Summary:** A distribution of messages by number of recipients

For these reports, see also, [“Code Explanations” on page 503](#).



Use this report to see how busy the system has been over the day; it shows in hourly intervals messages per second, the number of messages in the queue, and inbound/outbound rates so you can easily see when the busy times are overloading the system.

Message Events by Hour

The **Message Events by Hour** shows the following fields for each hour of the selected date:

Table 35 Number-and-Rate Summary

Statistic	Description
Recv / Rate	The number of messages received during the sample period and the rate at which the messages were received
Queue / Rate	The number of message queued during the sample period and the rate at which the messages were queued
Local / Rate	The number of message delivered to local addresses during the sample period and the rate at which the messages delivered
Remote / Rate	The number of messages handled by the system that were sent to remote hosts during the sample period and the rate at which the messages were sent

Average Size Summary

The **Average Size Summary**, at the bottom of the Mail Traffic Summary report, shows the number of messages in each of several size ranges handled by the system during the most recent hour. Messages larger than 8MB are counted in the same range.

Table 36 Message-Size Summary

Statistic	Description
Size	The size range
Count	The number of messages in each size range
Percent	The percentage of the total number of messages accounted for by the messages in each size range
Average Size	The average message size

Average Number of Recipients Summary

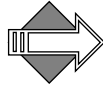
The **Average Number of Recipients Summary**, at the bottom of the Mail Traffic Summary report, shows the number of messages addressed to specific numbers of recipients during the most recent hour. Messages having more than 7 recipients are counted together.

Table 37 Number-of-Recipients Summary

Statistic	Description
Rcpt	The number of recipients
Count	The number of messages addressed to each number of recipients
Percent	The percentage of the total number of messages accounted for by the messages addressed to each number of recipients
Average Number of Recipients	The average number of recipients

Detailed (Mail Logs)

The **Detailed Mail Logs** report lists all SMTP transactions for the selected day chronologically. The fields are described below.



Most web browsers provide a way (such as shift-click) to save a linked file directly to your disk without displaying it; if you find that the detailed reports are often too large for your browser to display, you can save them to disk and view them using your favorite text editor.



The full mail traffic logs for the day can be quite large; use the search function to find references. This report is helpful in tracing a message through the system showing everything that happened to the message up to the point that it is delivered or leaves the system.

An example of the format of each transaction record is:

```
originator
  queue-id <message-id@example-host-name>
  evt-time event
  evt-time event...
```

Table 38 Detailed Mail Logs

Statistic	Description
<i>originator</i>	The sender of the message
<i>queue-id</i>	The unique ID that identifies the message within the mail queue
<i>message-id@example-host-name</i>	A string created to uniquely identify a message. The string can be created by a mail client, or by the first SMTP server that sees a message. Usually the text string is followed by “@ <i>host-name</i> ” where the value of <i>hostname</i> depends on the configuration of the originating host machine of the message
<i>evt-time</i>	The time the event occurred
<i>event</i>	One of the following: <ul style="list-style-type: none"> ❖ received <i>num-bytes num-recipients host-received-from</i> The message was received. ❖ filtering code (see Code Explanations) The message was filtered for <i>recipient</i> ❖ queued <i>recipient</i> The message was queued for <i>recipient</i> ❖ sent <i>elapsed-time recipient-list</i> The message was sent. ❖ Split from <i>queue-id</i> The message was copied from <i>queue-id</i> and assigned a new queue ID to facilitate internal processing.

Table 38 Detailed Mail Logs (Continued)

Statistic	Description
<i>num-bytes</i>	The number of bytes in the message
<i>num-recipients</i>	The number of recipients of the message
<i>host-received-from</i>	The host from which the message was received
<i>recipient</i>	The address of the recipient
<i>elapsed-time</i>	The total time that elapsed between receipt and final delivery
<i>recipient-list</i>	A space-separated list of recipients to which the message was sent

Code Explanations

For the **filtering** event option various codes are used to indicate what filtering took place. These codes translate as follows.

Table 39 Filtering Event Codes

Code	Description
A	Already Done (this service already done; not repeating)
AV	Anti-Virus
AS	Anti-Spam
D	Default (this service done by default)
DS	Domain Signatures
DF	Domain Filters
IAV	Anti-Virus, Inbound Only
IAS	Anti-Spam, Inbound Only
IDS	Domain Signatures, Inbound Only
IDF	Domain Filters, Inbound Only
N	Not Allowed (COS denied this service)
QN	Quarantine

Table 39 Filtering Event Codes (Continued)

Code	Description
R	Recipients (this service done due to recipient address)
S	Senders (this service done due to sender address)
SS	Spam In Subject
WL	Allowed Senders list (formerly White List)
Accept	Host from which to accept X-Mirapoint-State header

Search

The Mail reports offer a search facility; to use it, follow these steps.

1. To view the Detailed Search reports for a specific day, click the **Search** link.
Result: A search form displays.
2. Click the day you want to search and enter the text you want to find in the **Search:** option. Optionally, in the **in last** option, you can enter the number of most recent records (message log entries) that you want to search. If you do not specify a number of records, all entries are searched.
3. Click **Search**.
Result: The **Detailed Mail Logs** report for that date displays. The fields are described in [“Detailed \(Mail Logs\)” on page 501](#).

Logins Reports

The **Login Reports** show connections to the system through the access protocols and interfaces that the system offers. These include WebMail, WebCal, POP, IMAP, and the administration protocol.

These are the available **Logins** reports:

- ◆ **Top (Logins):** The most frequent logins for the selected day.
- ◆ **Summary (Logins):** The number of successful and failed connection attempts per user to the IMAP and POP services, and to the administration server. These statistics are sorted by user login name.
- ◆ **Traffic Rates (Logins):** The number and rate of logins for each hour of the selected day. Note that changing the system time zone during the report period causes a gap or repetition in the hours listed.
- ◆ **Detailed (Logins):** All connections and connection attempts to the POP, IMAP, and administration services for the selected day chronologically.
- ◆ **Failed by User (Logins):** The failed login attempts by user for the selected day.
- ◆ **Failed by IP (Logins):** The failed login attempts by connecting system IP address for the selected day.

Top (Logins)

The **Top Logins By User** report lists by user login name the 100 users who made the most connections to the system.

Each line contains the following fields:

Table 40 Top Logins By User

Field	Description
User	The login name of the user
Svc	The name of the service to which the user connected. Possible values are POP, IMAP, ADMIN, XMLML (XML Mail), WEBML (WebMail), CLNDR (WebCal—the user logged in through http://hostname/mc).

Table 40 Top Logins By User (Continued)

Field	Description
Security	A two-part field separated by a colon (:). The first part indicates the kind of encryption used in the connection; possible values are CLR (cleartext, no encryption), SSH (secure shell; for administration connections only), and SSL (secure sockets layer). The second part indicates the authentication method used to connect; possible values are PLAIN (plaintext authentication) and KERB4 (Kerberos version 4).
Stat	The status of the connection. No value means the connection was successful. FAIL means the connection failed.
Count	The total number of connections by the user for this service since midnight of the selected day.
Time	The total duration of all connections by the user for this service since midnight of the selected day. The format is <i>days</i> (if more than an entire day), followed by <i>hours:minutes:seconds</i> .

Traffic Rates (Logins)

The **Login Traffic Rates** report shows the number of logins by hour for several services, and the rate of logins by hour in logins per second for the POP and IMAP services.

Table 41 Login Traffic Rates

Field	Description
Time	The hour to which the statistics apply.
POP/ Rate	These two columns give the number of POP logins during the hour and the rate of logins in logins per second for that hour.
IMAP/Rate	These two columns give the number of IMAP logins during the hour and the rate of logins in logins per second for that hour.
Admind	The number of administration service logins during the hour.
WebMail	The number of WebMail logins during the hour.
WebCal	The number of WebCal logins during the hour.
XMLcal	The number of XML calls for WebCal during the hour.
Other	The number of logins to other services during the hour.

Table 41 Login Traffic Rates (Continued)

Field	Description
Bad	The number of failed login attempts for all services during the hour.

Detailed (Logins)

The **Detailed Login Report** shows all logins and login attempts to the POP, IMAP, and administration services for the selected day chronologically.

The format of each line in the detailed login report is:

event date time GMT-offset service security IP-addr user duration

Table 42 Detailed Login Report

Statistic	Description
<i>event</i>	The login event; either LOGIN, LOGOUT, or BAD.
<i>date</i>	The date of the event in the format <i>year/month/day</i> .
<i>time</i>	The time of the event in the format <i>hours:minutes:seconds</i> .
<i>GMT-offset</i>	The offset in hours from Greenwich Mean Time (GMT)
<i>service</i>	The name of the service to which the user connected. Possible values are POP, IMAP, ADMIN, XMLML (XML Mail), WEBML (WebMail), CLNDR (WebCal—the user logged in through http://hostname/mc).
<i>security</i>	A two-part field separated by a colon (:). The first part indicates the kind of encryption used in the connection; possible values are CLR (cleartext, no encryption), SSH (secure shell; for administration connections only), and SSL (secure sockets layer). The second part indicates the authentication method used to connect; possible values are PLAIN (plaintext authentication) and KERB4 (Kerberos version 4).
<i>IP-addr</i>	The IP address of the connecting host.
<i>user</i>	The login name of the connecting user.
<i>duration</i>	(LOGOUT only) The duration of the connection in seconds.
<i>activity count</i>	A count of the number of appends (app), deletes (del), and expunges (exp) done by the user.

Failed by User (Logins)

The **Failed Logins by User** report lists failed login attempts for the selected day by user. Users are listed according to most failed login attempts. Each line in the report has the following fields:

Table 43 Failed Logins By User

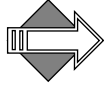
Field	Description
User	The login name of the user
Svc	The name of the service to which the user failed to connect. Possible values are POP, IMAP, ADMIN, XMLML (XML Mail), WEBML (WebMail), CLNDR (WebCal—the user logged in directly).
Security	A two-part field separated by a colon (:). The first part indicates the kind of encryption used in the login attempt; possible values are CLR (cleartext, no encryption), SSH (secure shell; for administration connections only), and SSL (secure sockets layer). The second part indicates the authentication method used in the login attempt; possible values are PLAIN (plaintext authentication) and KERB4 (Kerberos version 4).
Stat	The status of the connection. The value is always FAIL, meaning the connection failed.
Count	The total number of failed login attempts by the user for this service since midnight of the selected day.

Failed by IP (Logins)

The **Failed Logins by Remote IP Address** report lists failed login attempts for the selected day by the IP address of the remote system attempting the connection. IP addresses are listed according to most failed login attempts. The first field in each line of the report is IP Addr, the IP address of the remote system. The remaining fields are as described in Table 43, “Failed Logins By User,” above.

Security Reports

The system maintains daily logs of security-related events on the primary system, including the identification of junk mail and virus-bearing messages, and content-filtering activity.



The security report does not display if you have selected a delegated domain.

These are the available **Security** reports:

- ◆ **Anti-Virus Reports:** Summary and detailed information about viruses found on your system.
- ◆ **Anti-Spam Reports:** Detailed information about messages identified as junk mail.
- ◆ **Content Filtering Reports:** Detailed information about content filtering policies applied to messages on your system.
- ◆ **MailHurdle Reports:** Detailed information about MailHurdle policies applied to messages on your system.



When you have high volume of incoming mails causing high load and CPU usage, look for some type of pattern (based on sender/recipient) in the antivirus and/or antispam reports, this can help if your system is hit by some denial of service or spam attack. If you are seeing that some valid mails are getting filtered (rejected/discard), then content filtering is the right place to look. Content filtering tells you which filter triggered on a particular message.

Anti-Virus Reports

The **Anti-Virus Reports** show a recent history of virus scanning activity on the system. Click one of the following:

- ◆ **Summary:** Displays the Virus Scanning Summary, showing a summary of viruses found on your system during the selected day.
- ◆ **Detailed:** Displays the Detailed Virus Scanning Information report, showing detailed information about these viruses.

Virus Scanning Summary Report

The **Virus Scanning Summary** report contains these summary reports for the selected day:

- ◆ **Viruses By Originator:** A list of addresses that sent viruses sorted alphabetically by originator
- ◆ **Viruses By Recipient:** A list of local addresses that received viruses sorted alphabetically by recipient
- ◆ **Viruses Found:** A list of viruses found

Both the **Viruses by Originator** and **Viruses by Recipient** reports have the following fields:

address *virus-name* *count*

The **Viruses Found** report has only these fields:

virus-name *count*

Table 44 Virus Scanning Summary Report

Field	Description
<i>address</i>	The address that sent or received the virus
<i>virus-name</i>	The name of the virus, as identified by the Sophos virus-scanning software
<i>count</i>	The number of instances of this virus sent or received by this address

Detailed Virus Scanning Information Report

The **Detailed Virus Scanning Information** report lists, in table format, every virus event chronologically for the selected day. Each table row has the following fields:

xport Date:
 Virus: *name* in [*mime-part*] (*filename*)
 Recipient:
 Sender:
 Action:

Table 45 Detailed Virus Scanning Information Report

Field	Description
<i>xport</i>	The message transport protocol; this field always has the value SMTP
Date	The date and time that virus was found
Virus name, mime-part, filename	The virus name, as identified by the Sophos virus scanning software (the virus name is a link to information about the virus on the Sophos web site), the number of the MIME part of the attachment containing the virus, and the filename of the attachment containing the virus
Recipient	The local address that received the virus
Sender	The address of the sender of the infected message
Action	The action taken on the virus; possible values are FOUND, meaning the virus was found and passed on to the recipient without further action; CLEANED, meaning that the virus was purged from the infected attachment; DELETED, meaning that the infected attachment was deleted; and QUARANTINED, meaning that the message was forwarded to the specified quarantine address. Anti-Virus Quarantine is different from Content Filtering Quarantine in that it uses a host the system administrator specifies, not the Quarantine Manager. For details on the Quarantine action, see “How Antivirus Quarantine Works” on page 398 .

Anti-Spam Reports

The **Anti-Spam Information** report contains two reports for the selected day:

- ◆ **Top Spammer Statistics:** A list of the top 100 addresses that sent messages identified as junk mail, starting with the largest number of junk mail messages sent.
- ◆ **Top Spam Recipient Statistics:** A list of the top 100 addresses that received junk mail, starting with the largest number of junk mail messages received.

Both reports have the following fields:

address *sent-recv* *count*

Table 46 Anti-Spam Information Report

Field	Description
<i>address</i>	The address that sent or received the junk mail
<i>sent-recv</i>	Possible values are sent for messages sent, and rcv for messages received
<i>count</i>	The number of junk mail messages sent or received by this address

Content Filtering Reports

The **Content Filtering Statistics** report lists the content filtering policies applied to messages during the selected day. For each policy, the following fields are shown:

Policy Name: *domain/rule-name*

Action: *action*

Total Hits: *count*

Table 47 Content Filtering Statistics Report

Field	Description
<i>domain</i>	The domain name (such as example.com) or pseudo-domain (such as primary , local , nonlocal , or any) to which the policy applies. See “Creating a Message Filter” on page 339 for details on using this filtering option.
<i>rule-name</i>	The unique name of the rule that defines this policy; this is usually a system-generated name, such as Unnamed Rule 0 or (implicit)
<i>action</i>	The action taken on the messages to which the policy was applied; the possible values are the message filter actions. See “Creating a Message Filter” on page 339 for details on filtering.
<i>count</i>	The number of messages to which this policy was applied during the selected day

MailHurdle Reports

The **MailHurdle** reports categorize the email addresses and domains responsible for spamming your box. There are three summary reports, described below.



Use these reports to find out delay based on sender or recipient, what percentage is getting delayed or rejected, and if some valid mails are getting delayed, then exempt the sender or recipient, respectively, from MailHurdle using the Allowed Senders and/or Allowed Mailing Lists filters; for details, see [“Setting the Allowed Senders List” on page 425](#) or [“Setting the Allowed Mailing Lists List” on page 431](#).

Host (MailHurdle)

The **MailHurdle Host Summary** breaks down the information by host name. It is sorted by the percentage of messages rejected, and then total number of rejections.

Table 48 MailHurdle Host Summary

Field	Description
<i>Host</i>	The host running MailHurdle.
<i>% Delayed</i>	The percentage of messages from that sender IP, that were delayed by MailHurdle because no valid triplet existed.
<i>Delays</i>	The number of messages that did not retry within the allotted time period and were rejected.
<i>Accepts</i>	The number of messages that did retry within the allotted time period and were accepted for delivery.
<i>Sender IP</i>	The IP address from which the spam came.

To Address (MailHurdle)

The **MailHurdle To Address Summary** breaks down the information by IP address for recipients; and then each chunk is sorted by the percent of rejections, and then the total number of rejections.

Table 49 MailHurdle To Address Summary

Field	Description
<i>To</i>	The email address to which the spam was sent.
<i>% Rejected</i>	The amount of mail that did not retry within the allotted time period and was rejected.
<i>Msg Rej</i>	The number of messages that did not retry within the allotted time period and were rejected.
<i>Msg Acpt</i>	The number of messages that did retry within the allotted time period and were accepted for delivery.
<i>Sender IP</i>	The IP address from which the spam came.

From Address (MailHurdle)

The **MailHurdle From Address Summary** breaks down the information by IP address for senders; and then each chunk is sorted by the percent of rejections, and then the total number of rejections.

Table 50 MailHurdle From Address Summary

Field	Description
<i>From</i>	The email address from which the spam came.
<i>% Rejected</i>	The amount of mail that did not retry within the allotted time period and was rejected.
<i>Msg Rej</i>	The number of messages that did not retry within the allotted time period and were rejected.
<i>Msg Acpt</i>	The number of messages that did retry within the allotted time period and were accepted for delivery.
<i>Sender IP</i>	The IP address from which the spam came.

System Reports

The **System Information** report for a specified date lists all system log events (for that day) in chronological order.



Many items listed in the system information report are informational and require no action. Usually items that require attention have the phrase “System Alert” associated with them. As with other reports, it is important to understand what your baseline looks like so that you can react, if needed, to something new that starts to show up in the system information report.

The format for each line is:

year month day hh:mm:ss event cause

Table 51 System Information Report

Field	Description
<i>year</i>	The four-digit year of the event
<i>month</i>	The two-digit month of the event
<i>day</i>	The two-digit day of the event
<i>hh</i>	The two-digit hour of the event
<i>mm</i>	The two-digit minute of the event
<i>ss</i>	The two-digit second of the event
<i>event</i>	The event name
<i>cause</i>	The event description or the reason that the event was logged

Command Report

The **Command Report** lists every administration protocol command received by the message server on the selected day and all command responses. The format for each line is:

year/month/day hh:mm:ss id userin-out cmd-resp

Table 52 Command Report

Field	Description
<i>year</i>	The four-digit year of the event
<i>month</i>	The two-digit month of the event
<i>day</i>	The two-digit day of the event
<i>hh</i>	The two-digit hour of the event
<i>mm</i>	The two-digit minute of the event
<i>ss</i>	The two-digit second of the event
<i>id</i>	The unique identifier for the administration service connection (session) in which the command was issued
<i>userin-out</i>	The user who issued the command (including domain name, for a delegated domain user), followed by > or <, which indicates whether <i>cmd-resp</i> is a command (>) or a command response (<)
<i>cmd-resp</i>	The text of the command or command response. See the Administration Protocol Reference for details about administration protocol commands.

Folders Report

The Folders report has the following sections:

- ◆ **Folder Size & Quota Information:** Information on all folders on the system.
- ◆ **Largest 50 Folders:** Information on the largest 50 system folders.
- ◆ **Top 50 Folders Nearest Quota:** Information on folders closest to being over-quota.



Use this report to ensure that users are not going over quota; also, to develop an understanding of how storage is being used on the system. If there are storage problems on the system, you might be able to identify users that are exploiting the storage space and/or candidates for archiving.

Folder Size & Quota Information

The **Folder Size & Quota Information** report lists all folders on the system hierarchically and alphabetically. For example, the folders `user.fred.Draft` and `user.fred.Sent` would be represented this way:

```
user
  fred
    Draft
    Sent
```

There is a **Folder Size & Quota Information** report for the primary domain and for each delegated domain on the system. Each line in the report has the following fields:

Table 53 Folder Size & Quota Information

Field	Description
Folder name	The name of the folder; indented folder names are subfolders.
Size	The folder size in kilobytes (KB)
Quota	The disk usage and quota of the folder in kilobytes, in the format <i>used/ quota</i>

Largest 50 Folders

The **Largest 50 Folders** report lists the largest 50 folders on the system by size, starting with the largest. Each line in the report has **Folder name** and **Size** fields, as described in Table 53, “Folder Size & Quota Information,” above, except that **Folder name** is the full folder path, such as `user.fred.Draft` and not indented hierarchically.

Top 50 Folders Nearest Quota

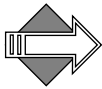
The **Top 50 Folders Nearest Quota** report lists the 50 folders that are closest to over quota, starting with the folder closest to quota. Each line in the report has **Folder name** and **Size** fields, as in the **Largest 50 Folders** report, and a **Quota Percentage** field that shows the percentage of quota that the folder is using (for example, a folder that’s occupying 9KB and has a quota of 10KB has a quota percentage of 90%).

Backup and Restore Tasks

Data stored on a Mirapoint Message Server must be backed up regularly to ensure that mail data can be recovered in the event of a disaster or if it is accidentally deleted.

The following topics are included:

- ◆ [Mirapoint Backup Solutions](#): An overview of backup available options.
- ◆ [Backup and Restore Concepts](#): Concepts you should understand before proceeding with a Mirapoint backup option.
- ◆ [Using NDMP for Backup](#): How to use the NDMP backup solution.
- ◆ [Using the Administration Protocol for Backup](#): How to use the Mirapoint administration protocol backup solution.



This chapter includes several pointers to articles in the Mirapoint Knowledge Base on the Customer Support website, <http://support.mirapoint.com>. You need your Mirapoint customer service login name and password to access this information. If you don't have a Mirapoint Support login ID, send an email to support-admin@mirapoint.com requesting one.

Mirapoint Backup Solutions

Mirapoint supports two backup solutions:

- ◆ Network Data Management Protocol (NDMP) by means of the following supported clients:
 - ❖ Veritas NetBackup (4.5, 5.1 or 6.0)
 - ❖ Legato NetWorker (7.1)
 - ❖ Tivoli Storage Manager (5.2.2)
 - ❖ BakBone NetVault (7) with NDMP Plugin Module
- ◆ Mirapoint administration protocol **Backup** and **Restore** commands with these backup devices:
 - ❖ Local tape—A directly connected tape drive.
 - ❖ Remote Magtape Protocol (RMT)—The tape drive is remote, so backup uses the RMT protocol.



NDMP is the Mirapoint recommended backup solution. NDMP offers higher data rates and capacities, especially if you choose image backup, and most importantly if the need arises to restore data.

About NDMP Backup

An NDMP client requires these two NDMP services to do backups: **data** and **mover/tape**. Third-party clients do not necessarily have the services required, so they look for other servers to provide services. Some third-party clients provide only the **mover/tape** service. Mirapoint NDMP service provides the **mover/tape** and **data** services required.

Depending on the NDMP client, you can perform a backup or restore in one of two ways:

- ◆ **Local**—Data on the Mirapoint server is backed up to a storage device that is attached to it by a SCSI.
- ◆ **Three-way**—Data on the Mirapoint server is backed up to a storage device that is attached to a different server. One example would be NetWorker server via SnapImage.

NDMP Backup Process

The NDMP client resides on a system other than the Mirapoint Message Server. The client initiates a request for information from a system that has the NDMP **mover/tape** service enabled and started. That **mover/tape** service responds with the information requested.

The client then sends a command along with the information returned from the **mover/tape** service to the **data** service. That **data** service then begins the backup, and sends that backup information to the system that is connected to the specified remote tape device.

Veritas NetBackup NDMP

You can use Veritas NetBackup BusinessServer to perform image-based backups and restores to either local or three-way tape drives. Mirapoint currently requires Veritas NetBackup version 4.5 or higher and NetBackup for NDMP on the same server.

For information about setting up and using Veritas for Mirapoint backups and restores, see the following articles in the Mirapoint Knowledge Base at <http://support.mirapoint.com>:

- ◆ [Article #323](#), “Configuring Veritas NetBackup Version 4.5 for NDMP (MOS 3.6 and Later)”
- ◆ [Article #370](#), “Configuring Veritas NetBackup Version 5.1 for NDMP (MOS 3.6 and Later)”
- ◆ [Article #213](#), “Performing an NDMP Message-Based Incremental Backup Using Veritas NetBackup”
- ◆ [Article #297](#), “Using Veritas NetBackup Version 4.5 to Perform a Manual Backup”
- ◆ [Article #374](#), “Using Veritas NetBackup Version 5.1 to Perform a Manual Backup”
- ◆ [Article #374](#), “Using Veritas NetBackup Version 4.5 or 5.1 to Perform an NDMP Selective Restore From Image”
- ◆ [Article #289](#), “Using Veritas NetBackup Version 4.5 to Perform an NDMP Restore”

- ◆ [Article #201](#), “Using a Veritas NetBackup Image Backup to Recover the System”

For more information about Veritas NetBackup go to:

<http://www.veritas.com>

Legato NetWorker NDMP

You can use Legato NetWorker 6 or higher with NDMP to perform image-based backups and restores to either local or three-way tape drives.

For information about setting up and using Legato NetWorker for Mirapoint backups and restores, see the following articles in the Mirapoint Knowledge Base at <http://support.mirapoint.com>:

- ◆ [Article #326](#), “Configuring Legato NetWorker Version 7.1 for Mirapoint NDMP Backup (MOS 3.6 and Later)”
- ◆ [Article #242](#), “Using Legato NetWorker to Perform a Manual Full Backup”
- ◆ [Article #243](#), “Performing a Mirapoint NDMP Restore Using Legato NetWorker”
- ◆ [Article #270](#), “Using Legato NetWorker to Perform a Save Set Restore”
- ◆ [Article, #298](#), “Using Legato NetWorker Version 7.1 to Perform an NDMP Selective Restore From Image”

For more information about Legato NetWorker go to:

<http://www.legato.com>

Tivoli Storage Manager NDMP

You can use Tivoli Storage Manager (TSM) to perform image-based backups and restores to local tape drives. Mirapoint currently requires TSM version 5.2.2 or higher.

For information about setting up and using Veritas for Mirapoint backups and restores, see the following articles in the Mirapoint Knowledge Base at <http://support.mirapoint.com>:

- ◆ [Article #400](#), “Configuring Tivoli Storage Manager for Mirapoint NDMP Backup”
- ◆ [Article #401](#), “Using Tivoli Storage Manager to Perform a Backup”
- ◆ [Article #402](#), “Using Tivoli Storage Manager to Restore Files”

BakBone NetVault NDMP

You can use BakBone NetVault with the NDMP Plugin Module to perform Mirapoint backups and restores. Mirapoint currently requires NetVault version 7 or higher.

For information about setting up and using BakBone NetVault for Mirapoint backups and restores, see the Mirapoint Knowledge Base at <http://support.mirapoint.com>.

For more information about BakBone NetVault, go to:

<http://www.bakbone.com>

About Administration Protocol Backup

Local backups and Remote MagTape (RMT) backups share system facilities. The only differences are the **tape** versus **remote** command keyword, and the ability to set blocksize for RMT.

Mirapoint appliance software supports a local tape drive. One SCSI tape drive or one tape library operating in **sequential mode** (also called “stacker” mode) can be attached to a Mirapoint appliance for performing local system backup and restore.

To find out which devices Mirapoint currently supports, refer to the Customer Support website at <http://support.mirapoint.com>.

Alerts and Completion Status

The Mirapoint appliance predefines two distribution lists related to administration protocol backups. These distribution lists receive status messages and alerts informing recipients of backup and restore status.

- ◆ **Backup-alerts:** A backup or restore operation requires changing remote media (such as tape). The message is the same as output of the **Backup Media Wanted** or **Restore Media Wanted** command.
- ◆ **Backup-status:** A backup or restore operation has completed, so a message is sent to indicate success or the reason for failure.



These two distribution lists have no members at first. You must decide who should receive these alerts and add their email addresses to the distribution lists. You can use a pager email address so that person is paged when a backup alert or status email is sent.

Backup and Restore Concepts

Backing up and being able to restore your appliance data is a vital part of any system management plan. This section provides information about backup and restore and summarizes the Mirapoint implementation.

Backup Schemes

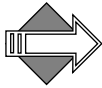
The backup scheme answers *How* you are going to back up *What*:

- ◆ **Image-based** versus **message-based**—An image-based backup takes a “snapshot” of the entire system. This is quick, but memory intensive. Message-based backups can save all system information, or only the information that changed since the last message-based backup was performed. This is slower, but it is easier to back up and restore individual mailboxes.
- ◆ **Full** versus **incremental** versus **selective**—A full backup backs up all the data on the specified system. An incremental backup backs up

only the data that has changed since the last backup. A selective backup backs up only specified mailboxes.

The administration protocol backup method supports **message-based** backup and restore. This allows incremental backup and restore, selective backup and restore of a specified user mailbox, and the ability to back up or restore while messaging services are up and running.

Mirapoint administration protocol (local tape and RMT) backup supports multiple incremental backup levels between 0 and 9.

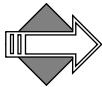


The recommended backup scheme is to do image-based backups with NDMP on a regular schedule.

Image-Based Backups with NDMP

Image-based backups bypass the Mirapoint file system, copying to backup media only sectors of the disk that are in use by the system. Image-based backup and restore uses NDMP and is faster, for both backup and restore, than message-based full backup and restore. Message-based restore could take days on very large systems.

Image-based restore is also time-consuming and works *only* if you are restoring to *exactly* the same MOS version from which the backup was taken. Also, licenses must be applied before starting the restore. As of Release 3.6, selective restore from image backup is supported, making it more convenient to restore mailboxes on demand.



You must reboot the appliance after performing an image-based restore. Image-based full restore is intended primarily for disaster recovery and should be done immediately after reinstalling the appliance.

What Is and What Is Not Backed Up

Table 54 summarizes what is saved by *image-based* versus *message-based* backups.

Table 54 What Gets Backed Up—Image-Based vs. Message-Based

Data	Image-Based	Message-Based
Mailboxes	Yes	Yes

Table 54 What Gets Backed Up—Image-Based vs. Message-Based (Continued)

Data	Image-Based	Message-Based
User accounts	Yes	Yes
Distribution lists	Yes	Yes
Calendar and address book	Yes	Yes
The SMTP delivery queue	Yes	No
Mail logs and system logs	Yes	No
\Recent and \Seen mailbox flags	Yes	No
Directory Information	Yes	No
Operations Console Information	Yes	No
Mirapoint licenses	No	No
SSH keys	No	No
The appliance host name	No	No
The appliance DNS domain name	No	No
Appliance IP address and router	No	No

Message-based incremental backups save only messages added to a mailbox since the last backup. Other mailbox state changes (such as deletions and changes to message flags) are not saved.

Selective backups allow you to save one or more individual mailboxes. For more details, enter **Help Backup Selective** from the CLI.

When performing a message-based selective backup or restore, first run the **Domain Setcurrent** command to set the proper domain. Selective backup or restore can be done one domain at a time only.

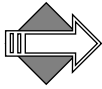
Selective restore from image backup is initiated with NDMP software, and can be traced with the **Ndmp Merge Status** command.

About Tape Drives and Tape Libraries

A **locally attached tape drive** is a peripheral device that reads and writes magnetic tape. Mirapoint supports one locally attached tape drive per appliance. The SCSI interface for it is either single-ended or low voltage differential (LVD), depending on the model.

A **tape library** (also called **autochanger** or **jukebox**) is a storage device for magnetic tapes moved by robotic mechanism and inserted into one or more tape drives for reading and writing. When a tape becomes full, the library supplies the tape drive with empty media so backup can continue without interruption.

To find out which devices Mirapoint currently supports, see [Article # 159](#), “Approved Local Tape and Library Devices” in the Mirapoint Knowledge Base at <http://support.mirapoint.com>.



All administration protocol backups, whether full or incremental, always start from the beginning of the tape.

Backup Protocols

Backup can be done using NDMP or the administration protocol.



Mirapoint recommends that you implement an NDMP-base backup solution.

NDMP Protocol

The Network Data Management Protocol (NDMP) is a standard that specifies the data exchange method between the various components used to back up a network-attached storage (NAS) device. Mirapoint's current implementation is NDMP version 3. NDMP is often associated with NetApp servers.

NDMP separates the data path and the control path, so network data can be backed up locally, yet readily managed from a central location. For more information on NDMP, see <http://www.ndmp.org>.

Administration Protocol

A Mirapoint appliance can be backed up and restored using a local tape drive, or a remote tape device connected to a Sun Solaris system using the RMT protocol.

Both Administration Protocol methods use the following syntax:

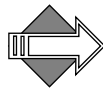
```
Backup type-of-backup device blocksize  
Restore type-of-backup device blocksize
```

Default blocksize is 10240 bytes (10 KB) for RMT. Before using RMT to back up and restore a Mirapoint appliance from a Sun Solaris system, the Solaris system must be properly configured with tape drive and RMT software package.



Mirapoint does not recommend using RMT tape backup. NDMP image-based backups are the recommended backup scheme.

With the administration protocol you can back up to a stand-alone locally attached tape drive, or to a tape library in sequential mode.



Two administration roles are given the permissions needed to perform Mirapoint appliance backups: administrator and backup operator. An administrator has the ability to use all commands. The backup operator can perform backups and view appliance settings only. The backup operator is not allowed to perform restores or use any of the other commands that change appliance configuration in any way.

Using NDMP for Backup

To use an NDMP backup solution, you need to enable and start the Mirapoint NDMP service on the appliance you're backing up, and configure your data management application (DMA) to perform Mirapoint backups.



The NDMP license and service is required for all NDMP backup solutions.

Setting Up the NDMP Service

To set up the NDMP service:

1. Make sure you have applied the NDMP license to your appliance.
2. Enable and start the NDMP service with the **Service Enable** and **Service Start** commands:

```
Service Enable Ndm  
Service Start Ndm
```

3. Set the Data Management Application (DMA) and the NDMP version with the **Ndm Set** command. (This is optional.)

```
Ndm Set Dma Product  
Ndm Set Version 3
```

Product can be **Default**, **Legato**, **Veritas**, **Tivoli**, or **BakBone** and *version* can be 2, 3, or 4. Setting the correct version might improve function.

Configuring Your DMA

To find information about how to configure your DMA to perform Mirapoint Backups, see [Article #330, “NDMP Backup and Restore: Where Do I Begin?”](#) in the Mirapoint Knowledge Base at <http://support.mirapoint.com>.

Restoring Data with NDMP

NDMP image-based full restore is intended for disaster recovery, and must be done on a freshly installed appliance with licenses reapplied and messaging services turned off. To perform an NDMP disaster recovery:

1. Install the MOS release used at backup time.
2. Configure network parameters.
3. Apply all licenses using the keys on your license sheet.
4. Perform the image recovery as described in the Mirapoint Knowledge Base article for your DMA on the Customer Support website at <http://support.mirapoint.com>.

5. Reboot the appliance.

You can also perform selective restores from the backup image to recover individual folders. For more information, see the selective restore article for your DMA in the Mirapoint Knowledge Base at <http://support.mirapoint.com>.

Using the Administration Protocol for Backup

The command-line interface (CLI) provides two commands for initiating administration protocol backup and restore operations:

- ◆ **Backup**—initiates full, incremental, and selective backups. Also monitors backup operations.
- ◆ **Restore**—initiates recovery for the various backup types. Also monitors restore operations.

The Mirapoint administration protocol supports either local SCSI tape drive or remote storage using Remote MagTape (RMT) protocol to a Sun Solaris system.

For RMT, you must first configure a Solaris system with tape drive, as described by “Configuring a Solaris System for RMT” on page 534. RMT backup to disk is neither recommended nor supported.



Mirapoint recommends using NDMP to perform image-based backups instead of using RMT. For more information, see “Using NDMP for Backup” on page 528.

For more information about the backup and restore commands, see **Help Backup** and **Help Restore** in the CLI.

For information on backup, restore, protocols, and tape devices, see “Backup and Restore Concepts” on page 524.

For information on what data is saved by message-based backup, see “What Is and What Is Not Backed Up” on page 525.

Using the Administration Protocol with a Local Storage Device

This section describes how to:

- ◆ Install a Local Tape Drive for Backup
- ◆ Perform a Full Backup to a Local Storage Device
- ◆ Perform a Selective Backup to a Local Storage Device
- ◆ Perform a Full Restore from a Local Storage Device
- ◆ Perform a Selective Restore from a Local Storage Device

Installing a Local Tape Drive for Backups

To install a tape drive and prepare for backing up:

1. Power down the Mirapoint appliance to prepare the SCSI connection.
2. Connect one end of the cable to the Mirapoint appliance's SCSI tape port and the other end to either of the tape drive's SCSI ports.
3. Make sure that the SCSI bus is properly terminated. If necessary, place a terminator on the remaining SCSI port of the tape drive. This enables impedance matching to prevent reflections.
4. Mirapoint hardware provides a built-in SCSI tape connector.
5. Power up components in this order:
 - ❖ RAID disk shelf if your appliance is equipped with one
 - ❖ The tape drive or library
 - ❖ The Mirapoint appliance

When the appliance boots, it recognizes the newly connected tape drive.



Important reminders:

- ◆ Never power down a digital linear tape (DLT) device with a tape in the drive. This causes directory information to be lost, which results in excessive reboot times and slower tape access times.
- ◆ Never power down the tape or autoloader while the Mirapoint appliance is running. This action can cause the appliance to become unreliable, including the possibility of a appliance crash.

- ◆ Never cable the tape or autoloader to the RAID connectors used by the disk arrays. This can result in severe data corruption.

Performing a Full Backup to a Local Device

To perform a full backup of a Mirapoint appliance to local tape drive or library:

1. Load a tape into the drive.

For a tape library:

Ensure that the device is set to sequential (or stacker) mode, place tapes into contiguous storage slots, load the first tape according to manufacturer instructions, and close the door.

2. Wait for the device's **Tape in Use** light (or similar) to stop flashing.
3. Start the backup using the CLI **Backup** command, which issues a numeric job ID:

```
Backup Full Tape ""  
* Backup-jobID
```

Backup begins. When the tape fills, members of the backup-alerts distribution list receive email and the drive ejects the tape.

4. Place the filled, ejected tape cartridge in a safe location. To continue backup, insert a new tape and use the command-line interface to inform the Mirapoint software that the tape was changed.

For a tape library:

By default, backup does not continue automatically when the stacker library changes tapes. For locally attached tape libraries in sequential mode, the **Backup** and **Restore** commands accept **continue=true** parameter to enable automatic continuation.

5. Go to step 4 and repeat as necessary until backup is completed.

For a tape library:

After all tapes are filled, remove tapes from storage slots, place full tapes in a safe location, refill slots with new tapes, load the first tape, and close the door.

Performing a Selective Backup to a Local Device

To perform a selective backup to a local tape drive or library, start the backup with the following command:

```
Backup Selective Tape "" "User.username"
```

In this command:

- ❖ *System* is the name of the system to which the tape device is connected; for example, a Sun Solaris system.
- ❖ "" accepts the default block size.
- ❖ *User.username* is the name of the record you want to back up, for example "user.joe" for the user mailbox for joe.

Performing a Full Restore from a Local Device

To perform a full restore from a local storage device, start the restore with the following command:

```
Restore All Tape
```

Performing a Selective Restore from a Local Device

To perform a selective restore from a remote tape drive using RMT, start the restore with the following command:

```
Restore Selective Tape "" "User.username"
```

In this command:

- ❖ *System* is the name of the system to which the tape device is connected; for example, a Sun Solaris system.
- ❖ "" accepts the default block size.
- ❖ *User.username* is the name of the record you want to restore, for example "user.joe" for the user mailbox for joe.

Using the Administration Protocol with RMT

You can use the Remote Magtape (RMT) protocol to back up your appliance to a storage device on a remote Sun Solaris system.



Mirapoint recommends using NDMP to perform image-based backups instead of using RMT. For more information, see “Using NDMP for Backup” on page 528.

This section describes how to:

- ◆ Configure a Solaris System for RMT
- ◆ Issue Backup and Restore Commands for RMT
- ◆ Perform a Full Backup Using RMT
- ◆ Perform a Selective Backup Using RMT
- ◆ Perform a Full Restore Using RMT
- ◆ Perform a Selective Restore Using RMT

Configuring a Solaris System for RMT

Before you can use the CLI **Backup** and **Restore** commands with RMT, you must configure your Solaris system to allow your Mirapoint appliance to access the storage device.

To configure your Solaris system for Mirapoint backups via RMT:

1. Choose a user account to perform the backup. This backup user must have write permission on all special files associated with the backup device. The default backup user is **mira**. Create the backup user account if necessary, and set device permissions accordingly.
2. Grant the backup user (for example, **mira**) permission to log in to your Solaris system by creating or editing a file named **.rhosts** in the backup user’s home directory. Add the following line to that file, where *MirapointHost* represents the Mirapoint appliance name, and *BackupUser* the backup user’s login name:

```
MirapointHost BackupUser
```

- For security, restrict access to `.rhosts`; enter:

```
chown Backupuser .rhosts
chmod 400 .rhosts
```

- If the `/etc/rmt` command executable does not exist, create a symbolic link named `/etc/rmt` by entering:

```
ln -s RmtPath /etc/rmt
```

where *RmtPath* is the full path of the system **Rmt** command.



To restore **Rmt** backups from a tape device directly attached to the Mirapoint appliance, the blocksize must be set to 61440. Using any other blocksize will result in restore failures. (The tape itself is not affected by the restore failures and can still be used to complete a restore from a remote device.)

Issuing Backup and Restore Commands for RMT

To use RMT backup from a Mirapoint appliance, you issue **Backup** and **Restore** commands from the command-line interface.

When using a remote tape connected to a Unix system, the command specifies the **System:Devicename**. For example, if the appliance is called **dent**, and the tape device is called `/dev/rmt/0`, you would issue the following command to perform a full backup:

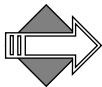
```
Backup Full dent:/dev/rmt/0
```

If you encounter problems using RMT for backups, see [Article #96](#), “Trouble with an Administration Protocol Backup Via RMT To A Unix System” in the Mirapoint Knowledge Base at <http://support.mirapoint.com>.

Performing a Full Backup Using RMT

To perform a full backup to a remote drive using RMT, start the backup with the following command:

```
Backup Full System:/dev/rmt/0
```



When using RMT, a full backup could take days, rather than hours. When tapes need to be changed, an alert is sent to members of the backup-alerts distribution list.

Performing a Selective Backup Using RMT

To perform a selective backup to a remote drive using RMT, start the backup with the following command:

```
Backup Selective System:/dev/rmt/0 "" "User.username"
```

In this command:

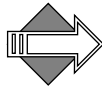
- ❖ *System* is the name of the system to which the tape device is connected; for example, a Sun Solaris system.
- ❖ */dev/rmt/0* is the default name of the tape device.
- ❖ "" accepts the default block size.
- ❖ *User.username* is the name of the record you want to back up, for example "user.joe" for the user mailbox for joe.

Performing a Full Restore Using RMT

To perform a full restore from a remote tape drive using RMT, start the restore with the following command:

```
Restore All System:/dev/rmt/0
```

System is the name of the system to which the tape device is connected; for example, a Sun Solaris system.



When using RMT, a full restore could take an extended period of time. When tapes need to be changed, an alert is sent to members of the backup-alerts distribution list.

Performing a Selective Restore Using RMT

To perform a selective restore from a remote tape drive using RMT, start the restore with the following command:

```
Restore Selective System:/dev/rmt/0 "" "User.username"
```

In this command:

- ❖ *System* is the name of the system to which the tape device is connected; for example, a Sun Solaris system.
- ❖ */dev/rmt/0* is the default name of the tape device.
- ❖ "" accepts the default block size.

- ❖ **User.username** is the name of the record you want to restore, for example “user.joe” for the user mailbox for **joe**.

Index



Symbols

"X" headers, about 236

A

abbreviations used in logs 494

about

Destination Domain filter option
332

domains 258

Exchange and Active Directory 126

Junk Mail filter 418

Junk Mail Manager accounts 453

mail filtering 332

MIME and filtering attachments
334

the Blacklist header 430

the Recipient-Whitelist header 434

the Whitelist header 428

trusted network specifiers 49

UCE Score Threshold 336

users and administrators 288

access control

changing 305

folders 301

permissions defined 302

accessing

Administration Suite 34

administrator, restricting 48

command line interface (CLI) 37

delegated domains 266

Junk Mail Manager 444

setting default 104

accounts

bulk creating for JMM 462

definition 288

Junk Mail Manager 453

Junk Mail Manager users, creating
454

Junk Mail Manager, bulk create file
format 462

Active Directory

about the MailHost attribute 126

getting the bindDN 126

setting for RazorGates securing
Exchange 127

setting for RazorGates with JMM
securing Exchange 162

Add/Edit Folders page 303

adding

arrays 246

delegated domain administrators to
the postmaster DL 264

delegated domains 261

delegated domains, task overview
260

distribution lists 312

- distribution lists to distribution lists
 - 312
 - groups, Operations Console 468
 - Junk Mail domains 451
 - members to distribution lists 312
 - remote members to distribution lists
 - 312
 - sub-folders 307
 - traps 255
 - users 292
 - users, Junk Mail Manager 454
- address book
 - configuring URLs 89
 - verifying the URL 102
- addressbook
 - url add**
 - syntax 89
- addresses
 - blocking 356
 - character limitations 291
- addressing mail
 - to folders 309
 - to sub-folders 309
- Admin Audit Trail** report 252
- administering groups, Operations
 - Console 469
- administration protocol
 - backup and restore commands 530
 - backups, about 528
 - backups, alerts and completion
 - status 524
- Administration Suite
 - accessing 34
 - administrator daily reports 476
 - setting the default timeout 68
 - Setup Wizard, using 36
- administration, setting security 50
- administrators
 - about 289
 - about the Quarantine
 - Administrator 289
 - accessing a user's folder 267
 - creating for delegated domains 263
 - default distribution lists 202
 - restricting access 48
- alarms, silencing 248
- alerts
 - antivirus notifications, RAPID 412
 - antivirus notifications, Sophos and
 - F-Secure 401
 - management 474
 - system health 250
 - viewing for groups 472
- all-in-one deployment
 - configuring antispam 76
 - configuring antivirus 69
 - configuring internal LDAP
 - directory 80
 - configuring MailHurdle 74
 - configuring user directory service
 - 80
 - example 63
 - required information 64
 - required licenses 65
 - requirements 64
 - troubleshooting 105
 - verifying 98
- Allowed Mailing Lists
 - about the Junkmail header 434
 - creating 432
 - domain level, creating 431
 - preventing MailHurdle delays 433
 - removing entries 434
 - searching for entries 433
 - setting 431
- Allowed Senders
 - domain level, creating 425
 - entries, finding 427
 - for antispam scanning 425

-
- AllowmisbehavingMailers 181
 - Anti-Spam Information** report 511
 - antispam scanning
 - about 416
 - about message filters 332
 - about the **Threshold** 336
 - configuring 420
 - configuring for all-in-one 76
 - configuring for multi-tier 183
 - configuring for RazorGates
 - securing Exchange 122
 - configuring for RazorGates with JMM securing Exchange 155
 - configuring MailHurdle 388
 - creating black lists 428
 - creating mailing list exemptions 431
 - creating RBL Host lists 437
 - creating Reject lists 435
 - creating Relay lists 434
 - creating white lists 425
 - destination domains, about 332
 - DSN (delivery status notification) filters 343
 - filtering out "virus deleted" messages 375
 - getting an immediate update 424
 - installing or removing rule groups 423
 - Junk Mail**, about 418
 - modifying 419
 - Principal Edition vs Signature Edition** 417
 - scanning outbound mail 422
 - setting the proxy server 424
 - specifying automatic updates 424
 - two techniques 336, 417
 - using **regex-matches** to modify the UCE score 374
 - antivirus
 - RAPID, configuring for multi-tier 183
 - Anti-Virus Reports** 509
 - antivirus scanning
 - available engines 397
 - checking current information, RAPID 415
 - checking current information, Sophos 409
 - common extension names 335
 - configuring for all-in-one 69
 - configuring for RazorGates
 - securing Exchange 114
 - configuring for RazorGates with JMM securing Exchange 148
 - configuring, RAPID 411
 - configuring, Sophos 400
 - F-Secure™**, pages 399
 - getting an immediate update, RAPID 415
 - getting an immediate update, Sophos 408
 - getting updates, RAPID 413
 - getting updates, Sophos and F-Secure 406
 - how quarantine works 398
 - predictive based, about 397
 - RAPID™**, pages 409
 - setting notifications, RAPID 412
 - setting notifications, Sophos and F-Secure 401
 - setting the proxy server, RAPID 415
 - setting the proxy server, Sophos 408
 - signature based, about 397
 - signature-based, configuring for multi-tier 182

- Sophos™, pages 399
 - specifying automatic updates,
 - RAPID 414
 - specifying automatic updates,
 - Sophos 408
 - types of viruses 398
- Array properties 246
- arrays
 - adding/configuring 246
 - deleting 247
 - installing 247
- attachments
 - about MIME and filtering 334
 - blocked, specifying 361
 - common virus extensions 335
 - redirected, specifying 364
- attribute value assertion, definition 59
- audience 25
- authentication 462
 - and filters 346
 - setting default 129
 - SMTP and MailHurdle 391
- autochanger 527
- autochangers, about 527
- AVA, definition 59
- Average Number of Recipients
 - Summary report 501
- Average Size Summary report 501
- B**
- Backup and Restore commands 520
- backup schemes
 - image-based 524
 - message-based 524
- backups
 - about tape drives and libraries 527
 - administration protocol commands 530
 - configuring Solaris for RMT 534
 - default blocksize on tape 535
 - full (local device) 532
 - full (RMT) 535
 - full vs. incremental vs. selective 524
 - image based 525
 - installing tape drives 531
 - message based 525
 - Mirapoint solutions 520
 - selective (local device) 533
 - selective (RMT) 536
 - supported tape drives 523
 - using admin (RMT) 534
 - what data gets backed up 525
- bindDN, getting for Active Directory 126
- blacklist header, about 430
- blocked
 - addresses 356
 - attachments 361
 - messages 359
- Blocked Senders
 - creating 429
 - finding entries 430
 - header, about 430
 - searching for entries 430
- boolean operators 241
- bulk accounts, Junk Mail Manager,
 - creating 461
- C**
- calendar
 - configuring URLs 86
 - enabling 88
 - enabling/starting 88
 - setting timeout 88
 - setting up group calendar 86
- calendars, subscribed, setting 285
- changing
 - default user limit in a delegated domain 273
 - folder access control 305

- folder access permissions 305
- folder quotas 306
- passwords for users 296
- passwords for users, Junk Mail Manager 455
- user data 296
- user data, Junk Mail Manager 455
- characters
 - disallowed for email addresses 291
 - prohibited in folder names 301
- checking
 - current antivirus information, RAPID 415
 - current antivirus information, Sophos 409
 - for software updates 46
 - the message queue 239
- Class of Service (COS)
 - finding 323
- class of service, *see* COS
- clearing, the message queue 230
- CLI commands
 - Backup and Restore 520
 - Domain Setcurrent 526
 - Ldap Addaccess 51
 - Ldap Flushcache 51
 - Ldap Set Cachetimeout 51
 - Ldap Testquery 51
 - Ndmp Merge Status 526
 - Netif Setlogical 440
- CLI, accessing 37
- codes used in reports 503
- colors, dashboard 473
- command line interface, *see* CLI
- Command Report** 515
- configuration
 - antivirus scanning, F-Secure 400
 - antivirus scanning, RAPID 410
 - junk mail scanning 419
 - pre-configuration checklist 31
 - prerequisites 33
 - SNMP 253
- configuring
 - address book URLs 89
 - antivirus for RazorGates securing Exchange 114
 - antivirus for RazorGates with JMM securing Exchange 148
 - arrays 246
 - calendar URLs 86
 - IMAP 93
 - inbound routing for RazorGates securing Exchange 125
 - inbound routing for RazorGates with JMM securing Exchange 161
 - internal LDAP directory all-in-one 80
 - Junk Mail Manager 447
 - Junk Mail Manager, multi-tier deployment 185
 - junk mail scanning 419
 - NIC failover 439
 - security screening, multi-tier deployment 180
 - SMTP 94
 - Solaris for RMT 534
 - user directory service for all-in-one 80
 - WebMail 91
- configuring antis spam
 - for all-in-one 76
 - for multi-tier 183
 - for RazorGates securing Exchange 122
 - for RazorGates with JMM securing Exchange 155
- configuring antivirus
 - for all-in-one 69
 - for multi-tier, RAPID 183

- for multi-tier, signature-based 182
- configuring MailHurdle
 - for multi-tier deployment 180
 - for RazorGates securing Exchange 119
 - for RazorGates with JMM securing Exchange 153
- configuring, MailHurdle
 - for all-in-one 74
- connections, SNMP setup 253
- content filtering
 - blocked addresses 356
 - blocked attachments 361
 - blocked messages 359
 - creating corporate word list 368
 - creating objectionable word list 371
 - creating wire taps 349
 - filter list entries 353
 - filter list words & phrases note 353
 - how quarantine works 337
 - order, general 334
 - redirected attachments 364
 - using the filter list 353
- Content Filtering Statistics** report 512
- conventions 25
- cookies, requiring 92
- corporate word list, creating 368
- COS
 - adding and populating 321
 - definition 317
 - enabling
 - features 318
- CPU Activity** graph
 - definitions 227
 - description 226
 - example use 227
- CPU usage, troubleshooting 206
- creating
 - administrators for delegated domains 263
 - Allowed Mailing Lists 432
 - antispam black lists 428
 - antispam mailing list exemptions 431
 - Blocked Senders entries 429
 - bulk accounts, Junk Mail Manager 461
 - corporate word list 368
 - delegated domain signatures 270
 - distribution lists in delegated domains 269
 - domain black lists 428
 - domain mailing list exemptions 431
 - domain quota messages 271
 - domain white lists 425
 - folders in delegated domains 268
 - groups, Operations Console 469
 - JMM accounts 462
 - Junk Mail domains 451
 - Junk Mail Manager accounts 454
 - message filters 340
 - objectionable word list 371
 - over-quota message delegated domains 271
 - RBL Host lists for antispam 437
 - Reject lists for antispam scanning 435
 - Relay lists for antispam 434
 - shared folders 307
 - white lists for antispam 425
 - wire taps 349
- customizing
 - Junk Mail domain Welcome messages 458
 - Junk Mail over-quota messages 459
 - over-quota message for delegated domains 271
 - quota messages for domains 271

-
- D**
- daily reports, attachments summary 476
 - dashboard
 - colors 473
 - how to use 472
 - data management application (DMA) 529
 - defaults
 - authentication, setting 129
 - backup user 534
 - boolean operator 239
 - changing user limit, delegated domains 273
 - distribution lists for administrators 202
 - filtering order 334
 - maximum number of group members 468
 - order of filtering 334
 - performance graphs view 204
 - setting HTTP access 104
 - tape blocksize 535
 - tape device name 536
 - user folder location 289
 - user folder location, Junk Mail Manager 453
 - virus alerts, Sophos and F-Secure 404
 - defaults, WebCal
 - main configuration in delegated domains 277
 - resources configuration in delegated domains 281
 - search configuration in delegated domains 279
 - setting in delegated domains 274
 - delegated domains
 - accessing 266
 - accessing a user's folder 267
 - adding the administrator to the postmaster DL 264
 - adding, procedure 261
 - adding, task overview 260
 - Blocked Senders 428
 - changing the default user limit 273
 - creating Allowed Mailing Lists 431
 - creating distribution lists 269
 - creating folders 268
 - creating signatures 270
 - creating the administrator 263
 - custom over-quota message 271
 - deleting 288
 - disk quota 262
 - editing 267
 - finding 265
 - LDAP enabled 259
 - properties 258
 - quota messages for 271
 - routing messages 259
 - selecting 265
 - sensitivity 260
 - setting user limit 262
 - setting user limits 268
 - setting WebCal defaults 274
 - WebCal subscribed calendars 285
 - what you can control 258
 - white lists for 425
 - delegated domains, WebCal
 - main configuration 277
 - resources configuration 281
 - search configuration 279
 - subscribed calendars 285
 - deleting
 - arrays 247
 - delegated domains 288
 - distribution lists 316
 - folders 308
 - groups, Operations Console 468

- Junk Mail users 456
 - spares 245
 - traps 255
 - user data, Junk Mail Manager 456
 - users 297
- deployments
 - all-in-one 63
 - RazorGate and Exchange 109
 - RazorGates securing Exchange 109
 - RazorGates with JMM securing Exchange 139
- Destination Domain**, filtering option 332
- Detailed Login Report** 507
- Detailed Mail Log** report 501
- Detailed Virus Scanning Information** report 510
- directory service
 - adding the address book URL 89
 - testing 102
- disallowed characters for email
 - addresses 291
- Disk** properties 245
- Disk Usage Information** graph
 - definitions 222
 - description 221
- Disk** view, properties 244
- distribution lists
 - adding distribution lists to 312
 - adding remote members to 312
 - adding/removing 312
 - adding/removing members 312
 - as aliases for users 311
 - creating in delegated domains 269
 - deleting 316
 - deleting, troubleshooting 316
 - editing 316
 - entry properties 310
 - finding 315
 - naming 311
 - reserved names 312
- DIT, definition 81
- DLs *see distribution lists*
- DLT device, power off 531
- documentation, about 26
- domain disk quota
 - setting 262
- domain names, definition 258
- Domain Setcurrent command 526
- domain user limit
 - setting 262
- domain, Junk Mail
 - customizing quota messages 459
- domains
 - about 258
 - creating black lists 428
 - creating mailing list exemptions 431
 - creating quota messages 271
 - creating white lists 425
 - primary, definition 258
- domains, delegated
 - accessing 266
 - accessing a user's folder 267
 - adding the administrator to the postmaster DL 264
 - adding, procedure 261
 - adding, task overview 260
 - changing the user limit 273
 - creating distribution lists 269
 - creating folders 268
 - creating signatures 270
 - creating the administrator 263
 - custom over-quota message 271
 - deleting 288
 - disk quota 262
 - editing 267
 - finding 265
 - LDAP enabled 259
 - properties 258
 - routing messages to 259

-
- selecting as current 265
 - setting user limit 262
 - setting user limits 268
 - setting WebCal defaults 274
 - WebCal main configuration 277
 - WebCal resources configuration 281
 - WebCal search configuration 279
 - WebCal subscribed calendars 285
 - what you can control 258
- domains, Junk Mail
- adding 451
 - administering 450
 - customizing Welcome messages 458
 - definition 444
 - finding 451
 - remote, definition 449
 - restoring the over-quota message 461
- DSN (delivery status notification) filters 343
- ## E
- editing
- antivirus notifications, RAPID 412
 - antivirus notifications, Sophos and F-Secure 401
 - blocked addresses list 356
 - blocked attachments list 361
 - blocked messages list 359
 - corporate word list 368
 - delegated domains 267
 - distribution lists 316
 - folders 303
 - groups, Operations Console 468
 - messages filters 340
 - objectionable word list 371
 - redirected attachments list 364
 - selecting domains for 265
 - traps 255
 - user data 296
 - wire taps list 349
- email messaging, overview 25
- enabling
- calendar 88
 - COS
 - IMAP 94
 - LDAP directory service 83
 - SMTP 95
 - WebMail 93
- envelopes, messages, reading 235
- Exchange
- outbound router KB articles 169
- exiting the groups administer pages 471
- exporting
- corporate word lists 368
 - group data 471
 - objectionable word lists 371
- exporting groups 471
- External Server Monitoring** graph
- definitions 220
 - description 218
 - example use 218
- ## F
- Failed Logins by Remote IP Address** report 508
- Failed Logins by User** report 508
- filter list
- entries 353
 - guidelines for using 353
 - using 353
 - words & phrases note 353
- filter templates
- LDAP group query 62
 - LDAP user query 62
- filtering
- about message filters 332
 - about MIME and attachments 334
 - about the antivirus quarantine 398

- about the Content Filtering quarantine 337
- about the Quarantine Administrator 289
- common virus attachment names 335
- creating filters 340
- Forward to vs. Send to Quarantine folder filter actions 355**
- order executed 334
- order, general 334
- out "virus deleted" messages 375
- reordering filters 347
- using patterns 323
- using **regex-matches** to modify the UCE score 374
- using the **Keep (process normally)** option 376
- filters
 - Allowed Mailing Lists 431
 - blocked addresses 356
 - blocked attachments 361
 - blocked messages 359
 - Blocked Senders 428
 - corporate word list 368
 - creating 340
 - destination domain 332
 - filter list entries 353
 - filter list words & phrases note 353
 - for DSN (delivery status notifications) 343
 - Junk Mail**, about 418
 - LDAP client query 59
 - logical operators 61
 - objectionable word list 371
 - redirected attachments 364
 - reordering 347
 - using for empty To/CC lines 344
 - using the filter list 353
 - using wordlists
 - white lists 425
 - wire taps 349
- filters, domains
 - black lists 428
 - mailing list exemptions 431
 - white lists 425
- finding
 - Blocked Senders entries 430
 - Class of Service 323
 - delegated domains 265
 - directory service contacts 102
 - distribution lists 315
 - folders 302
 - Junk Mail Manager accounts 455
 - messages in the queue 239
 - users 296
 - white list entries 427
- flushing the queue for a domain 242
- Folder Size & Quota Information** report 517
- folders
 - access control 305
 - access control lists 301
 - access permissions meanings 302
 - accessing in a delegated domain 267
 - adding sub-folders 307
 - address mail to sub-folders 309
 - addressing mail to 309
 - changing access permissions 305
 - changing quotas 306
 - creating in delegated domains 268
 - definition 300
 - deleting 308
 - finding 302
 - Folder Size & Quota Information** report 517
 - hierarchy separator 300
 - Largest 50 Folders** report 517
 - naming conventions 300
 - removing quotas 296

- renaming 307
- root 300
- setting quotas 295
- setting quotas, Junk Mail accounts 454
- setting the domain disk quota 262
- shared, creating 307
- special characters you cannot use 301
- Top 50 Folders Nearest Quota**
 - report 517
 - using patterns to search 323
 - working with 303
- folders reports 516
- Forward to vs. Send to Quarantine**
 - folder filter actions 355
- F-Secure
 - modifying 399
 - scheduling updates 406
 - setting notifications 401
- full backup, definition 524
- full name, definition 291
- fully qualified domain name (FQDN), definition 258
- function, definition 177

G

- gauges for performance graphs 203
- group calendar
 - configuring URLs 86
 - LDAP Routing license requirement 197
 - setting up 86
 - url add**
 - syntax 86
- group calendar attributes 86
- groups
 - Dashboard** page 472
 - exiting the administer pages 471
 - importing/exporting 471

- importing/exporting data 471
- groups, Operations Console
 - adding, editing, deleting 468
 - administering 469
 - creating 469
 - synchronizing 471

H

- hardware, monitoring disk, array, and store views 244
- headers, messages
 - about "X" headers 236
 - reading 235
- hosts, SNMP configuration 254
- HTTP redirection 52
- HTTP Root, setting 104

I

- IDE, definition 243
- image based backups 525
- IMAP
 - configuring 93
 - enabling 94
 - quota warning limit 94
- IMAP proxying 52
- importing
 - corporate word lists 368
 - group data 471
 - objectionable word lists 371
- importing groups 471
- inbound routing
 - configuring for RazorGates
 - securing Exchange 125
 - configuring for RazorGates with JMM securing Exchange 161
- incremental backup, definition 524
- installing
 - antispam rule groups 423
 - hot spare disks 245

MailHurdle known good mailers
 423
 new arrays 247
 tape drives for backups 531
internal LDAP directory, configuring
 for all-in-one 80
international login names 291
IP addresses, setting "trusted" 49

J

JMM, *see* *Junk Mail Manager*
jukebox 527
Junk Mail domains
 adding 451
 customizing quota messages 459
 customizing Welcome messages 458
 definition 444
 searching for 451
Junk Mail Manager
 about 443
 accounts, about 453
 administering domains 450
 bulk create accounts format 462
 bulk creating accounts 462
 configuration 447
 configuring for multi-tier
 deployment 185
 creating bulk accounts 461
 deleting accounts 456
 LDAP queries 446
 provisioning users, multi-tier
 deployment 186
 searching for accounts 455
Junk Mail Statistics graph
 "Total Messages" note 213
 definitions 213
 description 212
junkmail scanning, *see* *antispam*

scanning

L

Largest 50 Folders report 517
LDAP
 mailgroup schema definition 54
 Routing license and Group
 Calendar 197
Ldap Addaccess command 51
LDAP attributes
 group calendar
 LDAP attributes
 calendar 86
 groupcalendar 86
 LoginID 86
 mailhost 86
 Mailroutingaddress 86
 miUUID 86
LDAP client queries
 attribute value assertion 59
 basics 56
 filter logical operators 61
 filter template, group query 62
 filter template, user query 62
 filters 59
 setting up filters 61
 setting up, Message Director 56
 specification, attribute map 58
 specifications 57
LDAP directory service
 enabling 83
 for delegated domains 259
LDAP Directory Statistics 214
LDAP Directory Statistics graph
 definitions 215

Ldap Flushcache command 51
LDAP lookups 52
Ldap Set Cachetimeout command 51
Ldap Testquery command 51
Legato NetWorker 520
limiting TCP connections 90
local backup 523–535
Local Mail Traffic report 498
local tape backup 520
locally-attached tape drive 527
logging in
 Administration Suite 34
 command line interface (CLI)
 to Mirapoint Support 46, 519
logical operators, LDAP client query
 filters 61
login account, definition 288
login names
 international 291
 permitted characters 290
 reserved 292
Login Summary report 497
Login Traffic Rates report 506
LoginID LDAP attribute, definition 86
logins
 tracking with the Admin Audit Trail
 253
 tracking with the User Audit Trail
 252
logins reports
 Detailed Login Report 507
 Failed Logins by Remote IP Address
 508
 Failed Logins by User 508
 Login Summary 497
 Login Traffic Rates 506
 options 505
 Top Logins By User 505

logs, abbreviations 494

M

mail reports
 **Average Number of Recipients
 Summary** 501
 Average Size Summary 501
 Detailed Mail Log 501
 Local Mail Traffic 498
 Mail Traffic Summary 500
 Message Events by Hour 500
 options 495
 Remote Mail Traffic 499
 searching 504
 Top Mail Users 496
Mail Traffic graph
 definitions 208
 description 207
 what to look for 208
Mail Traffic Summary report 500
mail, addressing to folders 309
Mailhost LDAP attribute, definition 86
MailHurdle
 advanced options 392
 Allowed Host 392
 Allowed Mailing Lists, where
 placed 433
 and SMTP authentication 391
 antispam, about 388
 modifying 389
 reports 513
MailHurdle report 513
MailHurdle, configuring
 for all-in-one 74
 for multi-tier deployment 180
 for RazorGates securing Exchange
 119
 for RazorGates with JMM securing
 Exchange 153
Mailroutingaddress LDAP attribute,

- definition 86
- Message Director, setting up
 - LDAP client queries 56
- Message Events by Hour** report 500
- message filters
 - about 332
 - about MIME and filtering
 - attachments 334
 - about the quarantine action 337
 - creating 340
 - filter list entries 353
 - filter list words & phrases note 353
 - how quarantine works 337
 - Junk Mail**, about 418
 - reordering 347
 - using patterns 323
 - using **regex-matches** to modify the
 - UCE score 374
 - using the filter list 353
 - using the **Keep (process normally)** option 376
- Message Server, setting up
 - user autoprovisioning 90
- message-based backups 525
- messages 250
 - "X" headers 236
 - addressing to sub-folders 309
 - clearing the queue 230
 - codes used in reports 503
 - flushing the queue for a domain 242
 - in queue, what you can view 239
 - order of filtering 334
 - reading envelopes and headers 235
 - refreshing the queue 230
 - routing to delegated domain 259
 - searching the queue 239
 - sorting the queue 232
 - viewing in the queue 233
 - viewing the queue summary 230
- messaging overview 25
- MIME, about 334
- mira, default backup user 534
- Mirapoint documentation 26
- Misc** graph
 - definition 217
 - description 217
- miUUID** LDAP attribute, definition 86
- MOC**, *see Operations Console*
- modifying
 - antispam scanning 420
 - antivirus scanning, **RAPID** 411
 - antivirus scanning, **Sophos** 400
 - MailHurdle** 389
- monitoring
 - adding/configuring arrays 246
 - deleting arrays 247
 - deleting spares 245
 - scanning the **RAID** system 248
 - silencing alarms 248
 - system alerts 250
 - system health data tables 250
 - using the views: **Disk**, **Array** , and **Store** 244
 - viewing **Alerts** data 474
 - viewing array data 246
 - viewing disk data 244
 - viewing storage data 242
 - viewing store data 248
 - viewing system health data 249
 - weekly reports 478
- Mtaverify** rule group 181
- multi-tier deployment
 - configuring antispam 183
 - configuring **Junk Mail Manager** 185
 - configuring **MailHurdle** 180
 - configuring **RAPID** antivirus 183
 - configuring security screening 180
 - configuring signature-based

-
- antivirus 182
 - provisioning users for JMM 186
 - requirements 176
- ## N
- naming
 - about domains 258
 - distribution lists 311
 - folders 300
 - folders, renaming 307
 - international login names 291
 - reserved distribution list names 312
 - NDMP 520
 - about 520
 - image based backups 525
 - setting up 528
 - Ndmp Merge Status** command 526
 - Netif Setlogical** command 440
 - Network Data Management Protocol,
see NDMP
 - network specifiers, about 49
 - Network Traffic** graph
 - definitions 225
 - description 224
 - NIC failover alert message 441
 - NIC failover, configuring 439
 - non-anonymous binding 51
 - non-ASCII characters in login names
290
 - nonconformant mailers 181
 - notifications, antivirus scanning
 - RAPID 412
 - Sophos and F-Secure 401
- ## O
- objectionable word list, creating 371
 - Operations Console
 - adding, editing, and deleting groups
468
 - administering groups 469
 - alerts, management 474
 - creating groups 469
 - default groups 468
 - groups, management 466
 - groups, maximum allowed 468
 - synchronizing groups 471
 - order of filtering, default 334
 - outbound routing, KB articles reference
169
 - outbound sender masquerading 52
 - over-quota messages
 - creating for domains 271
 - customizing for Junk Mail domains
459
- ## P
- passwords
 - about 289
 - changing for users 296
 - changing for users, Junk Mail
Manager 455
 - definition 291
 - patterns, using in input 323
 - performance graphs
 - about the different views 204
 - gauges 203
 - Junk Mail Statistics** 212
 - LDAP Directory Statistics** 214
 - Mail Traffic** 207
 - pie charts 204
 - POP/IMAP Activity** 209
 - WebMail Activity** 210
 - pie charts categories 204
 - POP proxying 52
 - POP/IMAP Activity** graph
 - definitions 209
 - description 209
 - postmaster DL, adding delegated

- domain administrators to 264
- pre-configuration checklist 31
- predictive based antivirus, about 397
- primary domain, definition 258
- Principal Edition** antispam scanning 417
- provisioning
 - user accounts 298
 - users for JMM, multi-tier deployment 186
- proxy
 - setting for junk mail scanning 424
 - setting for virus scanning, RAPID 415
 - setting for virus scanning, Sophos 408
- Q**
- quarantine
 - about the Quarantine Administrator 289
 - antivirus scanning, about 398
 - content filtering, about 337
 - usage tips 337
- query filters 59
- query specification
 - about 57
 - attribute mapping 58
- queue
 - clearing 230
 - flushing for a domain 242
 - refreshing 230
 - searching for messages 239
 - sorting messages in 232
 - viewing messages in 233
 - viewing the summary 230
- quota messages
 - creating for domains 271
 - customizing for Junk Mail domains 459
- quotas
 - changing, folders 306
 - custom message for delegated domains 271
 - removing on folders 296
 - setting delegated domain user limits 268
 - setting domain user limits 262
 - setting for delegated domains 262
 - setting on Junk Mail folders 454
 - setting on user folders 295
 - warning limit for IMAP 94
- R**
- RAID, definition 242
- RAPID™** antivirus scanning 409
- RazorGates securing Exchange deployment
 - configuring antispam 122
 - configuring antivirus 114
 - configuring inbound routing 125
 - configuring MailHurdle 119
 - example 109
 - required licenses 111
 - requirements 110
 - setting Active Directory 127
 - SMTP settings 130
- RazorGates with JMM securing Exchange deployment
 - configuring antispam 155
 - configuring antivirus 148
 - configuring inbound routing 161
 - configuring MailHurdle 153
 - example 139
 - required licenses 141
 - requirements 140
 - setting Active Directory 162
 - setting the outbound router on Exchange 169
 - SMTP settings 159

- RBL Host lists
 - for antispam scanning 437
- redirected attachments, specifying 364
- refreshing the message queue 230
- Reject lists, for antispam 435
- Relay lists, for antispam scanning 434
- Remote Magtape Protocol (RMT) 520
- Remote Magtape protocol *see* RMT
- Remote Mail Traffic** report 499
- removing
 - Allowed Mailing Lists entries 434
 - Allowed Senders entries 427
 - antispam rule groups 424
 - Blocked Senders entries 430
 - distribution lists 316
 - Junk Mail users 456
 - members from distribution lists 312
 - RAPID antivirus rulesets 415
 - users 297
- renaming folders 307
- reordering filters 347
- reports
 - abbreviations used 494
 - codes used 503
 - daily, attachments summary 476
 - e-mail traffic 495
 - large, saving 502
 - protocol commands 515
 - security-related events 509
 - system, **System Information** 515
 - User Audit Trail** 251
- reports, folders
 - Folder Size & Quota Information** 517
 - Largest 50 Folders** 517
 - sections 516
 - Top 50 Folders Nearest Quota** 517
- reports, logins
 - Detailed Login Report** 507
 - Failed Logins by Remote IP Address** 508
 - Failed Logins by User** 508
 - Login Summary** 497
 - Login Traffic Rates** 506
 - sections 505
 - Top Logins By User** 505
- reports, mail
 - Average Number of Recipients Summary** 501
 - Average Size Summary** 501
 - Detailed Mail Log** 501
 - Local Mail Traffic** 498
 - Mail Traffic Summary** 500
 - Message Events by Hour** 500
 - Remote Mail Traffic** 499
 - searching 504
 - Top Mail Users** 496
- reports, security
 - Anti-Spam Information** 511
 - Anti-Virus Reports** 509
 - Content Filtering Statistics** 512
 - Detailed Virus Scanning Information** 510
 - MailHurdle** 513
 - sections 509
 - Virus Scanning Summary** 510
- required licenses
 - all-in-one deployment 65
 - RazorGates securing Exchange deployment 111
 - RazorGates with JMM securing Exchange deployment 141
- reserved login names 292
- resources, configuring for WebCal 281
- restores
 - administration protocol commands 530
 - and backups, performing full 536
 - performing full (local device) 533
 - performing full (RMT) 536

- selective (local device) 533
 - selective (RMT) 536
 - restoring
 - default Welcome message 459
 - JMM domain over-quota message 461
 - restricting administrator access 48
 - RMT
 - backup and restores 534
 - configuring for Solaris 534
 - default blocksize 528
 - roles
 - about the Quarantine administrator 289
 - about users and administrators 289
 - Administrator** 294
 - root, definition 300
 - routing messages to delegated domains 259
- S**
- saving large reports 502
 - Scan** button 248
 - searching for
 - Allowed Mailing List entries 433
 - Blocked Senders entries 430
 - delegated domains 265
 - distribution lists 315
 - folders 302
 - junk mail domains 451
 - Junk Mail Manager accounts 455
 - mail reports 504
 - messages in the queue 239
 - setting WebCal defaults 279
 - white list entries 427
 - securing WebMail session IDs 92
 - security reports
 - Anti-Spam Information** 511
 - Anti-Virus Reports** 509
 - Content Filtering Statistics** 512
 - Detailed Virus Scanning Information** 510
 - MailHurdle** 513
 - options 509
 - Virus Scanning Summary** 510
 - security screening, multi-tier 180
 - security, setting for administration 50
 - selecting delegated domains 265
 - selective backup, definition 524
 - selective restore from image 525
 - Send to Quarantine folder** filter action 337
 - sequential mode, tape library 523
 - session IDs, securing for WebMail 92
 - setting
 - Administration Suite timeout 68
 - calendar timeout 88
 - default authentication 129
 - default HTTP access 104
 - delegated domain user limits 268
 - domain user limits 262
 - folder quotas, Junk Mail accounts 454
 - outbound router on Exchange, KB articles 169
 - quota warning limit for IMAP 94
 - the domain disk quota 262
 - timeout for WebMail 92
 - WebCal defaults for delegated domains 274
 - WebCal main configuration for delegated domains 277
 - WebCal resources configuration for delegated domains 281
 - WebCal search configuration for delegated domains 279
 - WebCal subscribed calendars for delegated domains 285
 - setting up
 - group calendar 86

- NDMP service and clients 528
 - user autoprovisioning, Message Server 90
- setting up LDAP client queries
 - filters 61
 - Message Director 56
- Setup Wizard, using 36
- shared folders, creating 307
- signature based antivirus, about 397
- Signature Edition** antisпам scanning 417
- signatures, creating for delegated domains 270
- Silence Alarm** button 248
- SMTP configuration
 - all-in-one deployment 94
 - and MailHurdle 391
 - enabling 95
 - for RazorGates securing Exchange 130
 - for RazorGates with JMM securing Exchange 159
 - specifying reject lists 435
 - specifying relay lists 434
- SMTP routing 52
- SNMP configuration
 - hosts 254
 - traps 255
- Solaris, configuring RMT 534
- Sophos
 - antivirus scanning, modifying 399
 - scheduling updates 406
 - setting notifications 401
- sorting, messages in the queue 232
- spam, see *antisпам scanning* 336
- spares
 - deleting 245
- special characters prohibited in folder names 301
- specifying
 - blocked addresses 356
 - blocked attachments 361
 - blocked messages 359
 - Junk Mail Manager bulk create accounts 462
 - redirected attachments 364
- storage
 - adding/configuring arrays 246
 - deleting arrays 247
 - IDE, data available 243
 - viewing array data 246
 - viewing data 242
 - viewing disk data 244
 - viewing store data 248
- Store** properties 248
- Store** view, properties 248
- sub-folders
 - adding 307
 - addressing mail to 309
- support
 - getting a login ID 46, 519
 - getting a Mirapoint Support login ID 46
- synchronizing groups, Operations Console 471
- system
 - adding Junk Mail Manager users 454
 - deleting Junk Mail users 456
 - deleting users 297
 - deleting users, Junk Mail Manager 456
 - editing users 296
 - editing users, Junk Mail Manager 455
 - health alerts 250
 - health data tables 250
 - viewing health data 249

- System Information report 515
- system reports, **System Information** 515
- system, services configuration
 - SNMP 253
- T**
- tape drives
 - about 527
 - installing 531
 - supported 523
- tape library 527
- tape library stacker mode 523
- tape library, definition 527
- TCP connections
 - limiting 90
- tier, definition 177
- timeout
 - setting 68
 - setting for calendar 88
 - setting for WebMail 92
- Tivoli Storage Manager 520
- Top 50 Folders Nearest Quota** report 517
- Top Logins By User** report 505
- Top Mail Users** report 496
- top-level domain, definition 258
- traps configuration 255
- troubleshooting
 - adding folders 300
 - alias addresses 295
 - all-in-one 105
 - all-in-one deployment required information 64
 - antispam scanning, end-user options 418
 - configuration prerequisites 33
 - CPU usage 206
 - distribution lists, deleting 316
 - domain disk quota 262
 - domain sensitivity 260
 - domains 266
 - email address character limitations 291
 - filter list entries 353
 - filter list guidelines
 - getting a Mirapoint Support login ID 46
 - Group Calendar and LDAP Routing license 197
 - mailing list exemptions, where placed 433
 - pre-configuration checklist 31
 - wire taps, empty 351
 - word lists 355
- trusted IP addresses
 - Services > Administration**, setting 49
- trusted network specifiers, about 49
- types of viruses 398
- typographic conventions 25
- U**
- UCE
 - about junkmail scoring 336
 - definition 436
- updates
 - antispam scanning 422
 - antivirus scanning, RAPID 413
 - antivirus scanning, Sophos and F-Secure 406
 - checking for 46
- updating
 - antispam rule groups and MailHurdle known good mailers 423
 - antispam scanning, immediate 424
 - antispam/junk mail, automatically 424
 - antivirus scanning, immediate, RAPID 415

-
- antivirus scanning, immediate, Sophos 408
 - antivirus, automatically, RAPID 414
 - antivirus, automatically, Sophos 408
 - url add**
 - syntax for addressbook 89
 - syntax for group calendar 86
 - url delete** 87
 - URLs
 - for address book 89
 - for group calendar 86
 - User Audit Trail** report 251
 - user directory service, configuring for all-in-one 80
 - user login authentication 52
 - users
 - about 289
 - about the Quarantine Administrator 289
 - accessing folders for, in delegated domains 267
 - adding 292
 - bulk creating JMM accounts 462
 - changing folder access permissions 305
 - changing the default limit for a delegated domain 273
 - default folder location 289
 - default folder location, Junk Mail Manager 453
 - deleting 297
 - editing 296
 - finding 296
 - folder access permissions, meanings 302
 - Junk Mail Manager, creating bulk 461
 - number limits on RazorGates 291
 - provisioning accounts 298
 - reserved login names 292
 - setting limits in delegated domains 268
 - working with folders 303
 - using
 - wordlist filters
 - UTF encoded login names 291
 - V**
 - verifying the address book URL 102
 - Veritas NetBackup 520
 - viewing
 - array data 246
 - disk data 244
 - group data and alerts 472
 - mail traffic 207
 - message envelopes and headers 235
 - messages, what you can view 239
 - sorted messages, in the queue 233
 - storage data 242
 - store data 248
 - system activity 203
 - system health data 249
 - the queue summary 230
 - virus deleted messages, filtering out 375
 - Virus Scanning Summary** report 510
 - viruses, types of 398
 - W**
 - WebCal
 - main configuration for delegated domains 277
 - resources configuration for delegated domains 281
 - search configuration for delegated domains 279
 - setting defaults for in delegated domains 274
 - subscribed calendars for delegated



domains 285

WebMail

configuring 91

enabling 93

requiring cookies 92

securing session IDs 92

setting the timeout 92

WebMail Activity graph

definitions 211

description 210

Webmail Activity graph

statistics breakdown 210

weekly reports, description 478

Welcome messages, customizing for

Junk Mail domains 458

white list, about the Junkmail header

428

wire taps

creating 349

empty, troubleshooting 351

Wizard, using 36

wordlists, *see filter list*