MIRAPOINT®

Message Server Administrator's Guide

Releases 3.10 and 4.1
March 2009
Part Number 010-00757b

This manual supports Messaging Operating System (MOS) releases 3.10.2 and 4.1.2 and later MOS releases until replaced by a newer edition.

MIRAPOINT SOFTWARE, 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 SOFTWARE LICENSE AGREEMENT.

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 you ("User") and your use of any and all computer software, any printed or electronic documentation, 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 User by MIRAPOINT SOFTWARE, INC. or its affiliate, if any ("Mirapoint"). USER 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 the User to make are subject to this License.

3. Permitted Uses. This License allows User 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. User may make copies 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. User acknowledges and agrees that the Mirapoint Software is copyrighted and contains materials that are protected by copyright, trademark, trade secret and other laws and international treaty provisions relating to proprietary rights. User 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. User acknowledges and agrees 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. Third Party Programs. Mirapoint integrates third party software programs with the Mirapoint Software which are subject to their own license terms. These license terms can be viewed at http://www.mirapoint.com/licenses/thirdparty/eula.php. If User does not agree to abide by the applicable license terms for the integrated third party software programs, then you may not install the Mirapoint Software.

6. Disclaimer of Warranty on Mirapoint Software. User expressly acknowledges and agrees 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.

7. 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.

8. Export Control. As required by the laws of the United States and other countries, User represents and warrants that it: (a) understands that the Mirapoint Software and its components may be subject to export controls under the U.S. Commerce Department's Export Administration Regulations ("EAR"); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, North Korea, Sudan and Syria, subject to change as posted by the United States government); (c) will not export, re-export, or transfer the Mirapoint Software to any prohibited destination or persons or entities on the U.S. Bureau of Industry and Security Denied Parties List or Entity List, or the U.S. Office of Foreign Assets Control list of Specially Designated Nationals and Blocked Persons, or any similar lists maintained by other countries, without the necessary export license(s) or authorizations(s); (d) will not use or transfer the Mirapoint Software for use in connection with any nuclear, chemical or biological weapons, missile technology, or military end-uses where prohibited by an applicable arms embargo, unless authorized by the relevant government agency by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Mirapoint Software to eligible users, it will, to the extent required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department's Bureau of Industry and Security, which include the name and address (including country) of each transferee; and (f) understands that countries including the United States may restrict the import, use, or export of encryption products (which may include the Mirapoint Software and the components) and agrees that it shall be solely responsible for compliance with any such import, use, or export restrictions.

9. 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, re-export, 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. [2008.02.28 Part Number: 010-00664]

Contents

Preface 15
Typographic Conventions 15
Icon Conventions 16
About Mirapoint Documentation 16
About this Book 16
Getting Customer Support 17

Part 1
Configuration Tasks

1
All Deployments Start Here 21
Pre-Configuration Checklist 21
DNS Records Recommended for a Multi-Tier Deployment 22
About LDAP User Records 23
Accessing the Administration Suite 24
Accessing the Command Line Interface 26
Initial Setup Common to All Deployments 26
Accessing the Setup Wizard 26
Completing the Setup Wizard 27
Checking for Software Updates 32
Restricting Administrator Access 34
Adjusting Administration Security 35
Checking Basic Configurations 36
Completing Your Configuration 36

2
All-In-One Message Server Deployment 37
Before You Begin 38
Information Required for this Configuration 38
Configuring An All-In-One Message Server 39
Accessing the Administration Suite 40
Checking for Licenses 41
Setting the Administration Timeout 41
Configuring Anti-Virus Scanning 42
Configuring MailHurdle 46
Configuring Anti-Spam Scanning 47
Setting Up a User Directory Service 50
Command Line Configuration Tasks—All-In-One 58
Configuring WebMail 65
Configuring IMAP 66
Configuring SMTP 67
Enabling and Starting Services 68
Resetting the Administration Timeout 69
Verifying the All-In-One Setup 70
Refresh the Administration Suite 70
Create a Class Of Service—Internal Directory Only 70
Create User Accounts—Internal Directory Only 71
Send a Test Message 72
Receive a Test Message 73
Verify the Address Book Directory Service 73
Create a Calendar Event—Internal Directory Only 74
Optional Configuration Tasks 74
Adding Networks or Domains to the Reject List 74
Setting the HTTP Default Access 74
Configuring Safe Lists and Blocked Lists 75
Adding a Multi-Listener 75
Troubleshooting 76
LDAP Errors 76
Getting the Active Directory bindDN 76
Test Message Send Fails 77
Next Steps, All-In-One Deployment 78
3
Message Server Setup for Multi-Tier Deployments 79
Before You Begin 79
Information Required for this Configuration 80
Configuring A Message Server for Multi-Tier Deployment 81
Accessing the Administration Suite 82

Checking for Licenses 83
Setting the Administration Timeout 83
Configuring Anti-Spam Scanning 83
Setting Up a User Directory Service 85
Command Line Configuration Tasks—Multi-Tier Message Server 94
Configuring WebMail 102
Configuring IMAP 103
Configuring SMTP 104
Enabling and Starting Services 105
Resetting the Administration Timeout 106
Verifying the Message Server Setup for Multi-Tier 107
Refresh the Administration Suite 107
Create a Class Of Service—Internal Directory Only 107
Create a Delegated Domain 108
Create User Accounts—Internal Directory Only 108
Send a Test Message 109
Receive a Test Message 110
Verify the Address Book Directory Service 111
Create a Calendar Event—Internal Directory Only 111
Optional Configuration 111
Adding a Multi-Listener 111
Troubleshooting 112
LDAP Errors 112
Getting the Active Directory bindDN 112
Test Message Send Fails 113
Next Steps, Message Server Setup for Multi-Tier 114

4
Multi-Tier, Multi-Appliance Deployments 115

Before You Begin 116
Multi-Tier Terminology 116
Configuring a Multi-Tier Deployment 117
Getting Started 117
Security Screening (RazorGate Appliances) 119
Directory Services for User Data (Mirapoint Appliances) 126
Routing (RazorGate Appliances) 129
Message Store and Calendar (Mirapoint Appliances) 131
Reset the Administration Timeout 133

Part 2
Administration Tasks

5
Monitoring Tasks 137

Internal Distribution Lists for Monitoring 137

Viewing Performance At-a-Glance 138
- Pie-Chart Categories 139
- Performance Gauges 140
- Mail Graphs 142
- POP/IMAP Graphs 144
- WebMail Graphs 145
- Junk Mail Graphs 146
- Directory Graphs 147
- Misc Graphs 149
- External Graphs 150
- Disk Graphs 152
- Network Graphs 154
- CPU Graphs 156

Using the Message Queue 157
- About the Queue 157
- What to Look for in the Queue 158
- Viewing the Queue Summary 159
- Sorting Messages in the Queue 160
- Searching the Queue 165
- Temporarily Stopping Mail Service 167
- Deleting the Queue for a Domain 167

Viewing Hardware Status 167
- Monitoring Storage 167
- Monitoring Hardware Health 173

Viewing Alerts 174

Viewing User and/or Administrator Activity 175
- Using the User Audit Trail 175
- Using the Admin Audit Trail 175

Monitoring External Systems via SNMP 176
- Configuring SNMP Monitoring 176
- Adding SNMP Hosts 177
- Adding SNMP Traps 177

6
Provisioning Tasks 179

Managing Delegated Domains 179
- Adding Delegated Domains 181
- Creating an Administrator for a Delegated Domain 183
- Adding Delegated Domain Administrators to the Postmaster DL 184
- Finding a Delegated Domain 184
- Selecting a Domain 185
- Editing Delegated Domains 186
- Configuring Calendar Options for Domains 192
- Adding Directory Services to Delegated Domains 201
- Deleting Delegated Domains 202

Managing User Accounts 203
- About Users and Administrators 203
- User Account Requirements 204
- Adding Users 206
- Finding a User 208
- Editing Users 208
- Deleting Users 209
- Viewing Presence/Last Login Times 209
- Establishing User Account Policies 209
- Bulk Provisioning Users 209

Managing Folders 211
- Folder Naming Conventions 211
- Folder Access Control Lists 212
- Finding/Viewing Folders 213
- Adding Folders 214
- Changing Folder Access Control 216
- Changing a Folder Quota 216
- Renaming a Folder 216
- Adding a Sub-folder 217
- Creating a Shared Folder 217
- Deleting a Folder 218
- Sending Messages to User Sub-Folders 218

Managing Messages 218
- Sending Messages to Folders 218

Managing Distribution Lists 219
- Distribution List Naming Conventions 220
- Adding and Populating Distribution Lists 221
- Finding Distribution Lists 223
- Editing Distribution Lists 223
- Deleting Distribution Lists 223

7
Policy Tasks 225

Managing Classes of Service 225
Class of Service Features and Configuration Options 226
Adding and Populating a Class of Service 228
Assigning Classes of Service 229
Finding Classes of Service 230
Editing Classes of Service 230
Deleting Classes of Service 231
Managing Storage Policies 231
Creating Storage Policies 232
Editing Storage Policies 235
Deleting Storage Policies 236
Managing Content Policies (Domain Filters) 236
Creating Content Policies 237
Content Filtering Options 238
Understanding Quarantine Management 241
Creating a Message Filter 243
Reordering a List of Filters 249
Example Policy Enforcement Filters 250
Attaching a Signature to All Messages From a Domain 251
Using Wire Taps 252
Using Word List Filters 253

8
Security Tasks 273

Using Security Features 273
Network Security Layer 274
Inbound Message Handling Layer 277
Message Content Handling Layer 279
Outbound Message Handling Layer 281
Working with MailHurdle 282
Modifying MailHurdle 283
Adding and Deleting MailHurdle Allowed Hosts 285
Setting MailHurdle Advanced Options 286
Using Antivirus Scanning 288
About the Anti-Virus Engines 288
About Cleanable vs. Non-cleanable Viruses 289
How Antivirus Quarantine Works 290
Modifying Signature-based Anti-Virus 290
Setting Notifications for Sophos and F-Secure Anti-Virus 293
Scheduling Updates for Sophos and F-Secure Anti-Virus 296
Modifying Predictive-based (RAPID) Anti-Virus 299

Setting Notifications for RAPID Anti-Virus 300
Scheduling Updates for RAPID Anti-Virus 301
Using Antispam Scanning 303
Antispam Scanning Options 304
Modifying Antispam Scanning 306
Scheduling Updates for Antispam Scanning 308
Setting the Allowed Senders List 310
Setting the Blocked Senders List 312
Setting the Allowed Mailing Lists List 314
Updating Relay Domains (Relay List) 317
Updating Blocked Domains (Reject List) 318
Updating Your Real-time Blackhole List (RBL) 319
Example System-Wide Antispam Filters 320
Configuring Multi-Listeners 323
Configuring NIC Failover 324
Using Security Quarantine 325
Assigning the Quarantine Administrator Role 325

9
Using the Operations Console 327

Managing Operations Console Groups 328
Adding, Editing, and Deleting Groups 330
Administering Groups 330
Synchronizing Groups 331
Importing and Exporting Groups 332
Using the Operations Console Dashboard 332
Using Operations Console Alerts 333

10
Using Logs and Reports 335

Receiving Daily and Weekly Reports 335
Time Strings 335
Daily Reports 336
Weekly Reports 337
Logs/Reports Overview 349
Abbreviations Used in Logs 350
Mail Reports 351
Top (Mail Users) 351
Summary (Logins) 353
Local (Mail Users) 353
Remote (Mail Users) 354

Traffic Summary 354
Detailed (Mail Logs) 356
Search 358
Logins Reports 358
Top (Logins) 359
Traffic Rates (Logins) 359
Detailed (Logins) 360
Failed by User (Logins) 361
Failed by IP (Logins) 361
Security Reports 362
Anti-Virus Reports 362
Anti-Spam Reports 364
Content Filtering Reports 364
MailHurdle Reports 365
System Reports 366
Command Report 367
Folders Report 367
Folder Size & Quota Information 368
Largest 50 Folders 368
Top 50 Folders Nearest Quota 368

11
Business Continuity Tasks 369

Backup and Restore Concepts 369
Backup Schemes 370
What Is and What Is Not Backed Up 370
About Tape Drives and Tape Libraries 371
NDMP Backup Solutions 371
NDMP DMAs 372
Using NDMP for Backup and Restore 374
Administration Protocol Backup Solution 375
Alerts and Completion Status 375
Administration Protocol 376
Using the Administration Protocol for Backup 376
Using the Administration Protocol with a Local Storage Device 377
Using the Administration Protocol with Remote Magnetic Tape (RMT) 379
Using Remote Server Replication 381
Overview 382
System Requirements 383
Installation, Configuration, and Synchronization 384
Scheduling Regular Synchronizations 386
Daily Operations 387
Monitoring and Troubleshooting 388

Updating Systems....391
Aborting a Synchronization in Progress....391
Removing a Replica Configuration....391
Performing a Failover....392
Restoring a Master....393

Index....395

Preface

Welcome to the *Mirapoint Message Server 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 an 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. Important terms are also defined in the Mirapoint Glossary.

Typographic Conventions

Table 1 explains what different fonts in this book indicate.

Table 1 Typographic Conventions

Font	Indicates	Example
Roman	Ordinary text	The email server organizes mailboxes hierarchically.
Bold	Definitions; also screen elements such as menus, commands, and option labels	A **folder** is a container that stores email messages. Use the **Ldap Set** command to enable autoprovisioning.
Italic	Emphasis; book titles	Specify *at least two* DNS servers. See the *Mirapoint Administration Protocol Reference* for details.
Typewriter	Screen display text; command names	Enter your password:
Typewriter Bold	Text that you type exactly as shown	**Smtp Set Smtpauth**
Typewriter Italic	Placeholders for variables you provide	*sys_IP_address*

Icon Conventions

Table 2 explains what the different icons in this book indicate.

Table 2 Icons Used in This Book

Icon	Indicates
	Important information.
	Critical information.
	License required.
	Best practices.

About Mirapoint Documentation

Documentation for all Mirapoint products is available through the Mirapoint Technical Library (MTL) on the Mirapoint Support website:

http://support.mirapoint.com/secure/MTL/MTL

The MTL provides the Hardware and Software documentation for all supported Mirapoint releases and appliances, a Glossary, and the Support Knowledge Base. The Support site is accessible to all customers with a valid Support Contract. If you have a valid Support Contract but need a Support login ID, send an email to:

support-admin@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 Site 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, Message Server Setup for Multi-Tier Deployments: A Message Server directory, delivery, and storage functions behind two RazorGates performing security and routing.
- Chapter 4, Multi-Tier, Multi-Appliance Deployments: Multiple appliances networked to provide routing, security, storage, directory, and proxy services.

Administrative tasks are provided following the configuration tasks section of the book:

- Chapter 5, Monitoring Tasks: How to monitor system performance, check hardware status, and track down problems using distribution lists, graphs, and alerts.
- Chapter 6, Provisioning Tasks: How to provision and manage a Message Server's domains, user accounts and folders, queue, and distribution lists.
- Chapter 7, Policy Tasks: How to manage policies for your domains and users. Policies control the features and limits (quotas, etc.) available to users.
- Chapter 8, Security Tasks: How to use the MailHurdle, Anti-Virus and Anti-Spam options, including Junk Mail Manager.
- Chapter 9, Using the Operations Console: How to use the Mirapoint Operations Console (MOC) to create groups of machines, assign a master, and replicate the configuration of the master throughout the group.
- Chapter 10, Using Logs and Reports: How to use reports to monitor message traffic, security screening, and system operation.
- Chapter 11, Business Continuity Tasks: How to backup your Message Server data and how to use Remote Server Replication.

Getting Customer Support

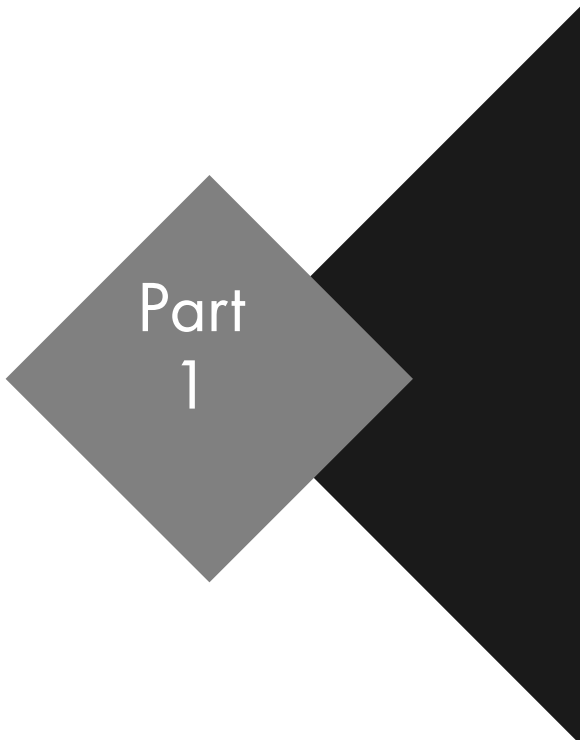
If you experience problems with your system, contact Mirapoint Technical Support by email or by telephone:

Email: support@mirapoint.com

Telephone: 1-877-MIRAPOINT (647-2764)

When contacting Mirapoint Technical Support, please be prepared with the following information about your system:

- MOS version (**Version** command in the CLI)
- Host ID (**License Hostid** command)
- Serial Number (**Model Get Serial** command)
- Hardware model (**Model Get Chassis** command, but double-check for the hardware model on the front panel of the system)



Configuration Tasks

1 All Deployments Start Here

This chapter describes the configuration steps that need to be performed for all Mirapoint appliances, Message Servers as well as RazorGates, 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.

In this document, the term **router** refers to an email router, rather than a network packet router. Email routers are also known 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 alerts you to some of these larger issues before you begin configuration. Refer to the *Mirapoint Site Planning Guide* for a complete discussion of these factors.

Table 3 Pre-Configuration Checklist

	Item
✔	**Domain Name System (DNS)**—Mirapoint appliances do not act as DNS servers; however, 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 and available to 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.

Table 3 Pre-Configuration Checklist (Continued)

	Item
✔	**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. **Important!** If an LDAP-related license expires, the LDAP settings revert to the default once an updated license is applied. 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.
✔	**Hardware installation and Basic System Setup**—All hardware must be rack-mounted, cabled, and powered on. As described on the Quick Start 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) ❖ New Administration password For details on your hardware, see your model's hardware manual.

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; they do not need to be repeated

DNS Records Recommended for a Multi-Tier Deployment

Both the *Message Server Administrator's Guide* and the *RazorGate Administrator's Guide* include configuration chapters for setting up a multi-tier deployment, with and without Junk Mail Manager (JMM).

The setups include specifications requiring special DNS records for a "round-robin" use of the RazorGates as the outbound router (OMR), local message router (LMR), SMTP proxy, and IMAP proxy. Also, DNS records are required for each

delegated domain. At a minimum, the multi-tier deployments require DNS records similar to this:

- To cause incoming mail to always go to the MailHurdle RazorGate (RG) first, create an MX record for each RG:

```
jmm.example.com     IN    A     192.168.0.1
example.com         IN    MX    100   jmm.example.com

mh.example.com      IN    A     192.168.0.2
example.com         IN    MX    10    mh.example.com
```

- For round-robin routing and scalability, create two "A" records for a "symbolic host," such as **`rgs.example.com`**, with the IP addresses of the two RGs; also, create four CNAME records for that host:

```
rgs.example.com     IN    A     192.168.0.1
rgs.example.com     IN    A     192.168.0.2

omr.example.com     IN    CNAME   rgs.example.com
lmr.example.com     IN    CNAME   rgs.example.com
smtp.example.com    IN    CNAME   rgs.example.com
mail.example.com    IN    CNAME   rgs.example.com
```

  The first two CNAMEs are set on the Mirapoint Message Server (MMS) as the SMTP outbound router (OMR), local message router (LMR), and WebMail OMR. The last two CNAMEs are used by end-users to connect to the system and send or retrieve email.

- For the pseudo-host (entered as the **JMM Host** on the MailHurdle RG), create an "A" record such as **`jmm-mms.example.com`** with the same IP address as the JMM server. To allow for the "fail-open," create dual MX records for the pseudo-host, one with high priority MX that points to the JMM server, and another with a low priority MX that points to the mail server:

```
jmm-mms.example.com  IN    A     192.168.0.1
jmm-mms.example.com  IN    MX    0     jmm.example.com
jmm-mms.example.com  IN    MX    10    mms.example.com
```

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

About LDAP User Records

If you have existing user data, we encourage you to convert it to LDAP format. This is what an LDAP user record looks like using the Mirapoint schema:

```
dn:mail=juser@example.com,miDomainname=mail.example.com,ou=domains,o=miratop
objectclass: mirapointUser
objectclass: mirapointMailUser
cn: Joe User
sn: User
uid: juser
userpassword: juser99
mail: juser@example.com
mailhost: mail.example.com
mailroutingaddress: juser@mail.example.com
miuuid: 33575dbe-93a7-10a9-39ec-0007d92f3b07
miquarantinehost: jmm.example.com
miCosDn: cn=defaultCOS,miDomainname=mail.example.com,ou=cos,o=miratop
```

The lines in red are only needed for Group Calendar. The final two lines are only needed for Junk Mail Manager. For more information about advanced LDAP features as well as the `Dir`, `Ldap`, and `Cos` commands, see the *Mirapoint Administration Protocol Reference*.

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 4 lists the various administration interfaces available. Table 5 lists the supported browsers.

Table 4 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

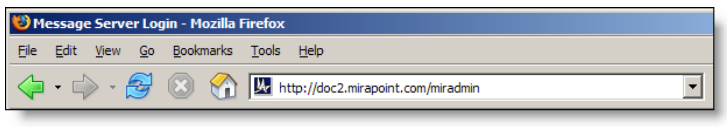
Table 5 Mirapoint Supported Browsers

Browser	Version
For Windows systems	❖ 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.

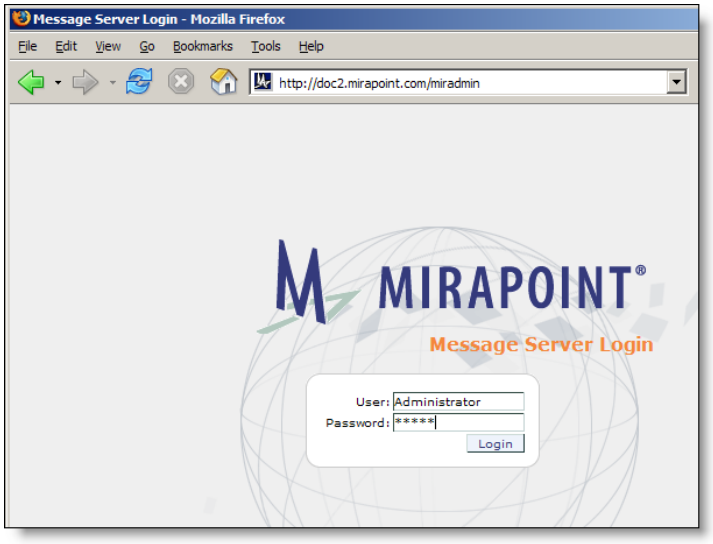
1. Go to this URL, where *miServer* is the IP address or name (if configured in your DNS) of your Mirapoint server.

   `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**.

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

This chapter describes how to perform the basic configuration of your Mirapoint appliance through the Setup Wizard. Some procedures require the command line interface (CLI); most procedures in this book describe how to set options through the regular Administration Suite pages.

Accessing the Command Line Interface

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

1. Open a command line window; for example, **Start > Run**. Use the telnet (terminal emulation) program to connect to the Mirapoint appliance by entering the IP address you assigned to it during the hardware setup:

   `telnet` *`hostname.domain.com`*

2. Enter the login name **Administrator.**

3. Enter the temporary administrator password you specified for the appliance during the hardware setup:

```
OK mail.example.com admind 3.10 server ready
User: Administrator
Password: password
OK User logged in
mail.example.com>
```

Telnet uses port 23 by default; you can enter another port, for example 10144, if needed, after typing the hostname.

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

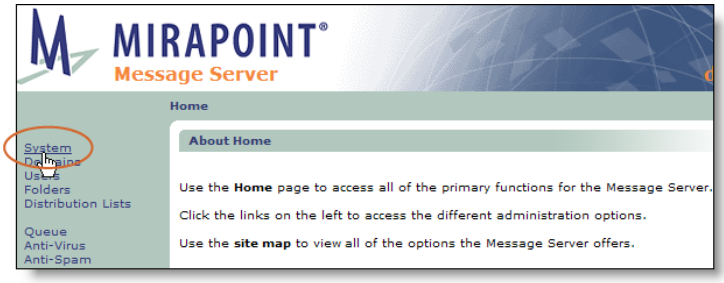
Accessing the Setup Wizard

The Setup Wizard start page is displayed automatically the first time you log into the Administration Suite.

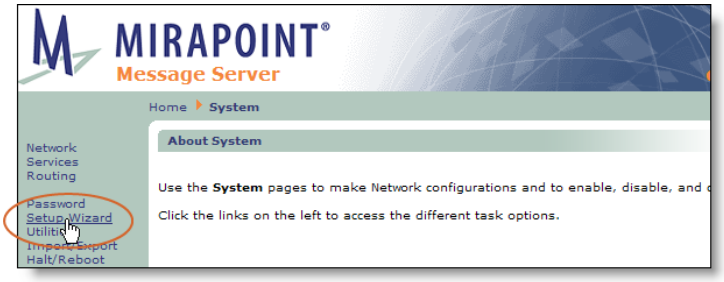
If you get the **First Use** screen, all of your licenses have not been applied. Log in as administrator and go to **System > Utilities > License** and click **Install Licenses.** Once all of the licenses you have purchased are installed, logout, and log back in to the appropriate URL given in Table 4, Administration Suite Interface Options, on page 24.

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.

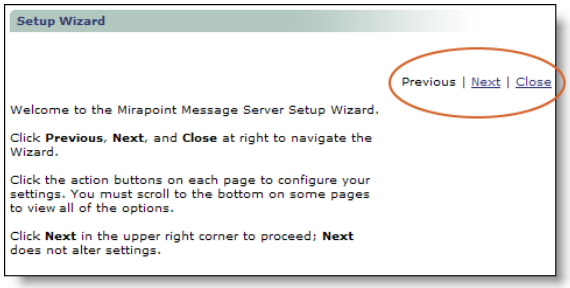


Completing the Setup Wizard

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 **Change Password** for the new password to take effect.

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



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

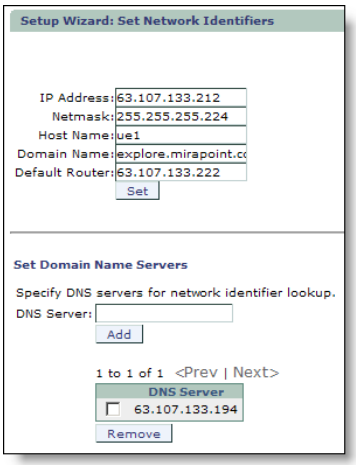
To change your password:

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 are 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 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 on page 325.

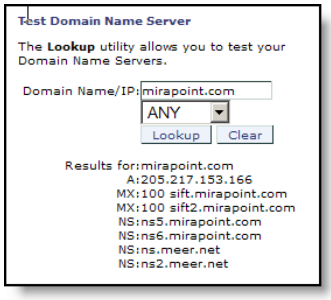
4. **Set Network Identifiers** page. The network settings and DNS server configured during installation are shown on the **Set Network Identifiers** page. Verify that the network settings are correct and configure at least one additional DNS server as a backup. If you are unsure what the appropriate network settings for your appliance are, consult your network administrator.



To add a DNS server:

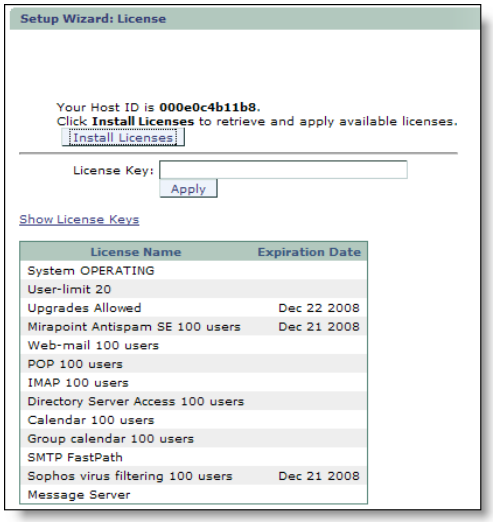
a. Enter the DNS server's IP address in the **DNS Server** option.
b. Click the **Add** button.
c. When you are done, test your DNS servers or click **Next** to continue.

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



a. Enter the domain name or IP address of an Internet server (e.g., **`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 are 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.



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

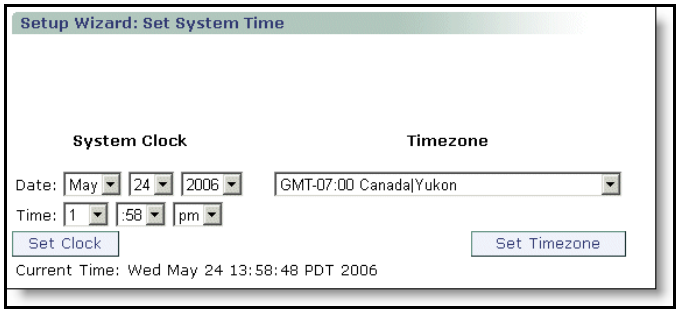
If your licenses cannot be retrieved, apply them one at a time:

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 are 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, email 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 are 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, Mirapoint recommends 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.

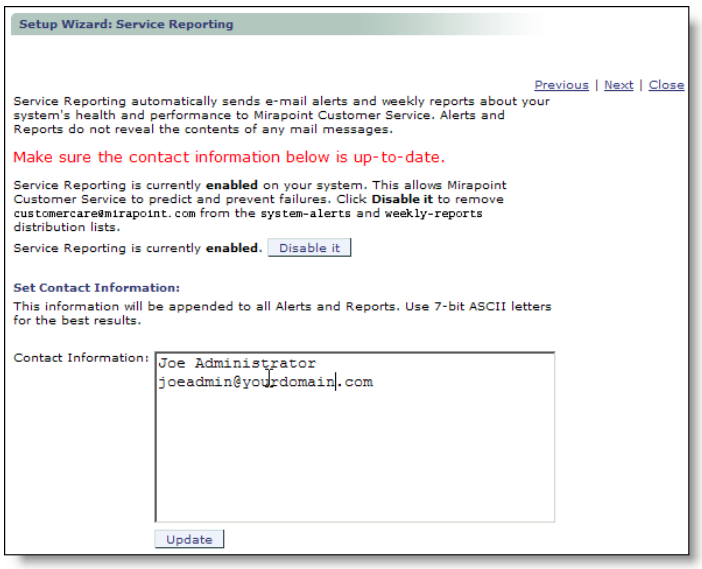
8. **Set Relay List** page. You do not need to configure any relays at this time. Click **Next** to continue.
9. **Set Mail Domains** page. You do not need to set mail domains at this time. Click **Next** to continue.
10. **Routing Via Local Router** page. You do not need to configure routing options at this time. Routing options are set as part of the deployment-specific configuration procedures. Click **Next** to continue.

If you have installed the Mail 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. You do not need to modify the default security (antispam and antivirus) options. Click **Next** to continue.

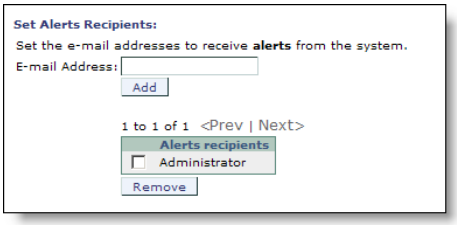
If no antispam or antivirus licenses have been installed, this page displays empty.

12. **Service Reporting** page. Configure service reporting to send alerts and weekly reports to selected administrators and Mirapoint Customer Service.

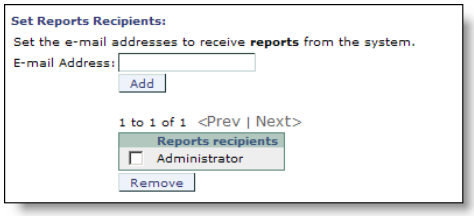


To set your service reporting options:

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

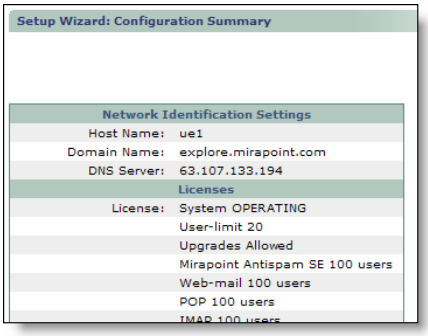


d. Enter the email address of each person who should receive Mirapoint system reports in the **Reports Recipients Email Address** option and click the **Add** button. (The Administrator is included in the report list by default.)

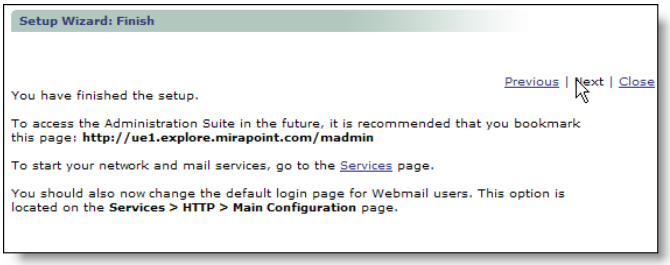


e. When you are done setting your service reporting options, click **Next** to continue.

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 are 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 is 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 on page 32
- Restricting Administrator Access on page 34
- Adjusting Administration Security on page 35

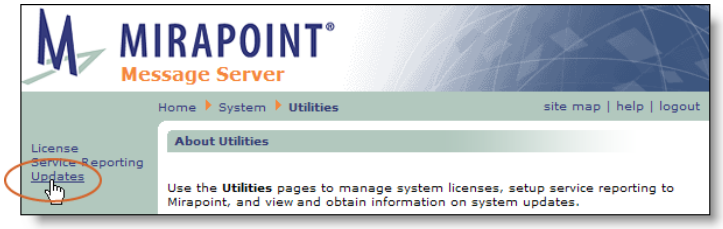
Checking for Software Updates

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**; you will need a login ID to do this. If

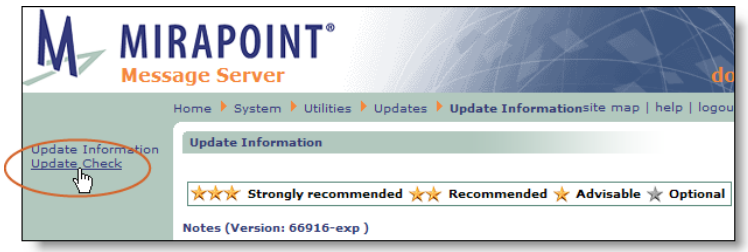
you do not have a Mirapoint Support login ID, send an email to support-admin@mirapoint.com requesting one.

To check for updates using the Administration Suite:

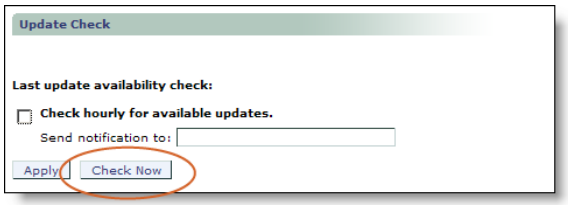
1. Go to **Home > System > Utilities**.
2. Click **Updates** to open the **Update Information** page.



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

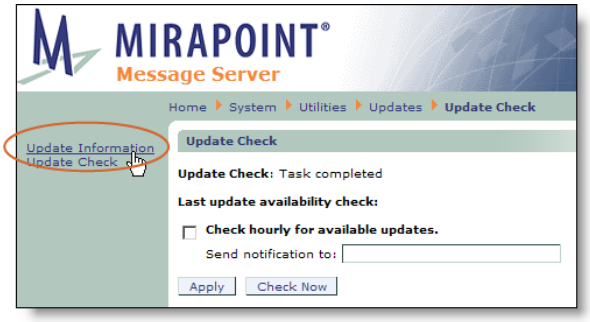


4. Click the **Check Now** button on the **Update Check** page to check for available updates. When the check is complete, the page displays the last machine update date. (**Update Check: Task Completed** is displayed if there are no updates.)



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.

5. 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.

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

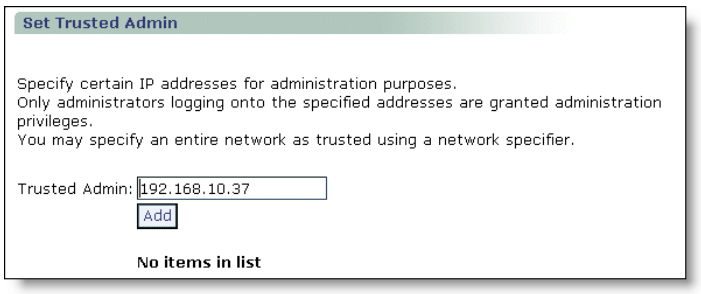
When you install an update, the system must reboot and all services are interrupted. Once the system has restarted, you will need to reconnect to the Administration Suite to proceed with the setup process.

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.



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 About Trusted Network Specifiers on page 35). 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).

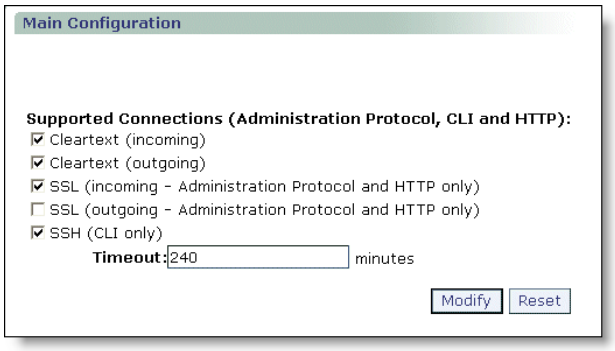
Only users whose IP addresses match one of the trusted IP addresses or network specifiers are allowed administration privileges. Users whose addresses do not match are denied access.

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.



Checking Basic Configurations

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

- Completing the Setup Wizard on page 27
- Checking for Software Updates on page 32
- Restricting Administrator Access on page 34
- Adjusting Administration Security on page 35

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, Message Server Setup for Multi-Tier Deployments
- Chapter 4, Multi-Tier, Multi-Appliance Deployments

2 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 Site Planning Guide*.

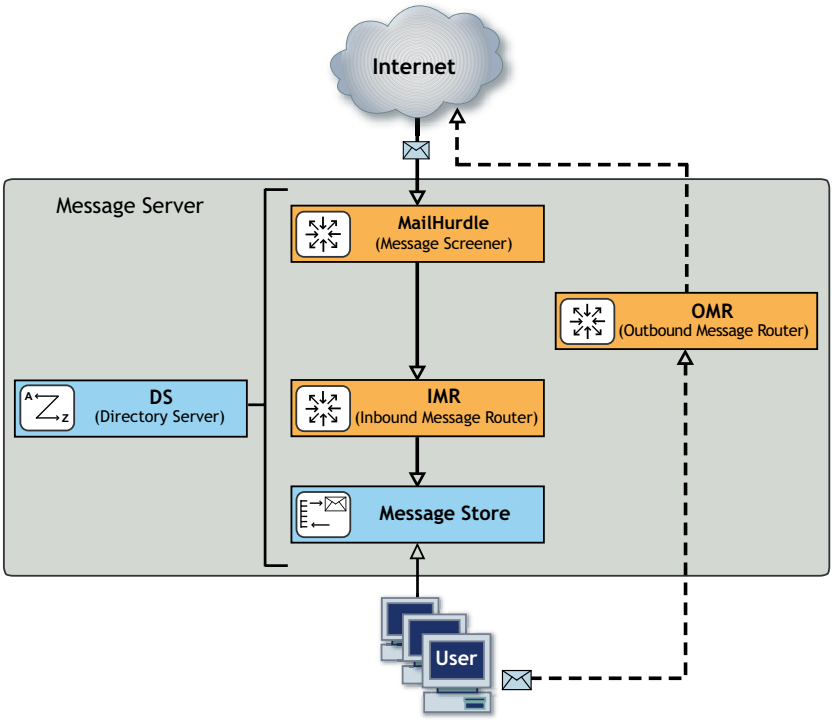


Figure 1 All-in-One Deployment Example

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 with needed DNS records ("A," "MX," "PTR," and "CNAME")
  - Lightweight Directory Access Protocol (LDAP) set up
  - Licenses obtained (licenses are implementation specific)
  - Backup requirements defined
  - Secure Sockets Layer (SSL) certificates obtained
  - Hardware installation (connected to the Internet)
  - 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 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. Adding senders and recipients to these safelists 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 (Real-time Blackhole List) servers.
- 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 (for example, mail.example.com) rather than using the primary (default) domain. This provides you with the flexibility of adding additional namespaces later. When you have delegated domains, use the primary domain only for global administration. All mail handling is best done through delegated domains.

Delegated domains are amongst the last things to be configured.

- **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 27.

Licenses are implementation-specific

  - Required licenses:
    - User Limit
    - Mail Routing
    - WebMail
    - Corporate Edition
    - POP
    - IMAP
    - Message Server
    - Group Calendar
    - (SSL) Weak Encryption and/or Strong Encryption
    - Directory Server
    - Delegated Domain Administration
  - Optional licenses (checking your licenses is described below on page 41):
    - Sophos (signature-based) virus filtering
    - F-Secure (signature-based) virus filtering
    - RAPID (predictive-based) virus filtering
    - Principal Edition Antispam or Signature Edition Rapid Antispam

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

Configuring An All-In-One Message Server

In this deployment, a Message Server performs security functions, plus message retrieval, storage and delivery, and outbound message handling. This configuration involves the following tasks:

- Accessing the Administration Suite
- Checking for Licenses
- Setting the Administration Timeout

- Configuring Anti-Virus Scanning
- Configuring MailHurdle
- Configuring Anti-Spam Scanning
- Setting Up a User Directory Service
- Command Line Configuration Tasks—All-In-One
- Configuring WebMail
- Configuring IMAP
- Configuring SMTP
- Enabling and Starting Services
- Resetting the Administration Timeout

To test your all-in-one setup, perform these tasks:

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

Four 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.
- Adding a Multi-Listener—Allows your system to listen for SMTP connections on multiple ports and interfaces at once.

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 27 before continuing.

If you are comfortable using the CLI, Mirapoint recommends using both interfaces as some tasks are more easily accomplished with the CLI and a few tasks can only be done using the CLI. However, if you do so, you will need to occasionally log out and then back in to the Administration Suite to see changes. For information on accessing the CLI, see Accessing the Command Line Interface on page 26.

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. Click **Install Licenses** if needed.

In the CLI, type:

```
hostname.com> license list
OK Completed

hostname.com> license fetch
OK Completed
```

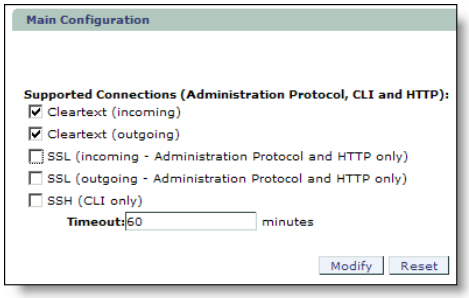
The MailHurdle license does not display; it is part of the Anti-Spam license. The internal LDAP directory requires the Mail Routing license.

Setting the Administration Timeout

You will 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.



In the CLI, type:

```
hostname.com> admin set timeout 60
OK Completed
```

You will want to change it back to 10 minutes once you are done.

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 47.

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. 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.

Mirapoint recommends leaving disabled (the default) notifications for F-Secure and Sophos caught virus-infected messages; but enabling notifications for RAPID caught virus-infected messages because those messages may not actually contain viruses.

Configuring F-Secure or Sophos Anti-Virus

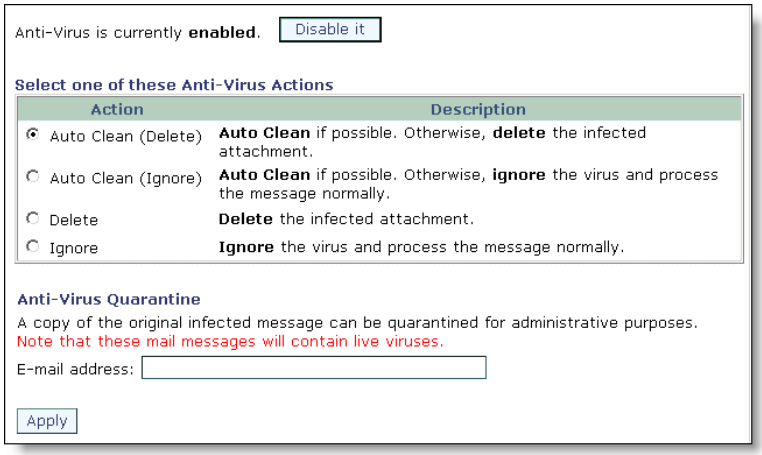
To configure Sophos or F-Secure Anti-Virus, follow these steps. You will need to repeat the procedure if you have both antivirus scanners.

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 email 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.

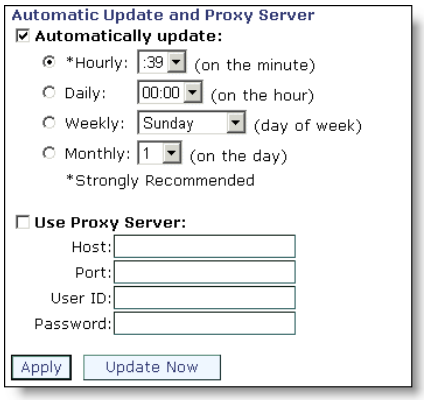


If you select the **Auto Clean** (**Ignore**) or **Ignore** options, infected messages will be delivered to your users. If you make changes, click **Apply** to save your changes.

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.



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 299 in the Administration Tasks part of this book.

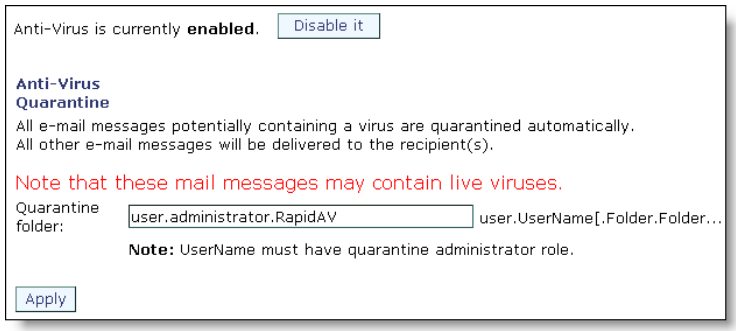
Before you can configure **RAPID Anti-Virus** scanning, you will need to:

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 203.
3. Create a folder for this user called *RapidAv* (or a name of your choosing). You configure RAPID Anti-Virus to send quarantined messages to this folder. For more information about creating folders, see Adding Folders on page 214

The default quarantine folder is a sub-folder of the *administrator* account: **user.administrator.RapidAv**.

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.



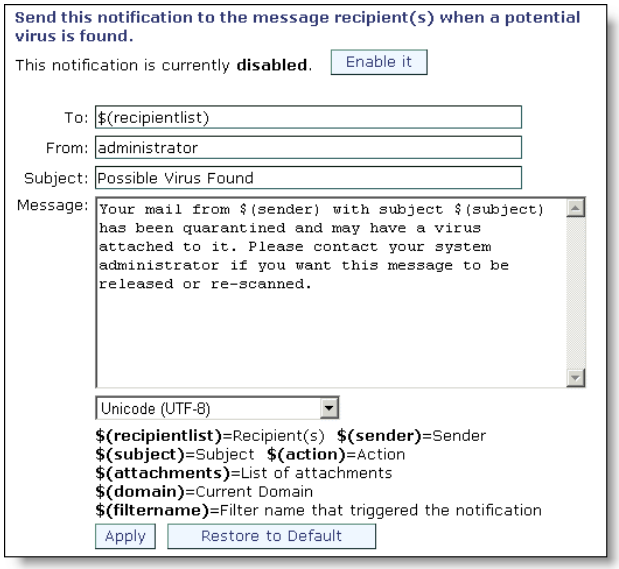
2. Accept the default **Quarantine folder** address, a subfolder of the Administrator account. Later, you might use any valid user.*username.subfolder* email address for an account with the Quarantine Administrator role. For details, see How Antivirus Quarantine Works on page 290, and Using Security Quarantine on page 325 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.

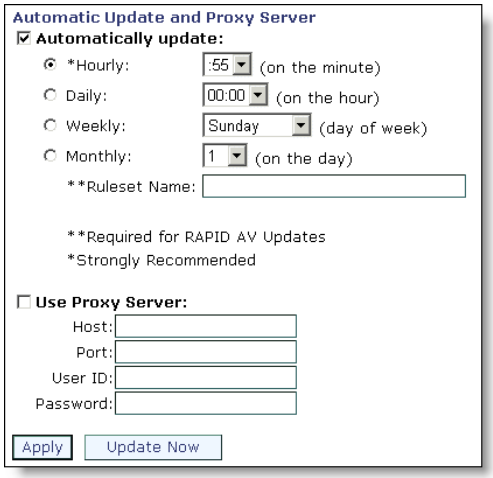
In the **To** option, add the appropriate administrator's email address (or just **Administrator** to use the default). Notifications are sent to the specified RAPID Anti-Virus quarantine administrator(s) when messages are quarantined. Use commas (,) as separators to enter multiple email addresses.

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



4. Go to **Home > Anti-Virus > RAPID > Updates**. Select the **Automatically update** option 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.



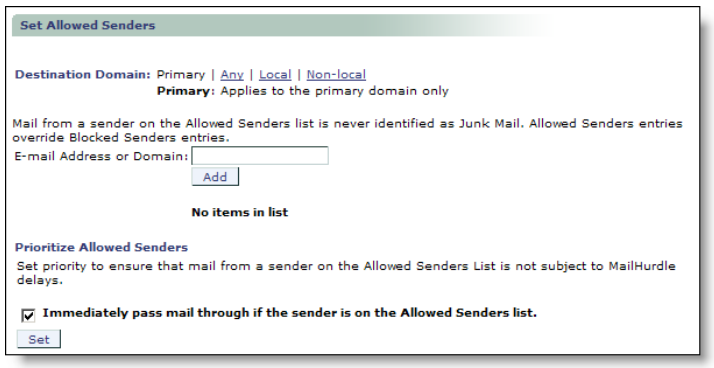
Configuring MailHurdle

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.

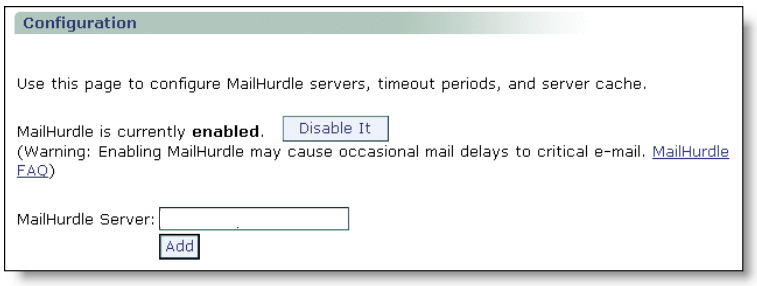


2. Go to **Anti-Spam > Allowed Mailing Lists**. Leave **Destination Domain** at **Primary** (default). Add recipients whose email should *not* be subject to MailHurdle screening; generally, this is used to protect distribution lists (also known as mailing lists). For example, you might want to add your support address to 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 **Enable It**; 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 have 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 282. Continue configuring Anti-Spam scanning with the following procedures.

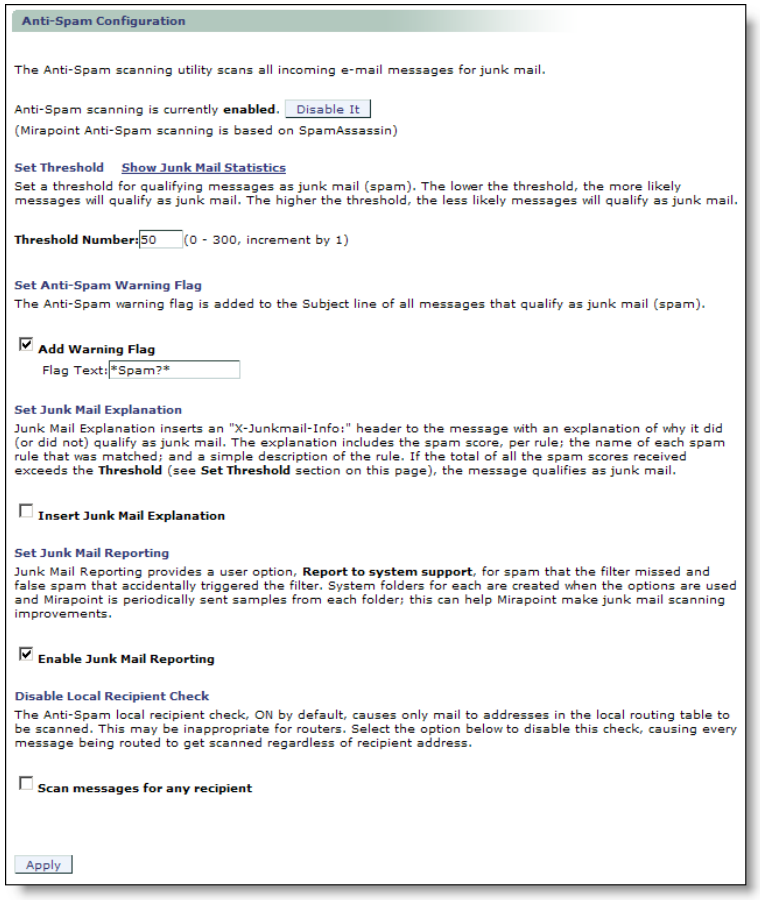
Configuring Anti-Spam Scanning

Anti-Spam scanning is a licensed feature. There are two antispam licenses, **Principal Edition Antispam** and **Signature Edition Rapid Antispam**, the configuration options for both are identical and the update options differ only slightly. For details , see Principal Edition vs. Signature Edition on page 304.

If you add an additional antispam scanner, be sure to go the the **Anti-Spam Updates** page for that scanner and click **Update Now** to get the most recent files for that scanner.

To configure Anti-Spam scanning:

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



Recommendations are:

- **Threshold Number**—Adjusts antispam scoring. Accept; keep threshold **50** (default). Lower values incur more false positives; higher values miss spam.
- **Add Warning Flag**—Adds a text string to the message subject indicating that the message is spam. Accept. The default string is ***Spam?***.
- **Insert Junk Mail Explanation**—Adds a header with antispam scoring information. Leave de-selected (default); in general, users do not need this feature.

This option only displays for **Principal Edition Antispam**.

- **Enable Junk Mail Reporting**—Adds an option allowing users to report spam. Leave selected (default); this helps Mirapoint tune the antispam scanning rules.
- **Scan messages for any recipient**—Disables the local recipient check. Leave de-selected (default); this option is not needed on an all-in-one deployment.

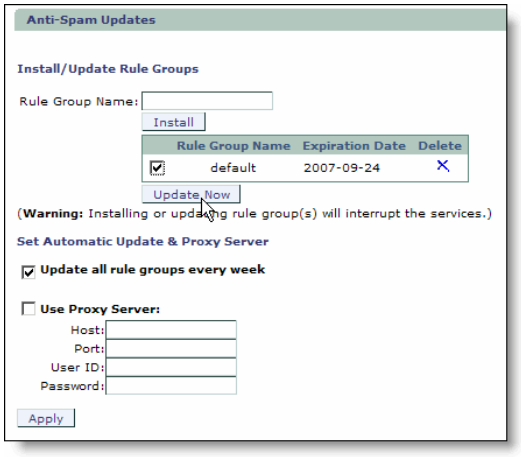
When you are done, click **Apply** to save your changes.

2. Go to **Anti-Spam > Updates**. Select the rulegroup for your anti-spam solution:

- **default** (Principal Edition Antispam)
- **rpdengine** (Signature Edition Rapid Antispam) or **rpdasia** (Signature Edition Rapid Antispam in Asia)

Click **Update Now**. If you do not see the appropriate rulegroup, enter the **Rule Group Name** and click **Install**.

Updating or installing rulegroups can take a few minutes.



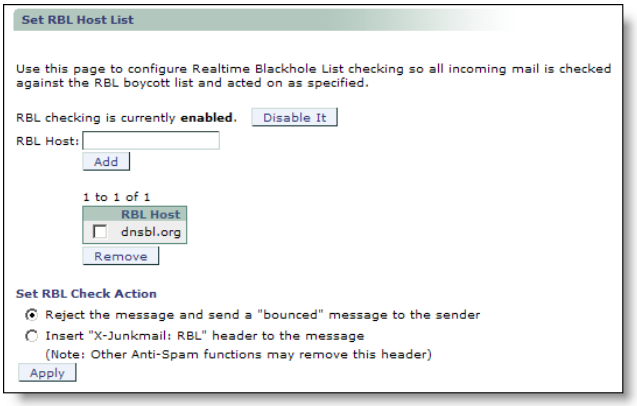
3. Select **Update all rule groups every week**. If your site has a proxy server, select **Use Proxy Server** and designate a **Host** and **Port**.

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

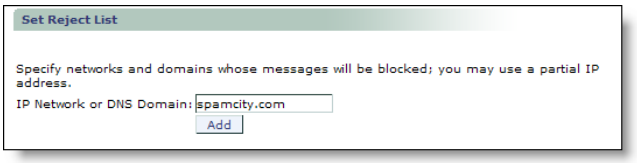
4. Do not modify the **Anti-Spam > Relay List** page unless you have an existing front-end, like Postini or Barracuda. You do not normally need to configure relays for an all-in-one deployment. If you are integrating with an existing system, enter the IP addresses of each front-end server.

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.

   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.



Additionally antispam methods available only through the CLI are detailed later in this chapter in Command Line Configuration Tasks—All-In-One on page 58.

Setting Up a User Directory Service

A user directory service manages user routing information and authentication. To set up an internal LDAP directory service or an Active Directory service, you must have the Mail Routing license.

This section describes two options for setting up a directory service when you are using a Message Server in an all-in-one configuration:

- Message Server's internal LDAP Directory; to do this, follow the instructions in Setting Up the Internal LDAP Directory," next.
- Microsoft Active Directory; to do this, follow the instructions in Setting Up Active Directory on page 55.

You need to use the command-line interface (CLI) to set up the directory and configure the Message Server to use it. Additionally, Mirapoint recommends that you use the CLI to set TCP (transmission control protocol), address book, and calendar options before returning to the Administration Suite to complete the configuration process. These procedures are provided in Command Line Configuration Tasks—All-In-One, following this section.

To access the CLI, connect to your Message Server using telnet in a command window, and log in as the Administrator:

```
Start > Run: telnet hostname.domain.com
OK hostname.domain.com admind 3.10 server ready
User: Administrator
```

```
Password: password
OK User logged in
```

CLI commands are case-insensitive. To make the examples easier to read, they are shown in mixed case.

About LDAP GUI

Part of the internal LDAP directory setup, described next, is enabling LDAP GUI, which allows certain pages of the Administration Suite to write data to, and retrieve data from, your LDAP database. Enabling these provisioning pages allows you to:

- Create domains and users in the administration protocol AND on a Directory Server in LDAP, or Internal LDAP—but not locally.
- Design and apply Classes of Service to users or domains.
- Authenticate logins with Class of Service.

In order for you to be able to use these provisioning pages, you must first set up LDAP, including importing an LDIF file, and also set up your LDAP client with queries, enable the services, and configure class of service (COS) (described next). Once you have enabled LDAP GUI, the **Domains** pages in the Administration Suite change to display this flag in the bottom left, **LDAP Domain**, indicating that it was created in your LDAP database.

Additionally, the **Class of Service** page displays at the top-level with this flag in the bottom left, **LDAP Enabled**, indicating that actions you take on that page are instantiated in your LDAP database.

You cannot use the Setup Wizard to enable the provisioning. If you have an existing Directory Server set up with LDAP, this procedure does NOT work; you may need to contact Mirapoint Support for migration.

Enabling LDAP GUI disables the **Use LDAP Password** option on the LDAP enabled **Domains > Users** page; passwords will be stored in LDAP.

Setting Up the Internal LDAP Directory

The Message Server includes a built-in LDAP directory server you can use for user authentication. This procedure sets up an LDAP database from scratch; you can use this procedure to set up an LDAP database locally (internal to the Message Server) or on a Mirapoint Directory Server. If you have never set up an LDAP database before, it would be wise to read through the procedure before beginning.

There are a few ways that you can use this procedure:

- In a web browser, go to http://www.mirapoint.com/support/allinone.html. Copy and paste the data from this file, including the LDIF, plugging in your own passwords. Everything that you need to do is included in the allinone.html file.
- You can copy the allinone.html file to a text editor (e.g., Notepad), change the passwords, and then enter the data (a chunk at a time works best) into your telnet window.

- You can use the following pages and manually enter the commands, one at a time.

If you have any problems accessing the HTML file, the data that needs to be entered is given in the steps below; you can use these steps to better understand what you are doing. Do not repeat the procedure. 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 manually set up the internal LDAP directory with a directory database named **miratop**.

Using the allinone.html file mentioned above is, generally, much simpler.

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 Adddbsuffix` command to add a new DIT (directory information tree) with the distinguished name (DN) `o=miratop` to the directory named miratop:

   ```
   hostname.com> Dir Adddbsuffix Miratop O=miratop
   OK Completed
   ```

3. Enter the `Dir Setdboption` command to set the directory administrator's `RootDN` (distinguished name):

   ```
   hostname.com> Dir Setdboption Miratop Rootdn Uid=administrator,o=miratop
   OK Completed
   ```

4. Enter the `Dir Setdboption` 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 Setdboption 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 "" miloginid 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 web 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
```

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
```

Configuring 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=$(login))(miloginid=$(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 Setting Up the Internal LDAP Directory on page 51 in place of ***adminpassword***:

```
hostname.com>Ldap Addaccess O=miratop Uid=administrator,o=miratop Pass
Password: adminpassword
OK Completed
```

Enabling LDAP GUI and COS

Use the following procedure to enable the LDAP GUI (described in About LDAP GUI on page 51) and Class of Service (COS) function.

1. Enter the `Conf Enable` command to enable all LDAP configuration options, including the LDAP auto-provisioning pages:

```
hostname.com>Conf Enable Ldapall
OK Completed
```

2. 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 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
```

To complete the setup of the internal directory service, keep your CLI window open and skip to Command Line Configuration Tasks—All-In-One on page 58.

Setting Up Active Directory

You can use Microsoft's Active Directory service for user authentication instead of using the Message Server's internal LDAP directory server.

To configure the Message Server to interoperate with Active Directory, you will need:

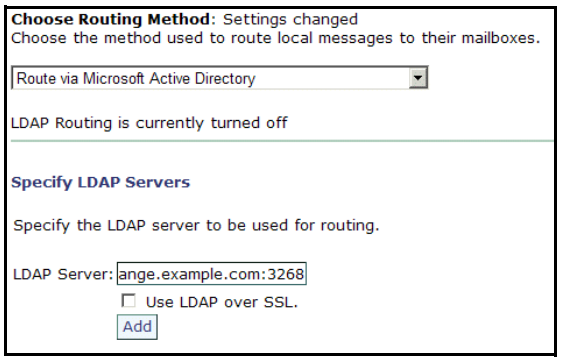
- The IP address or domain name of your Microsoft Exchange server, for example, 192.168.0.1 or adhostname.yourdomain.com
- The Administrator password for your Exchange server
- The Active Directory base DN (distinguished name), for example, DC=*adhostname*, DC=*yourdomain*, DC=com
- The Active Directory bind DN the Message Server will use for authentication when accessing the directory, for example CN=Administrator, CN=Users, DC=*adhostname*, DC=*yourdomain*, DC=com
- The password for the user identified in the bind DN, for example, the password for Administrator.
- Mirapoint recommends creating a new user for use by the Mirapoint server; you will need the DN and password for that user.

Instructions for getting your Active Directory DN information are provided in Getting the Active Directory bindDN on page 76.

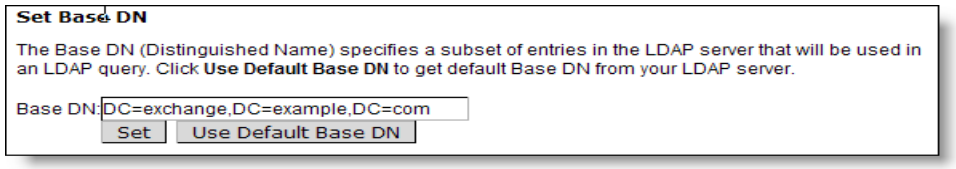
Most of the Active Directory setup can be done using the Administration Suite; follow these steps.

1. Go to **Home > System > Routing**. On the **Choose Routing Method** page, select **Route via Microsoft Active Directory**. For the **LDAP Server** option, type the

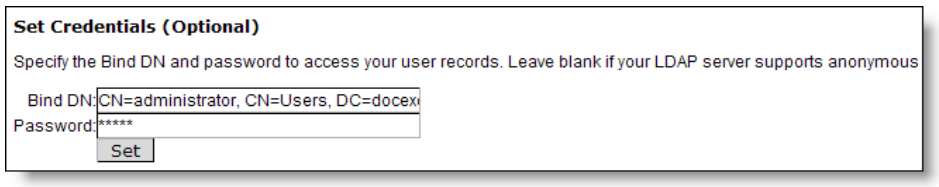
name of at least one Active Directory Exchange server plus the port (usually 3268). For example, `ldap://exchange.example.com:3268`.



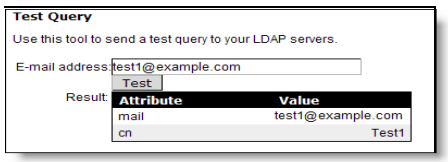
2. Go to **System > Routing > User Queries** page, under the heading **Set Base DN**, click **Use Default BaseDN**. All the user query filter and attribute names appear automatically.



3. In the **Set Credentials** area, enter the bindDN of the Active Directory administrator; this is not optional. Click **Set**.



4. Under the **Test Query** heading, type a user email address such as `test1@exchange.example.com` or some valid address in the Active Directory database. The **mail**, **mailhost**, and **cn** (full name) values should appear for that email address.



5. Go to **System > Routing > Mail Group Queries** page, under the heading **Set Mail Group Base DN**, click **Use Default BaseDN**. All the mailgroup query filter and attribute names appear automatically.
6. Skip the **Set Credentials** area, you set this in step 3.
7. Under the **Test Query** heading, type a mailgroup email address such as `TechPubs@exchange.example.com` or some valid group address in the Active

Directory database. The configured values for that group should appear for that email address.

8. Go to the **System > Routing > Mail Host Mapping** page. Enter all Active Directory domain names; for each, enter the Message Server hostname as the **Mail Host**. Click **Add** for each entry.
9. Ensure that the POP and IMAP service modes are set to normal by going to **System > Services > IMAP** and **System > Services > POP** pages and verifying that the **Mode: Normal** radio button is selected.
10. Enable HTTP routing via LDAP by going to **System > Services > HTTP > Mode** and selecting **LDAP Redirect**.
11. Set the Group Calendar user search mode to local by going to **Domains > Calendar > Search Configuration** and selecting **Local only**.

Configuring Outbound Routing on the Exchange Server

You must set your Message Server as the outbound router Smart Host on the Exchange server; follow these steps. For more information on configuring Exchange 2000/2003 to use Smart Host IP Addresses, see the knowledge base on the Microsoft Help and Support website.

1. Log in to your Exchange server as administrator and go to **Start > 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 Message Server and click **OK**.
6. The **Default SMTP Server Properties** dialog box re-opens, click **OK** again.

This completes the needed configurations on the Exchange server for this deployment.

To complete the setup of the Exchange directory service, you must use the CLI and follow the procedural steps in Command Line Configuration Tasks—All-In-One on page 58. To access the CLI, connect to your Message Server using telnet in a command window, and log in as the Administrator:

```
Start > Run: telnet hostname.domain.com
OK hostname.domain.com admind 3.10 server ready
User: Administrator
Password: password
OK User logged in
```

Command Line Configuration Tasks—All-In-One

While you are logged into the CLI, you may also want to perform the following configuration tasks:

- Setting the Default Authentication
- Setting Up Autoprovisioning of Users
- Configuring Banner Delay
- Configuring Second Scan for Anti-Spam
- Limiting TCP Connections
- Adding the Address Book URL—Internal Directory
- Adding the Address Book URL—Active Directory
- Setting up Group Calendar—Internal Directory

CLI commands are case-insensitive. To make the examples easier to read, they are shown in mixed case.

Setting the Default Authentication

You must use the CLI to set the authentication; do this for an Internal Directory setup or an Active Directory setup. Telnet to your mail server and enter this command:

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

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**.

Enable LDAP autoprovisioning with the `Ldap Set` command:

```
hostname.com> Ldap Set Autoprovision On
```

More information on autoprovisioning, including how to transfer existing records, is provided in Bulk Provisioning Users on page 209.

Configuring Banner Delay

You can configure your system to delay greeting acknowledgement during the SMTP chat session. Senders who violate the RFC by sending data before the greeting acknowledgement can be rejected.

Mirapoint recommends turning banner delay **On** if you are not using MailHurdle or you are using MailHurdle in SuspectList mode (see `Help About Mtaverify` in the CLI help for details).

To do this, enter these CLI `Smtp` commands:

Enable banner delay (default is **Off**).

```
hostname.com> Smtp Set Bannerdelay On
```

Sets banner delay time in seconds (default is 5). Setting delay to **0** sets the banner delay time to the default value, 5 seconds.

```
hostname.com> Smtp Set Bannerdelaytime 5
```

Use `Smtp Get Bannerdelay` and `Smtp Get Bannerdelaytime` to retrieve the configured delay state and time.

Banner delay is not subject to sender whitelisting. However, messages originating locally from the receiving server and senders on the relay list are exempted from banner delay.

These commands apply system wide and are not domain sensitive.

Configuring Second Scan for Anti-Spam

You can now run both Signature Edition (RAPID Anti-Spam) and Principal Edition antispam scans on the same server. Administrator's can choose to run both scans on all messages or to run the second scan only for messages classified as "bulk" by RAPID.

- `Multienginebulkonly`: Setting this to **Off** (default) configures both licensed scanners to run for all messages. The higher returned score is used to determine the UCE score in the header X-Junkmail-Status and X-Junkmail:UCE headers.
- `Multienginebulkonly`: Setting this to **On** configures second scan to run only for messages classified as bulk by Signature Edition (UCE scores between 50 and 60). For these bulk classified messages, the result of the second scan overrides the bulk classification.

If you run this command with only one Antispam scanner licensed, it has no effect until the second scanner is licensed. If two scanners are licensed but this option is **Off**, then the larger spam score wins, which can increase false positives. Running both scanners is resource intensive, but much less so with this option **On**.

Mirapoint recommends setting `Multienginebulkonly` to **On** if you consider that your two-engine spam scanning is taking too long.

To do this, enter the following CLI `Uce` command:

```
hostname.com> Uce Setoption Multienginebulkonly (Domain=local) On
```

Use `Uce Getoption Multienginebulkonly (Domain=local)` to retrieve the mode setting.

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 these CLI `Netif` commands that manage network interfaces:

- `LimitTcpConnectCount`: Setting this to **On** enables checking the count of TCP connections. The default is **Off**. When enabled, transmitted packets and incoming connections are dropped from any hosts exceeding the `MaxTcpConnectCount` limit (default is 50).
- `LimitTcpConnectRate`: Setting this to **On** enables checking the rate of TCP connections. The default is **Off**. When enabled, transmitted packets and incoming connections are dropped if the **MaxTcpConnectRate** limit (default is 400) is exceeded.

Enter these CLI commands:

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

Change the default count and rate limits with these CLI commands:

```
hostname.com> Netif Set MaxTcpConnectCount "" Integer
OK Completed
hostname.com> Netif Set MaxTcpConnectRate "" Integer
OK Completed
```

Use the `Netif AddTrustedIP` command to exempt selected hosts from the TCP limits; for more information, see `Help Netif Set` in the CLI help.

Adding the Address Book URL—Internal Directory

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" "url" "options"
```

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. If you entered all of the commands in the allinone.html file, you already entered the Address Book URLs.

This example uses the localhost as the addressbook directory service server; if you use the localhost, the addressbook directory service you add will be empty (no contacts). Replace this server, `ldap://127.0.0.1:389`, with the server address that contains your Address Book directory, if you have one.

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=mirapointmai
luser)(|(sn=$(cn))(givenname=$(cn))(cn=$(cn))(mail=$(mail)*)(maillocaladdr
ess=$(mail))))" ""
OK Completed
```

Traffic running through Address Book URLs only require Read access to the directory.

Adding the Address Book URL—Active Directory

Use the `Url Add` command to add an address book URL that points to the Active Directory by specifying the URL for your Active Directory, the Active Directory base DN, and your bind DN and password.

- Specify your Active Directory URL in place of *adhostname.yourdomain.com*
- Specify your Active Directory base DN in place of *DC=adhostname,DC=yourdomain,DC=com*
- Specify your Active Directory bind DN in place of *CN=Administrator,CN=Users,DC=adhostname,DC=yourdomain,DC=com*
- Specify the password that corresponds to the user specified in the bind DN in place of ***password***:

```
hostname.com> Url Add Addrbook:AD "Active Directory" "ldap://
adhostname.yourdomain.com:3268/
DC=adhostname,DC=yourdomain,DC=com??sub?(&(&(cn=$(cn))
(mail=$(mail)))(|(objectclass=person)(objectclass=group)))"
"(binddn=CN=Administrator,CN=Users,DC=adhostname,DC=yourdomain,DC=com)(bin
dpasswd=password)"
OK Completed
```

This is an example using `docexchange.mirapoint.com` and a bind DN/password of `administrator/1234abcd`:

```
hostname.com> Url Add Addrbook:AD "Active Directory" "ldap://
docexchange.mirapoint.com:3268/
DC=docexchange,DC=mirapoint,DC=com??sub?(&(&(cn=$(cn))
(mail=$(mail)))(|(objectclass=person)(objectclass=group)))"
"(binddn=CN=administrator,CN=Users,DC=docexchange,DC=mirapoint,DC=com)(bin
```

```
dpasswd=1234abcd)"
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 201.

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 203.

Traffic running through Address Book URLs only require Read access to the directory.

Setting up Group Calendar—Internal Directory

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.

If you are using Active Directory, refer to the SynQ Information website and access the *User Guide* for configuration and installation directions.

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. If you entered all of the commands in the allinone.html file, you already entered the Group Calendar URLs.

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

- **Mailroutingaddress** specifies where users receive email (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.**
- **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" "url" "options"
```

The `Url Add` command is domain-specific. These examples add the URL to your primary domain (`miDomainName=primary`). Adding the URL to delegated domains is explained in Configuring Calendar Options for Domains on page 192.

Traffic running through Calendar URLs only require Read access to the directory.

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. 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?(&(|(objectclas
   s=person)(objectclass=inetorgperson)(objectclass=mirapointUser))(|(uid=$(c
   n)*)(miloginid=$(cn)*)(sn=$(cn)*)(givenname=$(cn)*)))"
   "(uidalias=miloginid)"
   OK Completed
   ```

   The system LDIF uses **miloginid** to identify the user, not **uid**. In fact, the LDIF does not contain a **uid** attribute 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. 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)"
   ```

3. To allow for exact matching, entering the following commands, one for **User** matching, one for **Group** matching, and one for **Resource** matching. These commands add an extra layer of checking when you have many users, groups, or resources and may have name conflicts. If you choose, replace *User/Group Exact Match* with a custom name for this lookup. This URL uses 127.0.0.1 (localhost), replace this if your LDAP server is external:

   ```
   hostname.com> Url Add groupcalendar:matchuser "User Exact Match" "ldap://
   127.0.0.1:389/ou=domains,o=corp?cn?sub?(milogin=$(cn))" uidalias=milogin

   hostname.com> Url Add groupcalendar:matchgroup "Group Exact Match" "ldap://
   127.0.0.1:389/ou=domains,o=corp?cn?sub?(cn=$(cn))" ""
   ```

   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"
   ```

   For example, this command deletes the URL you added in step 1:

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

4. 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
```

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.

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

Completing Group Calendar Setup—Administration Suite

Continue Group Calendar setup using the Administration Suite pages; follow these steps.

1. Go to **Home > Domains > Calendar > Resources**. In the **Resourcegreoup 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.

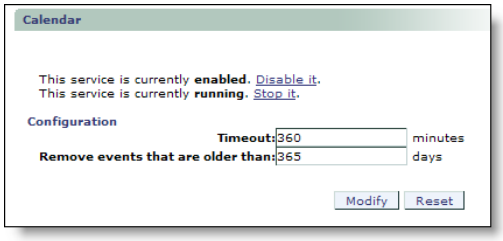
2. Specify the following for each resource (meeting rooms, equipment such as projectors, and so forth) that you want to make available for calendar users. This information is added to your LDAP database.

   - **Fullname**: The name of the resource as you want it to appear in the **Choose a Resource** drop-down menu 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: The resource entries are made available in the calendar **Schedules** tab **Choose a Resource** drop-down menu; 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. Idle WebCal connections are disconnected when the idle timeout is reached.

4. 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.



5. 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 192.

Configuring WebMail

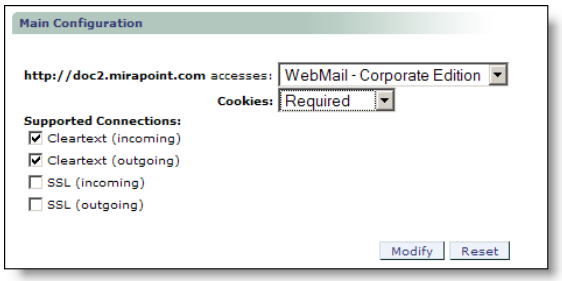
Enable the WebMail service to allow users to retrieve and manage their messages from a Web browser. When the **External Mail** feature is enabled, users can download POP3 mail from other clients. Idle WebMail connections will be disconnected when the idle timeout is reached.

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 menu for the **http://<hostname.domain.com> accesses** option.

   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.

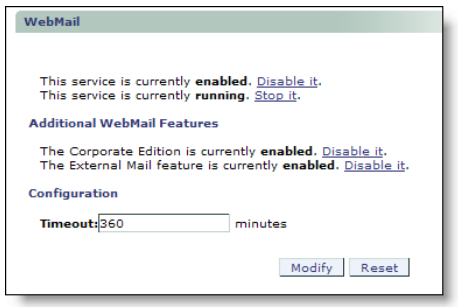
2. Also on the **HTTP > Main Configuration** page, protect WebMail session IDs by selecting **Required** for the **Cookies** option. This prevents users from unintentionally giving access to their mail by copying and pasting their session ID into an email.

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.



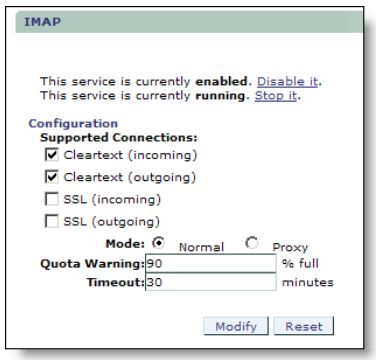
5. If the WebMail service is disabled, click **Enable it**. If the service is stopped, click **Start it**.

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**.

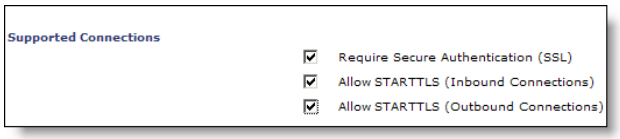
Configuring SMTP

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

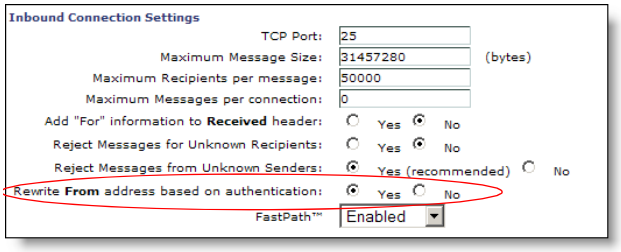
1. Go to **Home > System > Services > SMTP > Main Configuration**. Do not enable or start the service until the end of this procedure.

   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.

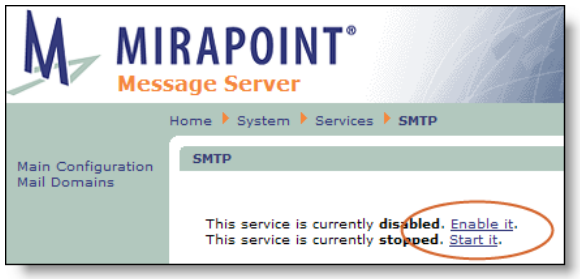


3. In the **Inbound Connection Settings** area, select the **Rewrite From address based on authentication** option and leave the rest of the options set to the defaults. The **Rewrite address based on authentication** option specifies whether sender addresses in message envelopes and **From** headers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



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**.

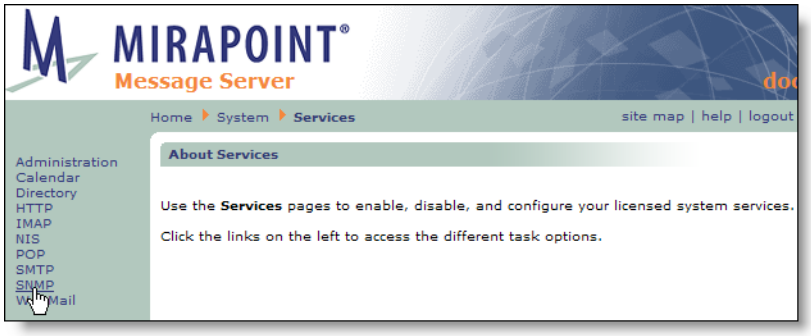


Enabling and Starting Services

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; 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**.



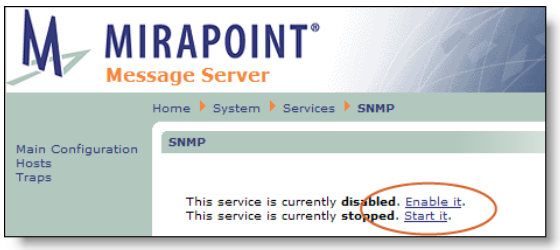
2. At this point, most services have already been enabled and started, the following might still need attention.

   - **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
     - Tivioli: Defaults to version 3
     - Veritas: Defaults to version 2

   For more information about these Data Management Applications (DMAs), see NDMP Backup Solutions on page 371.

   - **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.

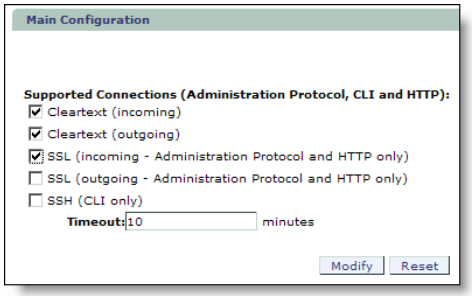
   To learn more about SNMP see Monitoring External Systems via SNMP on page 176 in the Administration Tasks part of this book.



Resetting the Administration Timeout

Setting the timeout to 60 minutes is recommended for the configuration procedures; however, once you are done, you will 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.

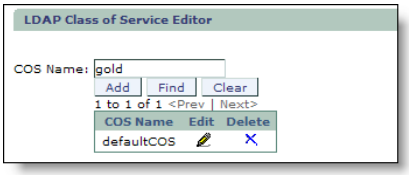
Refresh the Administration Suite

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—Internal Directory Only

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

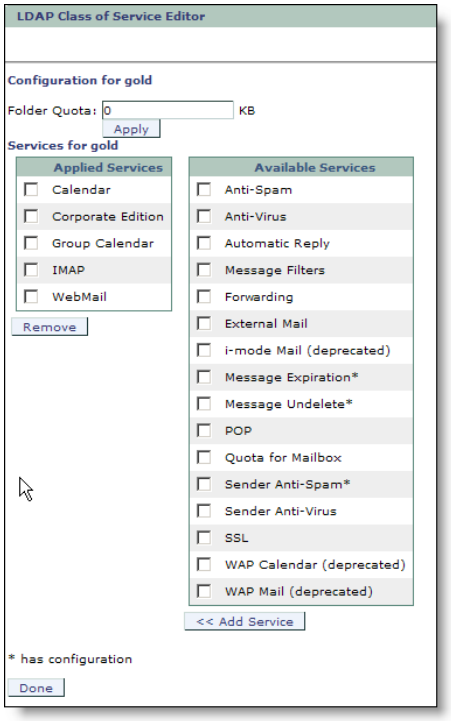
1. Go to **Home > Class of Service**, enter a name for the COS. For this test, enter **gold** as the **COS Name**. Click **Add**.



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 (at least) for the COS:

   - **Calendar**—WebCal Direct Standard Edition (Personal)
   - **Corporate Edition**—WebMail/Group Calendar Corporate Edition
   - **Group Calendar**—WebCal Direct Standard Edition (Group)
   - **IMAP**—Message sending and receiving
   - **WebMail**—WebMail Direct Standard Edition

   Click **Add Service**.

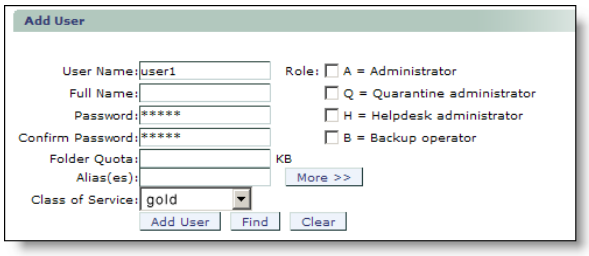


3. Click **Done** at the bottom of the page to return to the main **Class of Service** page.

Create User Accounts—Internal Directory Only

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.**



3. 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.**

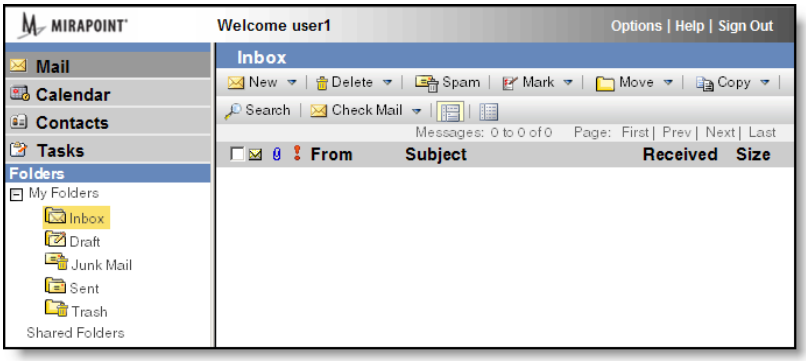
Send a Test Message

To send a test message:

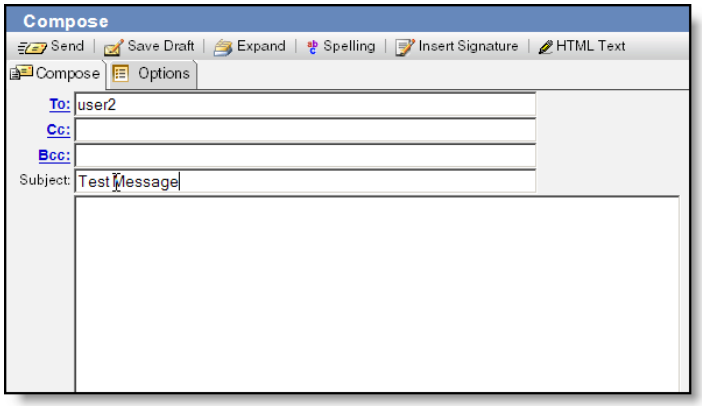
1. Open your Message Server's URL in a web browser; for example, `http://hostname.domain.com`.
2. Log into WebMail with the **user1** username and password for the Internal Directory setup. For the Active Directory setup, log in as a configured Active Directory user (you must know the username and password); verify that the user is created on the Message Server after login.

In the following examples, Corporate Edition WebMail is shown.

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

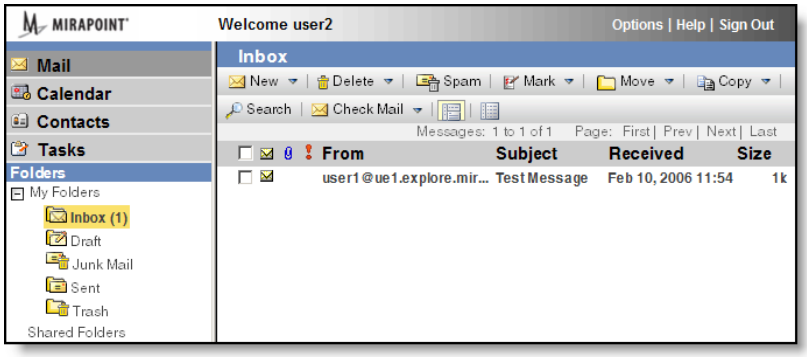


4. Address the message to **user2@*hostname.domain*.com** for the Internal Directory setup, to a configured Active Directory user for the Active Directory setup, and click **Send**.



Receive a Test Message

To receive the test message, log into WebMail with the **user2** username and password (Internal Directory) or the Active Directory username to which you sent mail. The test message should be listed in the user'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 76.

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 menu 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—Internal Directory Only

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.

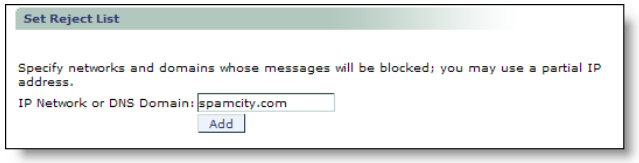
Optional Configuration Tasks

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 email from 10.127.1.1 through 10.127.1.128 but accepts email 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.



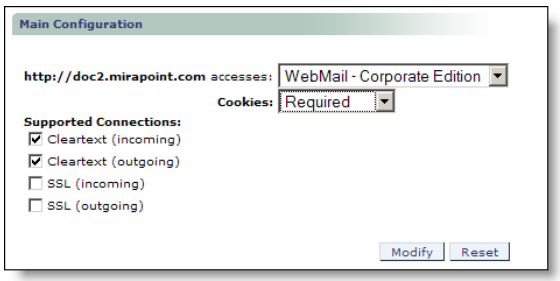
2. Enter the IP Network or domain name. Click the **Add** button.

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

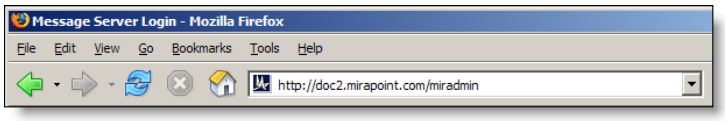
directed to WebMail when they load the appliance's URL. You did this in the Configuring WebMail on page 65 procedure, but you might want to change the HTTP default access, follow these steps.

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.

To access the administration interface after you've changed the HTTP default access, append **/miradmin** to the URL. For example, `http://hostname.domain.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 310, Setting the Blocked Senders List on page 312, and Setting the Allowed Mailing Lists List on page 314. These are tasks that will need to be done regularly as your system develops.

Adding a Multi-Listener

You must use the CLI to add multi-listeners; see Accessing the Command Line Interface on page 26 for details.

Imagine that you want to set up a Message Server that accepts email from the Internet on the conventional SMTP port 25 at the server's public IP address, 10.1.1.25 for example. This is the default for message transfer. You also want to accept mail submissions on the agreed-upon port 587; see RFC 2476. Here is the command needed:

```
Smtp Addlistener *:587
```

See Configuring Multi-Listeners on page 323 or, using the CLI, **Help About Smtp**, for more information.

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. Monitor your system license expiration dates and backup your system configuration to avoid unplanned downtime.

Getting the Active Directory bindDN

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

1. Connect to your Exchange 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:

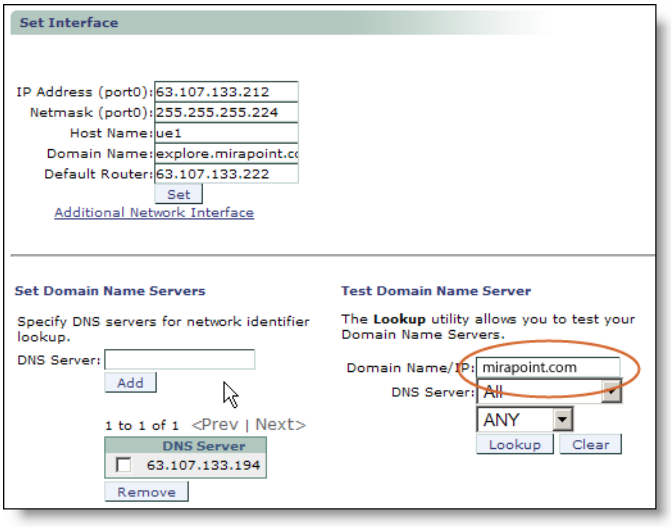
   ```
   dn: CN=Administrator, CN=Users, DC=adhostname, DC=yourdomain, DC=com
   ```

   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, the entire DN is specified as the bind DN: `CN=Administrator, CN=Users, DC=adhostname, DC=yourdomain, DC=com`.

Test Message Send Fails

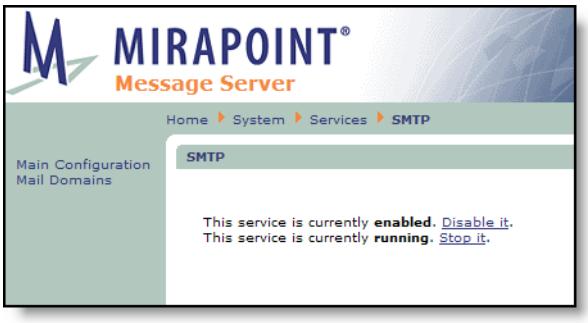
If you cannot send test messages between user accounts on your Message Server, check the following:

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 (e.g., mirapoint.com) in the **Domain Name/IP** field.



   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, All-In-One Deployment

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 233 and Setting Up Message Expiration on page 234.
- **Set up System Backups**—Mirapoint supports a number of different solutions for backing up and restoring user data. For more information, see Business Continuity Tasks on page 369.
- **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 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.

3

Message Server Setup for Multi-Tier Deployments

In this deployment, a Message Server appliance performs directory services, message storage, and delivery behind two RazorGates performing routing, antispam, and antivirus scanning. Setting up the Message Server functions is described in this chapter; see the *RazorGate Administrator's Guide* for details on setting up those functions.

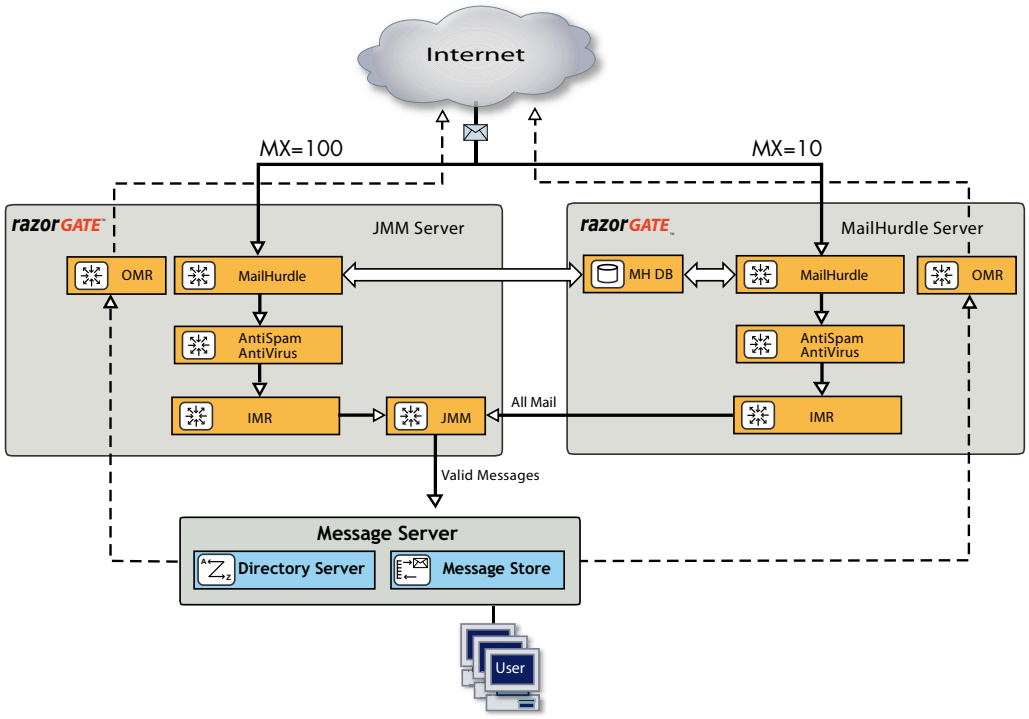


Figure 2 Message Server in a Multi-Tier Deployment Example

Before You Begin

Before you begin configuring your Message Server's directory 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 with needed records ("A," "MX," "PTR," and "CNAME"). For more information, see DNS Records Recommended for a Multi-Tier Deployment on page 22.
  - Lightweight Directory Access Protocol (LDAP) set up
  - Licenses obtained (licenses are implementation specific)
  - Backup requirements defined
  - Secure Sockets Layer (SSL) certificates obtained
  - Hardware installation (connected to the Internet)
  - 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 Message Server for Multi-Tier deployment, as documented here:

- The hostname, port number, and authentication credentials for your Firewall proxy server if your site blocks outgoing HTTP or FTP connections. This is required to get system updates, antivirus updates, 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 and hostnames for the two RazorGates fronting this Message Server or DNS symbolic hostname. See DNS Records Suggested for MMS Multi-Tier Configuration on page 81. These DNS records must be set up before attempting this configuration!

Even if you currently only expect to use a single domain, Mirapoint recommends that you create your domain as a delegated domain (for example, mail.example.com) 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 delegated domains.

Delegated domains are amongst the last things to be configured.

- **Licenses**—The licenses for this deployment are listed below. How to check for licenses is described below on page 83.

Licenses are implementation-specific.

  - Required licenses:
    - User Limit
    - Mail Routing
    - WebMail
    - Corporate Edition
    - POP
    - IMAP
    - Message Server
    - Group Calendar
    - (SSL) Weak Encryption and/or Strong Encryption
    - Directory Server
    - Delegated Domain Administration
  - 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
    - Principal Edition Antispam or Signature Edition Rapid Antispam

DNS Records Suggested for MMS Multi-Tier Configuration

In this deployment, an MMS performing directory services and mail storage/transfer sits behind two RazorGates performing routing and security functions. In order to set redundant routing we recommend you create a round-robin DNS record so, if either RG is not available, routing still occurs. You do this by creating a symbolic hostname, for example rgs.example.com, and assigning it two "A" records: the IP addresses of both RGs. This symbolic hostname is then used (through CNAME records) to specify the SMTP OMR and LMR, and WebMail OMR, on the MMS. This is discussed in detail in DNS Records Recommended for a Multi-Tier Deployment on page 22.

Configuring A Message Server for Multi-Tier Deployment

In this deployment, a Mirapoint Message Server (MMS) performs message storage and delivery, and outbound message handling. This configuration involves the following tasks:

- Accessing the Administration Suite
- Checking for Licenses
- Setting the Administration Timeout

- Configuring Anti-Spam Scanning
- Setting Up a User Directory Service
- Command Line Configuration Tasks—Multi-Tier Message Server
- Configuring WebMail
- Configuring IMAP
- Configuring SMTP
- Enabling and Starting Services
- Resetting the Administration Timeout

To test your multi-tier Message Server setup, perform these tasks:

- Refresh the Administration Suite
- Create a Class Of Service—Internal Directory Only
- Create a Delegated Domain
- Create User Accounts—Internal Directory Only
- Send a Test Message
- Receive a Test Message
- Verify the Address Book Directory Service
- Create a Calendar Event—Internal Directory Only

One optional configuration task is also described:

- Adding a Multi-Listener—Allows your system to listen for SMTP connections on multiple ports and interfaces at once.

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 may need to use the Setup Wizard to perform the basic configuration tasks described in Completing the Setup Wizard on page 27 before continuing.

If you are comfortable using the CLI, we recommend using both interfaces as some tasks are more easily accomplished with the CLI and a few tasks can only be done using the CLI. However, if you do so, you will need to occasionally log out and then back in to the Administration Suite to see changes. For information on accessing the CLI, see Setting Up a User Directory Service on page 85.

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. Click **Install Licenses** if needed.

In the CLI, type:

```
hostname.com> license list
OK Completed

hostname.com> license fetch
OK Completed
```

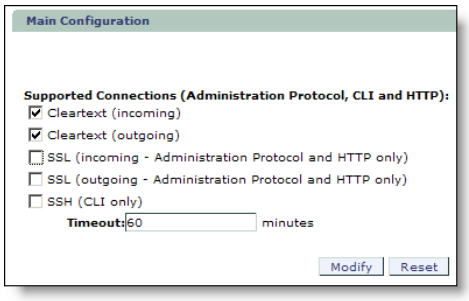
The MailHurdle license does not display; it is part of the Anti-Spam license. The internal LDAP directory requires the Mail Routing license.

Setting the Administration Timeout

You will want to change the default Administration Suite timeout from 10 minutes to at least 60 minutes while you configure the Message Server to give yourself time; afterwards, reset the timeout back to 10 minutes.

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

Click **Modify** to save your changes.



In the CLI, type:

```
hostname.com> admin set timeout 60
OK Completed
```

Configuring Anti-Spam Scanning

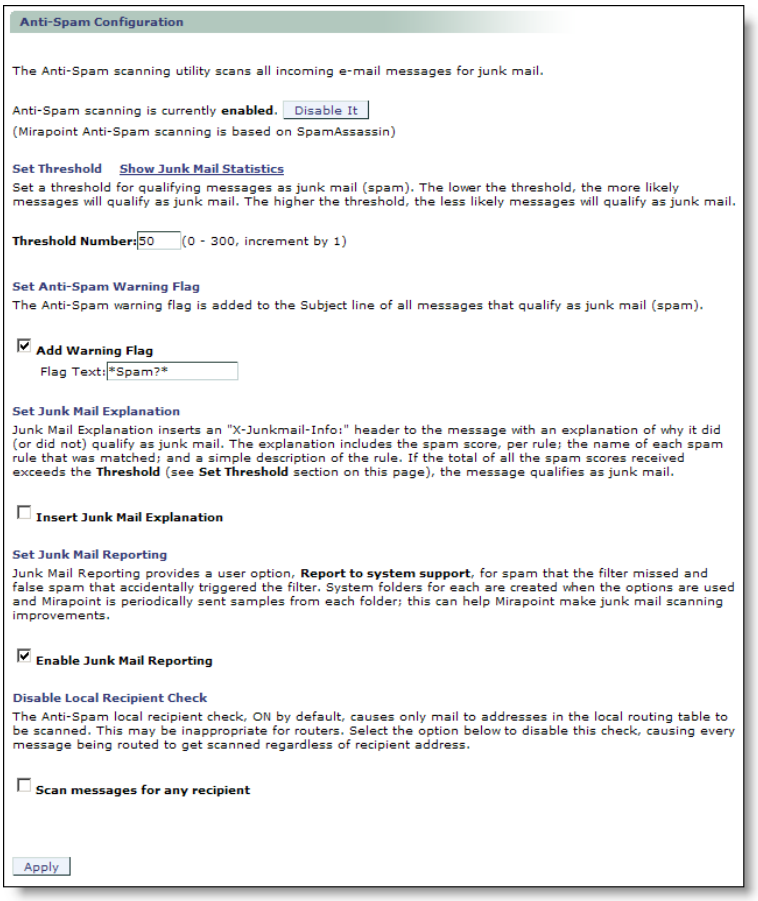
There are two antispam licenses, **Principal Edition Antispam** and **Signature Edition Rapid Antispam**. For details , see Principal Edition vs. Signature Edition on page 304.

Mirapoint recommends licensing Antispam on the MMS for this deployment but disabling it. The reason for this is to allow users to opt-out of JMM. If a user chooses to opt-out of JMM, then the Antispam license on the MMS will allow that user to receive their spam mail as they specify in their options/preferences (usually to a **Junkmail** folder).

If you add an additional antispam scanner, be sure to go the **Anti-Spam Updates** page for that scanner and click **Update Now** to get the most recent files for that scanner.

To configure Anti-Spam scanning for this deployment:

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



2. Skip the **Anti-Spam > Allowed Senders**, **Blocked Senders**, and **Allowed Mailing Lists** pages; set these on the RazorGates.
3. Go to the **Anti-Spam > Relay List** page, enter the IP addresses of the two RazorGates fronting this MMS.
4. Skip the **Anti-Spam > RBL Host List** and **Reject List** pages; set these on the RazorGates.
5. Skip the **Anti-Spam > MailHurdle** page; set MailHurdle on your RazorGates.

Additionally antispam methods available only through the CLI are detailed later in this chapter in Command Line Configuration Tasks—Multi-Tier Message Server on page 94.

Setting Up a User Directory Service

A user directory service manages user routing information and authentication. To set up an internal LDAP directory service or an Active Directory service, you must have the Mail Routing license.

This section describes two options for setting up a directory service on your Message Server:

- Message Server's internal LDAP Directory; to do this, follow the instructions in Setting Up the Internal LDAP Directory, next.
- Microsoft Active Directory; to do this, follow the instructions in Setting Up Active Directory on page 91.

You need to use the command-line interface (CLI) to set up the directory and configure the Message Server to use it. Additionally, Mirapoint recommends that you use the CLI to set other options before returning to the Administration Suite to complete the configuration process; those procedures are provided in Command Line Configuration Tasks—Multi-Tier Message Server, following this section.

To access the CLI, connect to your Message Server using telnet in a command window, and log in as the Administrator:

```
Start > Run: telnet hostname.domain.com
OK hostname.domain.com admind 3.10 server ready
User: Administrator
Password: password
OK User logged in
```

CLI commands are case-insensitive. To make the examples easier to read, they are shown in mixed case.

About LDAP GUI and LDAP GUI-JMM

Part of the Internal LDAP Directory setup, described next, is enabling LDAP GUI, which allows certain pages of the Administration Suite to write data to, and retrieve data from, your LDAP database. If your set up includes Junk Mail Manager (JMM), you will also want to enable LDAP GUI-JMM. Enabling these provisioning pages allows you to:

- Create domains and users in the administration protocol AND on a Directory Server in LDAP, or Internal LDAP—but not locally.
- Design and apply Classes of Service (with LDAP GUI-JMM, this includes JMM) to users or domains.
- Authenticate logins with Class of Service.

In order for you to be able to use these provisioning pages, you must first set up LDAP, including importing an LDIF file, and also set up your LDAP client with queries, enable the services, and configure Class of Service (COS) (described next). Once you have enabled LDAP GUI, the **Domains** pages in the Administration Suite change to display this flag in the bottom left, **LDAP Domain**, indicating that it was created in your LDAP database.

Additionally, the **Class of Service** page displays at the top-level with this flag in the bottom left, **LDAP Enabled**, indicating that actions you take on that page are instantiated in your LDAP database.

You cannot use the Setup Wizard to enable the provisioning. If you have an existing Directory Server set up with LDAP, this procedure does not work; you may need to contact Mirapoint Support for migration.

Enabling LDAP GUI disables the **Use LDAP Password** option on the LDAP enabled **Domains > Users** page; passwords will be stored in LDAP. Enabling LDAP GUI-JMM disables the **Select additional services link** on the LDAP enabled **Domains > Users** page.

Once LDAP GUI-JMM is enabled, these pages in the Message Server Administration Suite change, you will make these configurations later in this chapter, do not attempt these configurations yet:

- **Class of Service** page—An additional service, **Junk Mail Manager**, displays in the **Available Services** table. Like other services that require configuration, the Junk Mail Manager service is starred (*). Specifications to your Junk Mail Manager service here is recorded to your LDAP server Junk Mail Manager records.
- **Class of Service > Editor** page:—If the **Junk Mail Manager** service is selected, these configuration options for it display:
  - **JMM Message Expire**—How long spam message can remain in the Junk Mail Manager account before being automatically expired (permanently discarded).
  - **JMM Mailbox Quota**—How many spam messages can be delivered to the Junk Mail Manager account before being over-quota.

  Additionally, the **Anti-Spam**, **Message Expiration**, and **Quota for Mailbox** services are automatically selected; JMM requires them.
- **Domains > Administration** and **Edit** pages—An additional configuration option, **Junkmail Manager Host**, displays. Remember, Junk Mail Manager uses Message Server delegated domains as Junk Mail domains.
- **Domains > Add User** page—If you select a COS that includes the **Junkmail Manager** service, an additional configuration option, **JMM Folder Quota**, displays.

Once you enable LDAP GUI-JMM and make those configurations, the following attributes are added to the selected COS record:

```
miquarantinequota: quota
mimailexpirepolicy: QTNBOX.* expire days I
miservice: msgexpiration
miservice: quota
miservice: antispam
miservice: junkmailmanger
midefaultjunkmailfilter::
IOBNaXJhcG9pbnQtRmlsdGVyLTEuMAOKZmlsdGVyICJTeXNOZWOg
SnVuayBNYWlsIFJ1bGUiIFF1YXJhbnRpbmUgIlFUTkJPWC5KdW5rIE1haWwiIGFsbG9mIHNOb3
ANC
jpVQOUgaXMgIm5vcm1hbCINCg==
```

Setting Up the Internal LDAP Directory

The Message Server includes a built-in LDAP directory server you can use for user authentication. This procedure sets up an LDAP database from scratch; you can use this procedure to set up an LDAP database locally (internal to the Message Server) or on a Mirapoint Directory Server. If you have never set up an LDAP database before, it would be wise to read through the procedure before beginning.

There are a few ways that you can use this procedure:

- In a browser, go to http://www.mirapoint.com/support/allinone.html. Copy and paste the data from this file, including the LDIF, plugging in your own passwords. Everything that you need to do is included in the allinone.html file.
- You can copy the allinone.html file to a text editor (e.g., Notepad), change the passwords, and then enter the data (a chunk at a time works best) into your telnet window.
- You can use the following pages and manually enter the commands, one at a time.

If you have any problems accessing the HTML file, the data that needs to be entered is given in the steps below; you can use these steps to better understand what you are doing. Do not repeat the procedure. 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 manually set up the internal LDAP directory with a directory database named **miratop**.

Using the allinone.html file mentioned above is, generally, much simpler.

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 Adddbsuffix` command to add a new DIT (directory information tree) with the distinguished name (DN) o=miratop to the directory named miratop:

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

3. Enter the `Dir Setdboption` command to set the directory administrator's RootDN (distinguished name):

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

4. Enter the `Dir Setdboption` 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 setdboption 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 "" miloginid 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 web 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
```

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
```

Configuring 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 included in the allinone.html file. These commands direct the Message Server to the LDAP directory that you set up locally; if you set up the directory on a Mirapoint Directory Server, replace the host specified in the **Ldap Add Ldap** step with the IP address of the Directory Server.

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=$(login))(miloginid=$(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 Setting Up the Internal LDAP Directory on page 87 in place of ***adminpassword***:

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

Enabling LDAP GUI and COS

Use the following procedure to enable the LDAP GUI (described in About LDAP GUI and LDAP GUI-JMM on page 85) and Class of Service function.

1. Enter the `Conf Enable` command to enable all LDAP configuration options, including the LDAP auto-provisioning pages (LDAP GUI):

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

2. 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 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
   ```

To complete the setup of the internal directory service, keep your CLI window open and skip to Command Line Configuration Tasks—Multi-Tier Message Server on page 94. You do not need to set up Active Directory.

Setting Up Active Directory

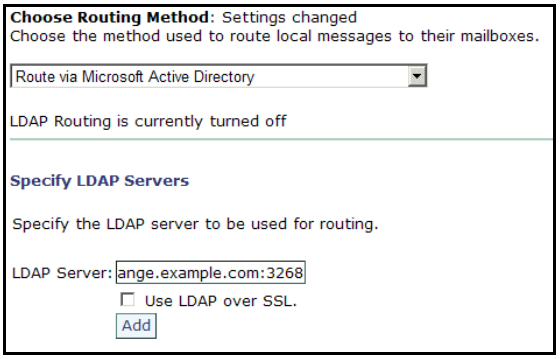
You can use Microsoft's Active Directory service for user authentication instead of using the Message Server's internal LDAP directory server. To configure the Message Server to interoperate with Active Directory, you will need:

- The IP address or domain name of your Exchange server, for example **192.168.0.1** or **adhostname.yourdomain.com**
- The **Administrator** password for your Exchange server
- The Active Directory base DN (distinguished name), for example **DC=*adhostname*, DC=*yourdomain*, DC=com**
- The Active Directory bind DN the Message Server will use for authentication when accessing the directory, for example **CN=Administrator, CN=Users, DC=*adhostname*, DC=*yourdomain*, DC=com**
- The password for the user identified in the bind DN. (For example, the password for **Administrator**.)
- Mirapoint recommends creating a new user for use by the Mirapoint server; you will need the DN and password for that user.

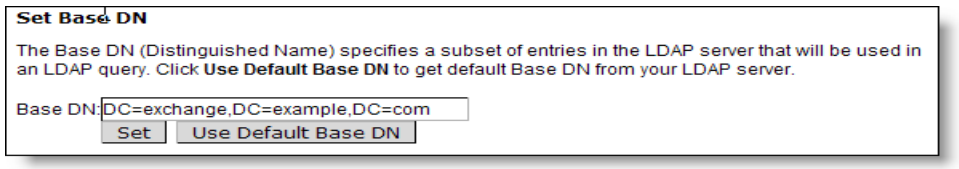
Instructions for getting your Active Directory DN information are provided in Getting the Active Directory bindDN on page 112.

Most of the Active Directory setup can be done using the Administration Suite; follow these steps.

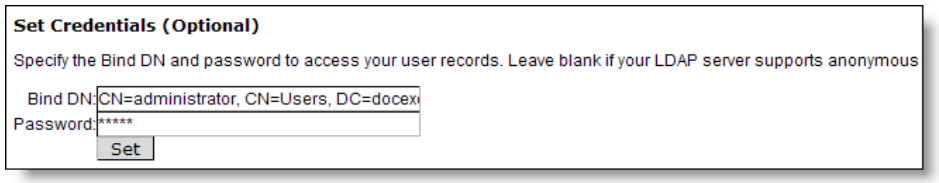
1. Go to **Home > System > Routing**. On the **Choose Routing Method** page, select **Route via Microsoft Active Directory**. For the **LDAP Server** option, type the name of at least one Active Directory Exchange server plus the port (usually 3268). For example, **ldap://docexchange.mirapoint.com:3268**.



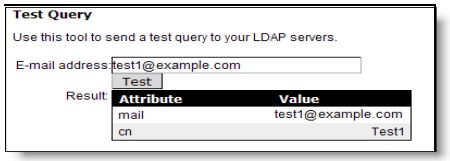
2. Go to **System > Routing > User Queries** page, under the heading **Set Base DN**, click **Use Default BaseDN**. All the user query filter and attribute names appear automatically.



3. In the **Set Credentials** area, enter the bindDN of the Active Directory administrator; this is not optional for Active Directory. Click **Set.**



4. Under the **Test Query** heading, type a user email address such as test1@exchange.example.com or some valid address in the Active Directory database. The **mail, mailhost,** and **cn** (full name) values should appear for that email address.



5. Go to **System > Routing > Mail Group Queries** page, under the heading **Set Mail Group Base DN**, click **Use Default BaseDN**. All the mailgroup query filter and attribute names appear automatically.
6. Skip the **Set Credentials** area, you set this in step 3.
7. Under the **Test Query** heading, type a mailgroup email address such as TechPubs@exchange.example.com or some valid address in the Active Directory database. The **mail, mailhost,** and **cn** (full name) values should appear for that email address.
8. Go to the **System > Routing > Mail Host Mapping** page. Enter all Active Directory domain names; for each, enter the Message Server hostname as the **Mail Host**. Click **Add** for each entry.
9. Ensure that the POP and IMAP service modes are set to normal by going to **System > Services > IMAP and System > Services > POP** and verifying that the **Mode: Normal** radio button is selected.
10. Enable HTTP routing via LDAP by going to **System > Services > HTTP > Mode** and selecting **LDAP Redirect**.
11. Set the Group Calendar user search mode to local by going to **Domains > Calendar > Search Configuration** and selecting **Local only.**

Configuring Outbound Routing on the Exchange Server

You must set your Message Server as the outbound router Smart Host on the Exchange server; follow these steps. For more infromation on configuring Microsoft Exchange 2003/2000 to use a Smart Host IP Address, search the knowledge base at the Microsoft Help and Support website (http://support.microsoft.com/).

1. Log in to your Exchange server as administrator and go to **Start > 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 Message Server and click **OK**. You can specify multiple smart hosts by separating the FQDNs with semi-colons.
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.

To complete the setup of the Exchange directory service, you must use the CLI and follow the Command Line Configuration Tasks—Multi-Tier Message Server," described next. To access the CLI, connect to your Message Server using telnet in a command window, and log in as the Administrator:

```
Start > Run: telnet hostname.domain.com
OK hostname.domain.com admind 3.10 server ready
User: Administrator
Password: password
OK User logged in
```

Command Line Configuration Tasks—Multi-Tier Message Server

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

- Setting the Default Authentication
- Setting Up Autoprovisioning of Users
- Configuring Banner Delay
- Configuring Second Scan for Anti-Spam
- Setting Up Autoprovisioning of JMM Users
- Setting the OMR for WebMail
- Trusted Hosts for Multi-Tier Installations
- Adding the Address Book URL—Internal Directory
- Adding the Address Book URL—Active Directory
- Setting up Group Calendar—Internal Directory Only

CLI commands are case-insensitive. To make the examples easier to read, they are shown in mixed case.

Setting the Default Authentication

You must use the CLI to set the authentication; do this for an Internal Directory setup or an Active Directory setup. Telnet to your mail server and enter this command:

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

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**.

Enable LDAP autoprovisioning with the **Ldap Set** command:

```
Ldap Set Autoprovision On
```

More information on autoprovisioning, including how to transfer existing records, is provided in Bulk Provisioning Users on page 209 in the Administration Tasks part of this book.

Configuring Banner Delay

You can configure your system to delay greeting acknowledgement during the SMTP chat session. Senders who violate the RFC by sending data before the greeting acknowledgement can be rejected.

Mirapoint recommends turning banner delay **On** if you are not using MailHurdle or you are using MailHurdle in SuspectList mode (see **Help About Mtaverify** in the CLI help for details).

To do this, enter these CLI **SMTP** commands:

Enable banner delay (default is **Off**).

```
hostname.com> Smtp Set Bannerdelay On
```

Sets banner delay time in seconds (default is 5). Setting delay to **0** sets the banner delay time to the default value, 5 seconds.

```
hostname.com> Smtp Set Bannerdelaytime 5
```

Use **Smtp Get Bannerdelay** and **Smtp Get Bannerdelaytime** to retrieve the configured delay state and time.

Banner delay is not subject to sender whitelisting. However, messages originating locally from the receiving server and senders on the relay list are exempted from banner delay.

These commands apply system wide and are not domain sensitive.

Configuring Second Scan for Anti-Spam

You can now run both Signature Edition (RAPID AS) and Principal Edition antispam scans on the same server. Administrator's can choose to run both scans on all messages or to run the second scan only for messages classified as "bulk" by RAPID.

- `Multienginebulkonly`: Setting this to **Off** (default) configures both licensed scanners to run for all messages. The higher returned score is used to determine the UCE score in the header X-Junkmail-Status and X-Junkmail:UCE headers.
- `Multienginebulkonly`: Setting this to **On** setting configures second scan to run only for messages classified as bulk by Signature Edition (UCE scores between 50 and 60). For these bulk classified messages, the result of the second scan overrides the bulk classification.

If you run this command with only one Antispam scanner licensed, it has no effect until the second scanner is licensed. If two scanners are licensed but this option is **Off**, then the larger spam score wins, which can increase false positives. Running both scanners is resource intensive, but much less so with this option **On**.

Mirapoint recommends setting `Multienginebulkonly` to **On** if you consider that your two-engine spam scanning is taking too long.

To do this, enter the following CLI `Uce` command:

```
hostname.com> Uce Setoption Multienginebulkonly (Domain=local) On
```

Use `Uce Getoption Multienginebulkonly (Domain=local)` to retrieve the mode setting.

Setting Up Autoprovisioning of JMM Users

If your deployment includes Junk Mail Manager, follow this procedure; if not, skip this and go directly to Setting the OMR for WebMail on page 96, next. In order for Junk Mail Manager accounts to be autoprovisioned properly, you must enable LDAP GUI on the Mirapoint Message Server; this is described in step 1 of the Configuring the Message Server to Use the Internal LDAP Directory on page 88 procedure. LDAP GUI-JMM autoprovisions JMM accounts for users when their first spam mail is tagged.

For this deployment, an additional step is required, enabling LDAP provisioning for JMM. To do this, access the CLI for your LDAP GUI enabled Message Server and enter this command:

```
hostname.com> Conf Enable Ldapgui-Jmm
OK Completed
```

Setting the OMR for WebMail

You must use the CLI to set the WebMail outbound router (OMR); do this for an Internal Directory setup or an Active Directory setup. Telnet to your mail server and enter this command, replacing *rgs.example.com* with the appropriate symbolic hostname:

```
hostname.com> Webmail Set OMR rgs.example.com
```

This specification requires the symbolic hostname DNS record as discussed in detail in DNS Records Recommended for a Multi-Tier Deployment on page 22. Later you will set an SMTP OMR.

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**.

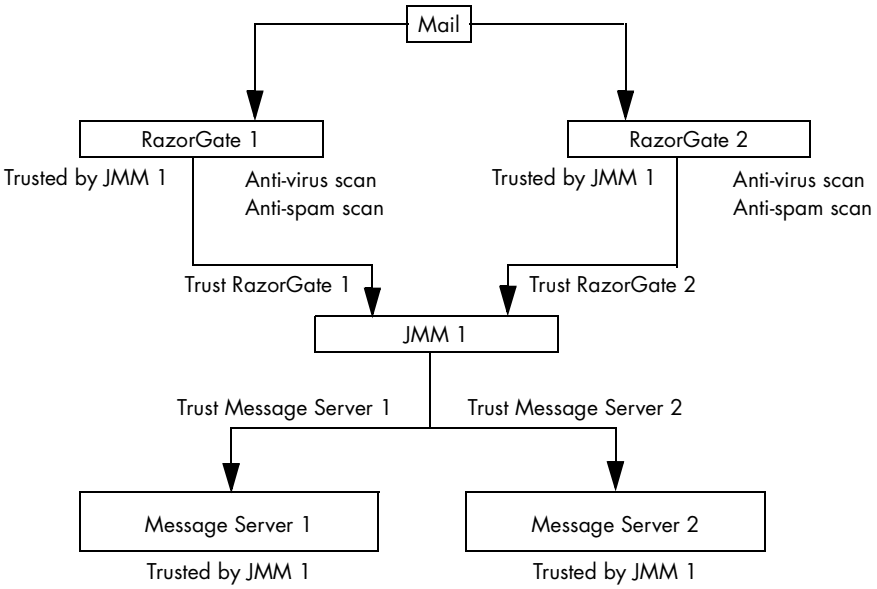


Figure 3 Trusted Host Relationships In A Multi-Tier Environment

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 doesn't exist.

Adding the Address Book URL—Internal Directory

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

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" "url" "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.

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. If you entered all of the commands in the allinone.html file, you already entered the Address Book URLs.

This example uses the localhost as the addressbook directory service server; if you use the localhost, the addressbook directory service you add will be empty (no contacts). Replace this server, ldap://127.0.0.1:389, with the server address that contains your addressbook directory, if you have one.

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

The **Url Add** command is domain-specific. These examples add the URL to your primary domain. Adding the URL to delegated domains is explained in Configuring Calendar Options for Domains on page 192.

If you are not using Active Directory, skip the next procedure and go to Setting up Group Calendar—Internal Directory Only on page 99.

Traffic running through Address Book URLs only require READ access to the directory.

Adding the Address Book URL—Active Directory

Use the **url add** command to add an address book URL that points to the Active Directory by specifying the **URL** for your Active Directory, the Active Directory **base DN**, and your **bind DN** and **password**. Specify your Active Directory URL in place of ***adhostname.yourdomain.com***, your AD base DN in place of ***DC=adhostname,DC=yourdomain,DC=com***, your AD bind DN in place of ***CN=Administrator,CN=Users,DC=adhostname,DC=yourdomain,DC=com***, and the password that corresponds to the user specified in the bind DN in place of *password*:

```
hostname.com>url add addrbook:AD "Active Directory" "ldap://
adhostname.yourdomain.com:3268/
DC=adhostname,DC=yourdomain,DC=com??sub?(&(&(cn=$(cn))
(mail=$(mail)))(|(objectclass=person)(objectclass=group)))"
“(binddn=CN=Administrator,CN=Users,DC=adhostname,DC=yourdomain,DC=com)(bin
```

```
dpasswd=password)"
OK Completed
```

This is an example using “docexchange.mirapoint.com” and a binddn/bindpasswd of “administrator/1234abcd”:

```
hostname.com>url add addrbook:AD "Active Directory" "ldap://
doxexchange.mirapoint.com:3268/
DC=docexchange,DC=mirapoint,DC=com??sub?(&(&(cn=$(cn))
(mail=$(mail)))(|(objectclass=person)(objectclass=group)))"
“(binddn=CN=administrator,CN=Users,DC=docexchange,DC=mirapoint,DC=com)(bin
dpasswd=1234abcd)"
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 201.

Traffic running through Address Book URLs only require READ access to the directory.

Setting up Group Calendar—Internal Directory Only

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. If you entered all of the commands in the allinone.html file, you already entered the Group Calendar URLs.

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

- **Mailroutingaddress** specifies where users receive email (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**.
- **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" "ldapurl" "options"
```

If you are using Active Directory, refer to the Synq Information website and access the *User Guide* for configuration and installation directions.

The **Url Add** command is domain-specific. These examples add the URL to your primary domain (miDomainName=primary). Adding the URL to delegated domains is explained in Configuring Calendar Options for Domains on page 192.

Traffic running through Calendar URLs only require READ access to the directory.

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. This URL uses 127.0.0.1 (localhost), replace this if your LDAP server is external:

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

The system LDIF uses **miloginid** to identify the user, not **uid**. In fact, the LDIF does not contain a **uid** attribute 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 groups, possibly on different servers. If you choose, replace *Group Lookup* with a custom name for this lookup. This URL uses 127.0.0.1 (localhost), replace this if your LDAP server is external:

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

3. To allow for exact matching, entering the following commands, one for **User** matching, and one for **Group** matching. These commands add an extra layer of checking when you have many users, groups, or resources and may have name conflicts. If you choose, replace *User/Group Exact Match* with a custom name for this lookup. This URL uses 127.0.0.1 (localhost), replace this if your LDAP server is external:

```
hostname.com> url add groupcalendar:matchuser "User Exact Match""ldap://
127.0.0.1:389/
ou=domains,o=corp?cn?sub?(&(|(objectclass=person)(objectclass=inetorgperso
n)(objectclass=mirapointUser))(miloginid=$(cn))""(uidalias=miloginid)"
OK Completed

hostname.com> url add groupcalendar:matchgroup "Group Exact Match""ldap://
127.0.0.1:389/
ou=domains,o=corp?cn?sub?(&(objectclass=mailgroup)(mail=$(cn)))"
"(cnalias=mail)"
OK Completed
```

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 deletes the URL you added in step 1:

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

4. 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.

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

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

1. Go to **Home > Domains > Calendar > Resources**. In the **Resourcegreoup 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.

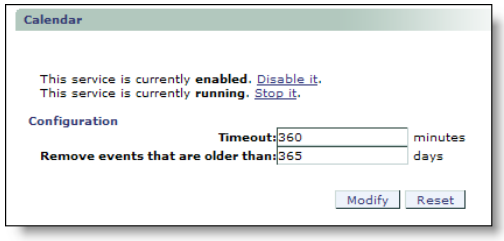
2. Specify the following for each resource (meeting rooms, equipment such as projectors, and so forth) that you want to make available for calendar users. This information is added to your LDAP database.

   - **Fullname**—The name of the resource as you want it to appear in the **Choose a Resource** drop-down menu 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: The resource entries are made available in the calendar **Schedules** tab **Choose a Resource** drop-down menu; 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. Idle WebCal connections are disconnected when the idle timeout is reached.

4. 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.



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

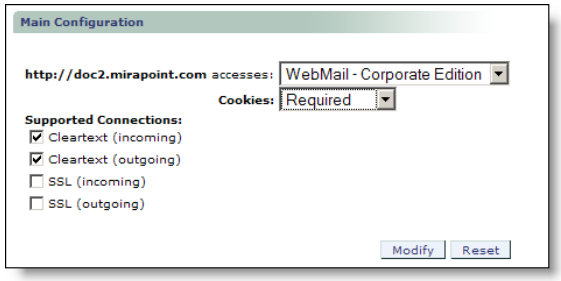
There are many Calendar defaults that you can set on a per-domain basis using the **Domains** menu **Calendar** pages for a selected domain. for full details on these defaults, see Configuring Calendar Options for Domains on page 192 in the Administration Tasks part of this book.

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.

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 menu for the **http://<hostname.domain.com> accesses** option.



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

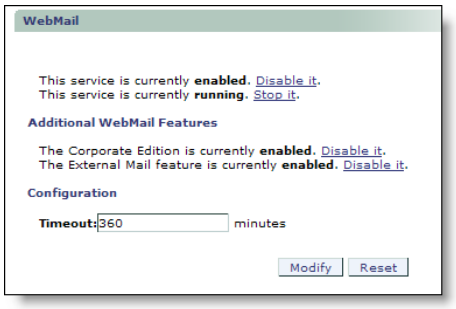
2. Also on the **HTTP > Main Configuration** page, protect WebMail session IDs by selecting **Required** for the **Cookies** option. This prevents users from unintentionally giving access to their mail by copying and pasting their session ID into an email.

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.

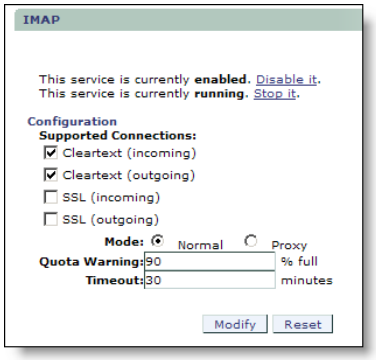


5. If the WebMail service is disabled, click **Enable it**. If the service is stopped, click **Start it**.

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. 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.

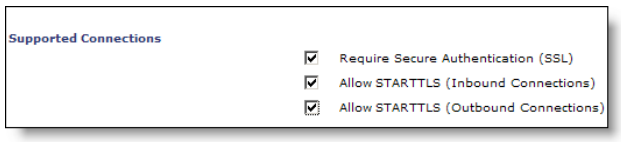
Use the defaults for options not mentioned in this procedure.

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.

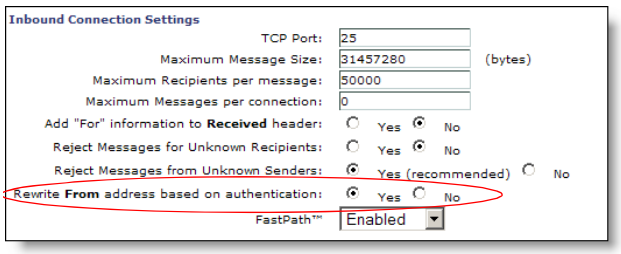
2. In the **Supported Connections** area:

   - **Require Secure Authentication (SSL)—Select.** All communications must be authenticated through the AUTH login (SMTP AUTH RFC 2554).
   - **Allow STARTTLS (Inbound Connections)—Select.** Encrypted incoming connections are supported.
   - **Allow STARTTLS (Outbound Connections)—Select.** Outgoing connections are encrypted.



3. In the **Inbound Connection Settings** area:

   - **Rewrite From address based on authentication—Select.** 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.



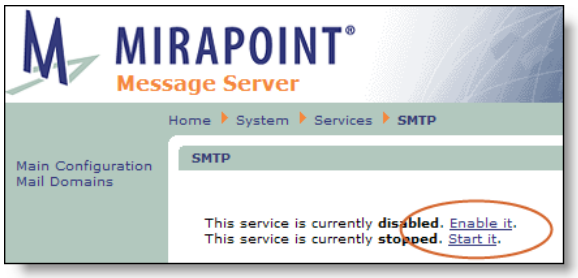
4. Accept the default settings in these areas of the page:

   - **Outbound Connection Settings**
   - **SMTP Authentication Settings**

- **Mail Queue Settings**

5. In the **Routing Settings** area:
   - **Use LDAP Routing**—Accept the default, **Never**. Routing will be done by the RazorGates.
   - **When using LDAP Routing, use**—Accept the default, **A** record.
   - **Local Message Router**—Type the symbolic hostname described in DNS Records Suggested for MMS Multi-Tier Configuration on page 81.
   - **Outbound Message Router**—Type the symbolic hostname described in DNS Records Suggested for MMS Multi-Tier Configuration on page 81.
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.

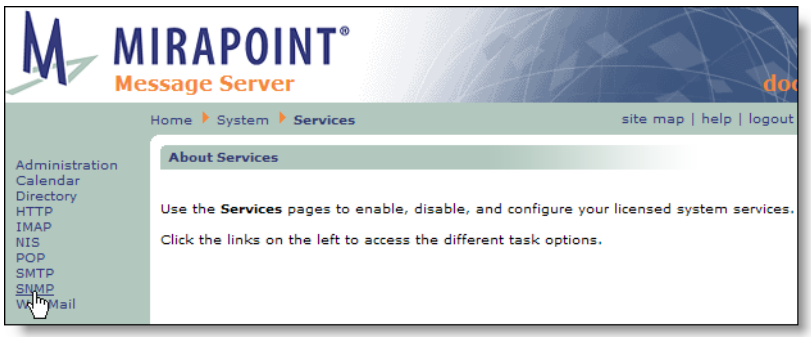
8. Click **SMTP** in the top navigation bar to return to the main **SMTP** service page. Click **Enable it**; click **Start it**.



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. 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**.



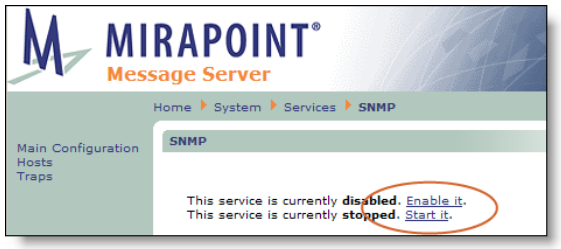
2. At this point, most services have already been enabled and started, the following might still need attention.

- **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
  - Tivioli: Defaults to version 3
  - Veritas: Defaults to version 2

For more information about these Data Management Applications (DMAs), see NDMP Backup Solutions on page 371.

- **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.

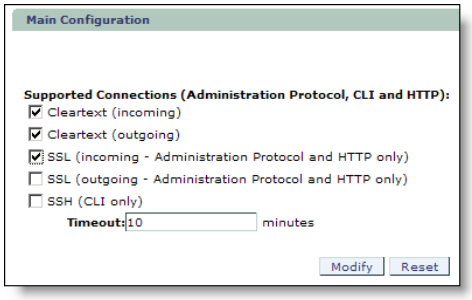
To learn more about SNMP see Monitoring External Systems via SNMP on page 176.



Resetting the Administration Timeout

Setting the timeout to 60 minutes is recommended for the configuration procedures; however, once you are done, you will 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 Message Server Setup for Multi-Tier

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.

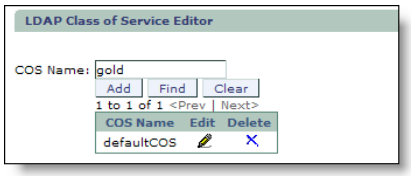
Refresh the Administration Suite

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—Internal Directory Only

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**.



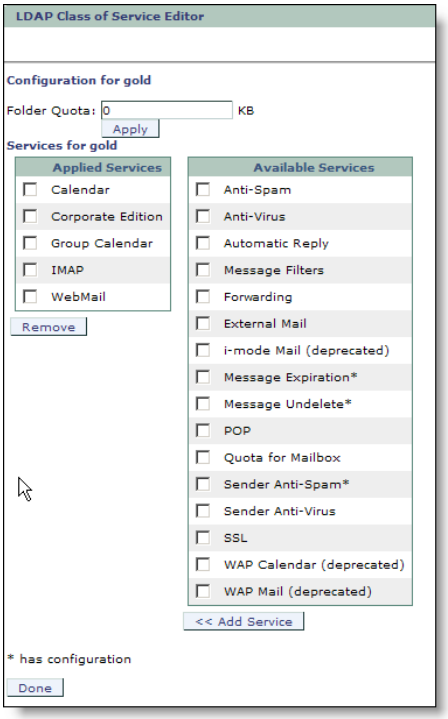
2. Click the **Edit** icon for the **gold** COS to open the **COS Editor** page. For this test, set the **Folder Quota** option at 1024 KB, select these services for the COS (Junkmail Manager may not be available):

   - **Anti-Spam**—Inbound antispam scanning
   - **Anti-Virus**—Inbound antivirus scanning
   - **Automatic Reply**—WebMail auto-reply
   - **Calendar**—WebCal Direct Standard Edition (Personal)
   - **Corporate Edition**—WebMail/Group Calendar Corporate Edition
   - **Message Filters**—WebMail message filters
   - **Forwarding**—WebMail mail forwarding (vacation mail)
   - **External Mail**—WebMail External POP mail
   - **Group Calendar**—WebCal Direct Standard Edition (Group)
   - **IMAP**—Message sending and receiving
   - **Junkmail Manager (JMM)**—Spam mail management
   - **POP**—Message sending and receiving
   - **Quota for Mailbox**—Quota setting
   - **SSL**—HTTPS secure connections
   - **WebMail**—WebMail Direct Standard Edition

   Click **Add Service**.

You will have to make additional specifications, if Junk Mail Manger is used:

- **Junk Mail Message Expire**—10 days (suggested).
- **JMM Message Expire**—10 days (suggested).
- **JMM Mailbox Quota**—1024 KB (suggested).



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

Create a Delegated Domain

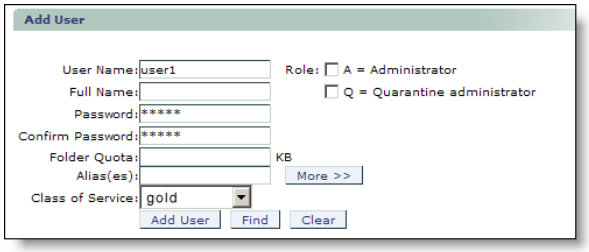
Mirapoint recommends creating a delegated domain in all cases (even if you intend to use only one domain on your MMS).

Go to **Home > Domains > Administration** and enter a **Domain Name**, for example mail.example.com. You can set a limit on the domain's disk quota and user limit. Assign the domain the **gold** COS that you created. Enter the JMM server hostname as the **JMM Host**. Click **Add Domain**.
Result: The domain displays in the status table at bottom and is selected for modifications.

Create User Accounts—Internal Directory Only

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

1. Go to **Home > Domains > Users** (if you just created a delegated domain, all you need to do is click **Users** in the left menu). Verify at the bottom left of the page that you are in the delegated domain that you created.
2. Create the first test account: enter ***user1*** in the **User Name**, **Full Name**, and **Password** options, and click **Add User.**



3. Create a second test account: enter ***user2*** in the **User Name**, **Full Name**, and **Password** options, and click **Add User.**
4. In order to test your Address Book and Calendar setup you also need to create two users in the primary domain. Go to **Home > Domains > Administration** and select the **<primary>** domain. Click **Users** in the left menu and create two more users, ***user3*** and ***user4***, following steps 2 and 3 above.

Send a Test Message

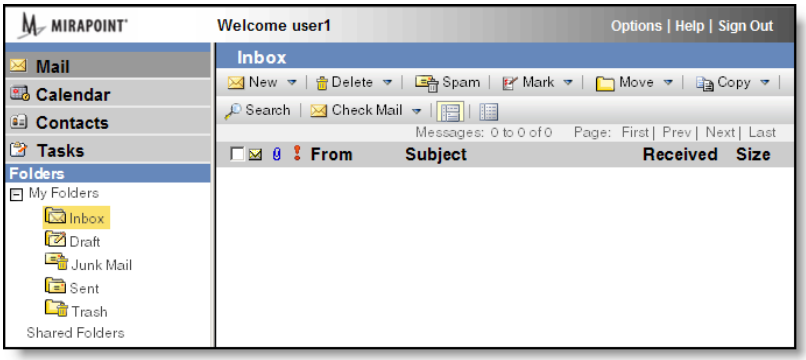
Before you send a test message, finish one of the configurations described in the *Mirapoint RazorGate Administrator's Guide* or else otherwise ensure that all routing is set up properly.

To send a test message:

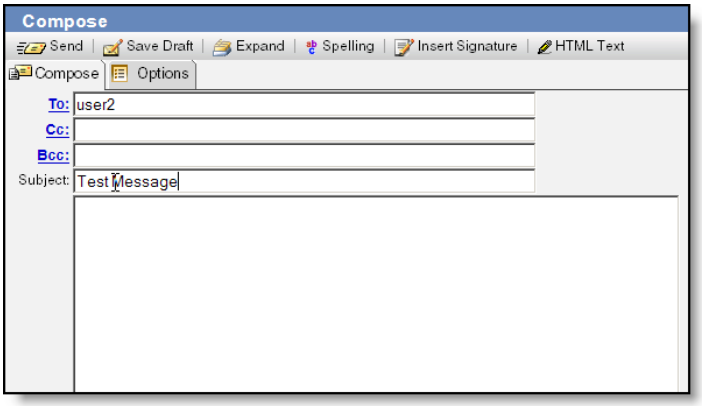
1. Open your Message Server's URL in a web browser; for example, **http://** ***hostname.domain.com***. Since you set WebMail as the default access, it should open to WebMail.
2. For the Internal Directory setup, log into WebMail with the **user1** username plus the delegated domain name (for example: user1@mail.example.com) and password. For the Active Directory setup, log in as a configured Active Directory user (you must know the username and password); verify that the user is created on the Message Server after login.

In the following examples, Corporate Edition WebMail is shown.

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

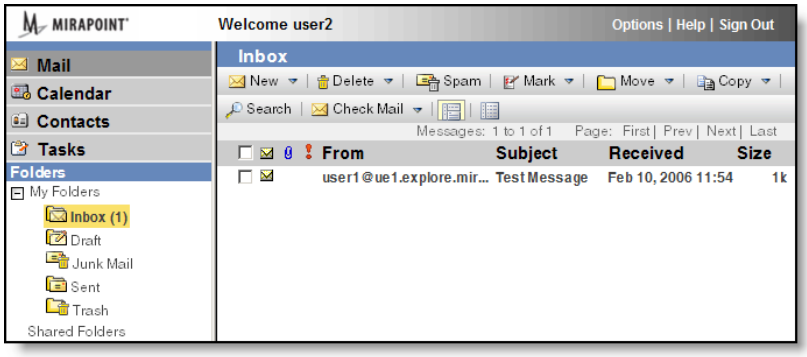


4. Address the message to **user2@*hostname.domain*.com** for the Internal Directory setup; to a configured Active Directory user for the Active Directory setup. Click **Send**.



Receive a Test Message

To receive the test message, log into WebMail with the **user2** username plus delegated domain, and password (Internal Directory); or the Active Directory username to which you sent mail. The test message should be listed in the user'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 112.

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 **use3** 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 menu 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—Internal Directory Only

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

1. Log into WebMail with the **user3** 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 **user4** 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 **use4** 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

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

Adding a Multi-Listener

You must use the CLI to add multi-listeners; see Accessing the Command Line Interface on page 26 for details.

Imagine that you want to set up a Message Server that accepts email from the Internet on the conventional SMTP port 25 at the server's public IP address, 10.1.1.25 for example. This is the default for message transfer. And you also want

to accept mail submissions on the agreed-upon port 587; see RFC 2476. Here is the command needed:

```
Smtp Addlistener *:587
```

Repeat the command to add port 465, if desired.

See Configuring Multi-Listeners on page 323 or, using the CLI, **Help About Smtp**, for more information.

Troubleshooting

This section provides some troubleshooting tips.

LDAP Errors

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 "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 "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.

Getting the Active Directory bindDN

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

1. Connect to your Exchange 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:

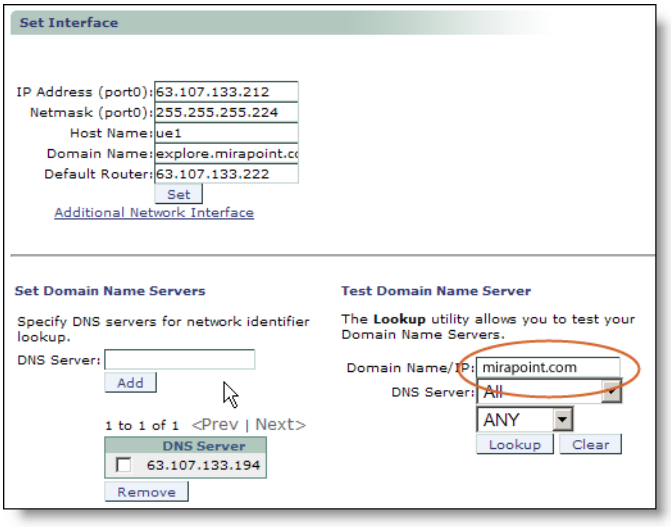
   ```
   dn: CN=Administrator, CN=Users, DC=adhostname, DC=yourdomain, DC=com
   ```

   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, the entire DN is specified as the **bind DN**: **CN=Administrator, CN=Users, DC=adhostname, DC=yourdomain, DC=com**.

Test Message Send Fails

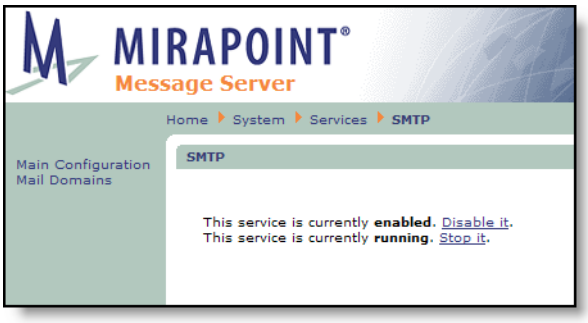
If you cannot send test messages between user accounts on your Message Server, check the following:

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.



   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, Message Server Setup for Multi-Tier

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 233 and Setting Up Message Expiration on page 234 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 Business Continuity Tasks on page 369 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 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.

4 Multi-Tier, Multi-Appliance Deployments

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 Site Planning Guide*.

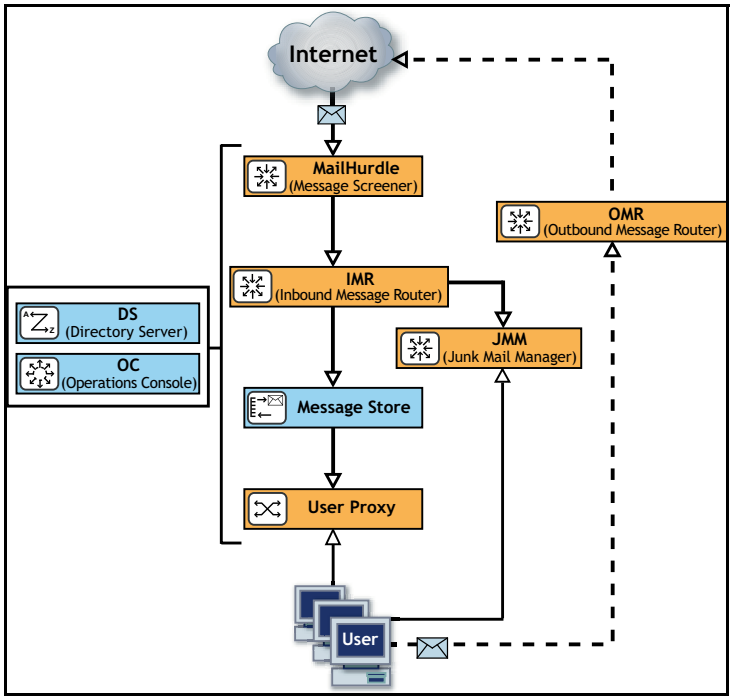


Figure 4 Multi-tier Deployment Example

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) servers configured with needed records ("A," "MX," "PTR," and "CNAME"). For more information, see DNS Records Recommended for a Multi-Tier Deployment on page 22.
  - Lightweight Directory Access Protocol (LDAP) setup
  - License requirements defined (licenses are implementation specific)
  - Backup requirements defined
  - Secure Sockets Layer (SSL) certificates purchased
  - Hardware installation
  - 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 (MOC)
- **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 section next, 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)

These procedures are described in the order in which a message comes through the system. If you are setting up a multi-tier deployment Mirapoint recommends that you set up the Directory Services, Message Store and Calendar functions first, and then the Security Screening and Routing functions.

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

Delegated domains are amongst the last things to be configured.

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 27 before continuing.

Accessing the Command Line Interface (CLI)

To access the CLI, connect to your appliance using telnet in a command window, and log in as the Administrator:

```
Start > Run: telnet hostname.domain.com
OK hostname.domain.com admind 3.10 server ready
User: Administrator
Password: password
OK User logged in
```

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. Click **Install Licenses** if needed. Which licenses you need for a particular appliance depends on the functions that it will perform in your multi-tier deployment.
In the CLI, type:

```
hostname.com> license list
OK Completed

hostname.com> license fetch
OK Completed
```

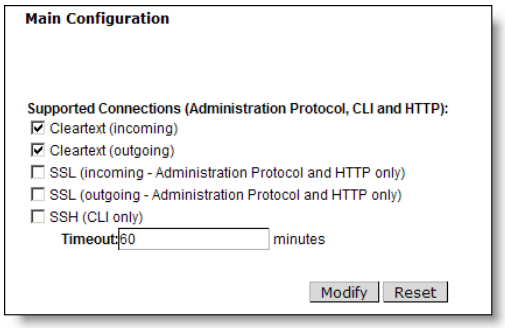
The MailHurdle license does not display; it is part of the Anti-Spam license.

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 will 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 will want to change it back to 10 minutes once you are done.



In the CLI, type:

```
hostname.com> admin set timeout 60
OK Completed
```

Security Screening (RazorGate Appliances)

Configure the security screening functions on tiers of RazorGates:

- MailHurdle
- Message Screening
- Junk Mail Manager

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 do not need to perform these preparation steps. Go directly to Configuring MailHurdle next.

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 email. 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 email during the transition phase, senders can send a short message first to prime MailHurdle with the appropriate triplet. The priming

email 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 email 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). For more information about the two scanners, see Principal Edition vs. Signature Edition on page 304.
- 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.

   Mirapoint recommends that you accept the default **Auto-Clean** (**Delete**) option. You could specify the email 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 emails, 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 290 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.

   Mirapoint recommends that you accept the default spam threshold of 50. Higher values incur more false positives; lower values miss spam.

   The **Add Warning Flag** option is useful for delivery to POP users who lack a Junkmail folder.

   The **Junk Mail Explanation** can be enabled to allow users to view the detailed headers that explain the spam scores.

   This option only displays for **Principal Edition Antispam**.

   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.

   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 will 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.

Configuring Banner Delay

You can configure your system to delay greeting acknowledgement during the SMTP chat session. Senders who violate the RFC by sending data before the greeting acknowledgement can be rejected. You must configure Banner Delay using

the CLI; for information on accessing the CLI, see Accessing the Command Line Interface (CLI) on page 118.

Mirapoint recommends turning banner delay **On** if you are not using MailHurdle or you are using MailHurdle in SuspectList mode (see **Help About Mtaverify** in the CLI help for details).

To do this, enter these CLI **SMTP** commands:

Enable banner delay (default is **Off**).

```
hostname.com> Smtp Set Bannerdelay On
```

Sets banner delay time in seconds (default is 5). Setting delay to **0** sets the banner delay time to the default value, 5 seconds.

```
hostname.com> Smtp Set Bannerdelaytime 5
```

Use **Smtp Get Bannerdelay** and **Smtp Get Bannerdelaytime** to retrieve the configured delay state and time.

Banner delay is not subject to sender whitelisting. However, messages originating locally from the receiving server and senders on the relay list are exempted from banner delay.

These commands apply system wide and are not domain sensitive.

Configuring Second Scan for Anti-Spam

You can now run both Signature Edition (RAPID AS) and Principal Edition antispam scans on the same server. Administrator's can choose to run both scans on all messages or to run the second scan only for messages classified as "bulk" by RAPID. You must configure Second Scan using the CLI; for information on accessing the CLI, see Accessing the Command Line Interface (CLI) on page 118.

Multienginebulkonly **Off** setting (default) configures both licensed scanners to run for all messages. The higher returned score is used to determine the UCE score in the header X-Junkmail-Status and X-Junkmail:UCE headers.

Multienginebulkonly **On** setting configures second scan to run only for messages tagged as bulk by Signature Edition (UCE scores between 50 and 60). For these bulk classified messages, the result of the second scan overrides the bulk tag.

If you run this command with only one Antispam scanner licensed, it has no effect until the second scanner is licensed. If two scanners are licensed but this option is **Off**, then the larger spam score wins, which can increase false positives. Running both scanners is resource intensive, but much less so with this option **On**.

Mirapoint recommends setting Multienginebulkonly to **On** if you consider that your two-engine spam scanning is taking too long.

To do this, enter this CLI **UCE** commands:

```
hostname.com> Uce Setoption Multienginebulkonly (Domain=local) On
```

Use **Uce Getoption Multienginebulkonly** (**Domain=local**) to retrieve the setting.

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 26.

   Junk Mail Manager and LDAP Routing must be licensed on the appliance to configure JMM.

2. On the **Set Junk Mail Manager** page, click the **Enable it** button. When 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 drop-down menu.
   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 email 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 are 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 are 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 SNMP service, if applicable. Do not start the SMTP service at this time. Click **Next** to continue.
10. If you do not have the Junk Mail Manager license, and do have the Mail Routing license, the **Proxies** page displays. You can do the following:
    a. If IMAP users connect through this system, set IMAP proxy.
    b. If POP users connect through this system, set POP proxy.
    c. If WebMail users connect through this system, set HTTP proxy.
11. On the **Service Reporting** page, verify that your service reporting options are correct. Click **Next** to continue.
12. 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 are 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 quarantine records for JMM as described in Junk Mail Manager LDAP Records on page 243.
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**.

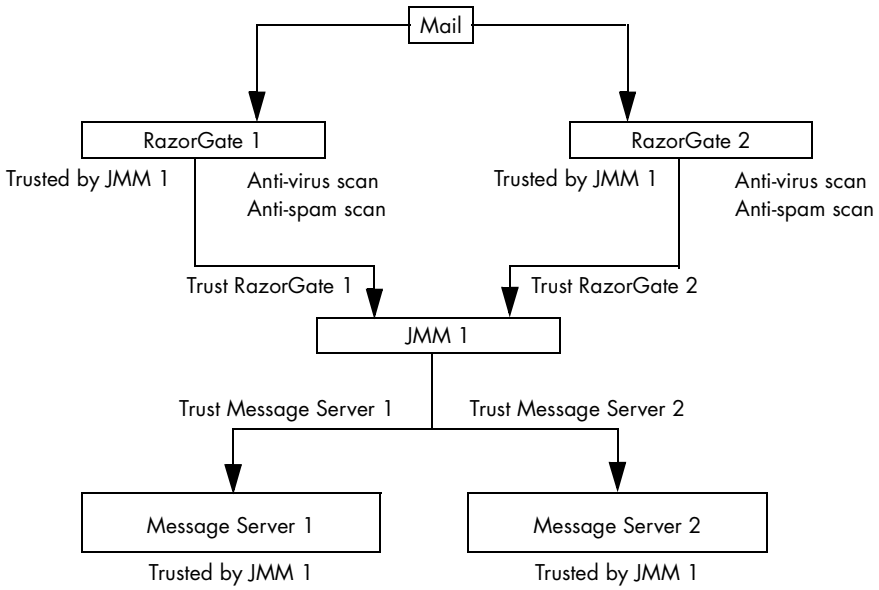


Figure 5 Trusted Host Relationships In A Multi-Tier Environment

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 Exchange with Active Directory, or by a Mirapoint LDAP Directory Server or Message Server with Internal LDAP.

To set up the Mirapoint Directory Server on a tier of Mirapoint appliances, complete the procedure described in LDAP Lookup on page 127.

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: antispam
miService: antivirus
miService: autoreply
```

```
miService: calendar
miService: enterpriseui
miService: filter
miService: forward
miService: getmail
miService: groupcalendar
miService: imap
miService: junkmailmanager
miService: msgexpiration
miService: msgundelete
miService: pop
miService: quota
miService: ssl
miService: webmail
objectclass: miClassOfService
cn: defaultCOS
miMailquota: 0
miMmailexpirepolicy: QTNBOX.* 14 I
miDefaultjunkmailfilter:: IOBNaXJhcG9pbnQtRmlsdGVyLTEuMAOKZmlsdGV
 yICJTeXNOZWOgSnVuayBNYWlsIFJ1bGUiIFF1YXJhbnRpbmUgIlFUTkJPWC5KdW5r
 IE1haWwiIGFsbG9mIHNOb3ANCjpVQOUgaXMgIm5vcm1hbCINCg==
```

The final two attributes are needed only for JMM, but not otherwise for COS. The **miMailexpirepolicy** 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
miQquarantinehost: 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.

```
Start > Run: telnet ldap 10144
OK ldap.example.com admind 3.10 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
- Connection Proxy
- Outbound Routing

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 120.

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 127.

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. The software asks you to **Confirm** your choice.
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 127.

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 127; 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. Under the **Test Query** heading, type a user email 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 email address.
6. 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.
7. 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.

   On the **System > Services > SMTP > Mail Domains** page, type the name of each mail domain for which this router delivers email. Give the full domain name: everything after the at-sign (@).
8. On the **Home > System > Services > SMTP > Main Configuration** page, set **Use LDAP Routing** to **For Junk Mail Manager** if this RG is JMM enabled, or to **For Local Messages** if it is not.
9. Click **SMTP** in the top navigation menu to open the **SMTP** service page and enable and start the service.

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 129.

To configure the connection proxy, follow these steps:

1. Go to **System > Services > IMAP**, for **Mode**, select the **Proxy** radio button and click Modify.
2. Go to **System > Services > POP**, for **Mode**, select the **Proxy** radio button and click Modify.
3. Go to **System > Services HTTP > Mode**, click **Proxy** (the IP address must be used to access the Administration Suite until next login). Set **Route URLs in LDAP** to **Always** for all back-end routing to be done through LDAP.

Require users to authenticate using LDAP; you must use the CLI:

```
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, email 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 email. 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 if it has not already been done.

5. On all Message Servers that will transmit email through this outbound router, set this outbound router as the OMR for SMTP. See Message Store on page 131 for instructions.

Message Store and Calendar (Mirapoint Appliances)

Configure these functions on tiers of Mirapoint appliances:

- Message Store
- Group Calendar

Message Store

To configure the message store, follow these steps:

- 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.

6. 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 127.
7. 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 127, otherwise type the suffix of your LDAP database.
8. 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.
9. Switch to the CLI. Enable LDAP autoprovisioning of new users:

   ```
   Ldap Set Autoprovision On
   ```

10. Enable LDAP-related features on this server, including autoreply, exceptions, forward, password update, WebMail preferences, and **ldapgui** with this one command:

    ```
    Conf Enable Ldapall
    ```

11. If this Message Server is going to autoprovision Junk Mail Manager accounts, enter this command:

    ```
    Conf Enable Ldapgui-jmm
    ```

12. Require users to authenticate using LDAP:

    ```
    Auth Set Default Plaintext:Ldap
    ```

13. To allow transmission of email 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
    ```

14. 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
```

15. On the **Home > System Services > SMTP** page, enable and start SMTP service, or do it in the CLI:

```
Service Enable Smtp
Service Start Smtp
```

16. 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

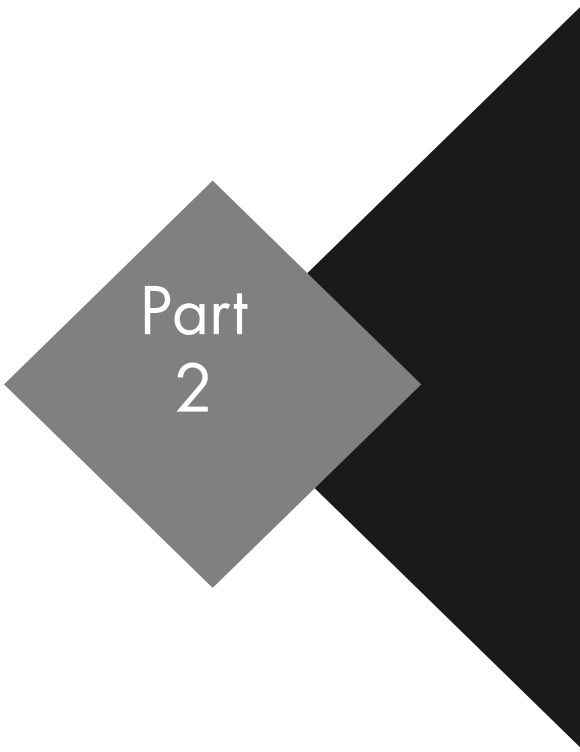
In a multi-tier environment, you must have the Mail Routing license in order for Group Calendar to work. To configure WebCal group calendar, follow these steps:

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 192 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



5 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. Includes Reading Message Envelopes and Headers.
- 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.

If you are using RazorGate software on an IBM BladeCenter® appliance, refer to your hardware documentation for monitoring information. Monitoring is turned off for RazorGates on blade servers.

Internal Distribution Lists for Monitoring

The default distribution lists (DLs) shown in Table 6 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.

DLs beginning with the word *system* are reserved for Mirapoint use. You cannot use "system" as the initial name in a custom DL.

Table 6 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 174. 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). 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. 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 335. 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 335. This list includes Administrator by default and is reserved for Mirapoint use.
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. 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

Performance Gauges

The performance gauges shown in Figure 6 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**—The run-queue of the system averaged over the past minute. This represents the number of processes waiting for resources. Busy systems range from 20 to 50. Anything over 65 is considered overloaded. If you receive an alert based on SYSTEM.LOAD, check Performance Graphs.
- **Mailq Size**—The number of messages in process of being routed to another message transfer agent (OMR) or to a local mail store (IMR).

You can view the averages over the last day or hour, or select the **Now** view to display an instant update.

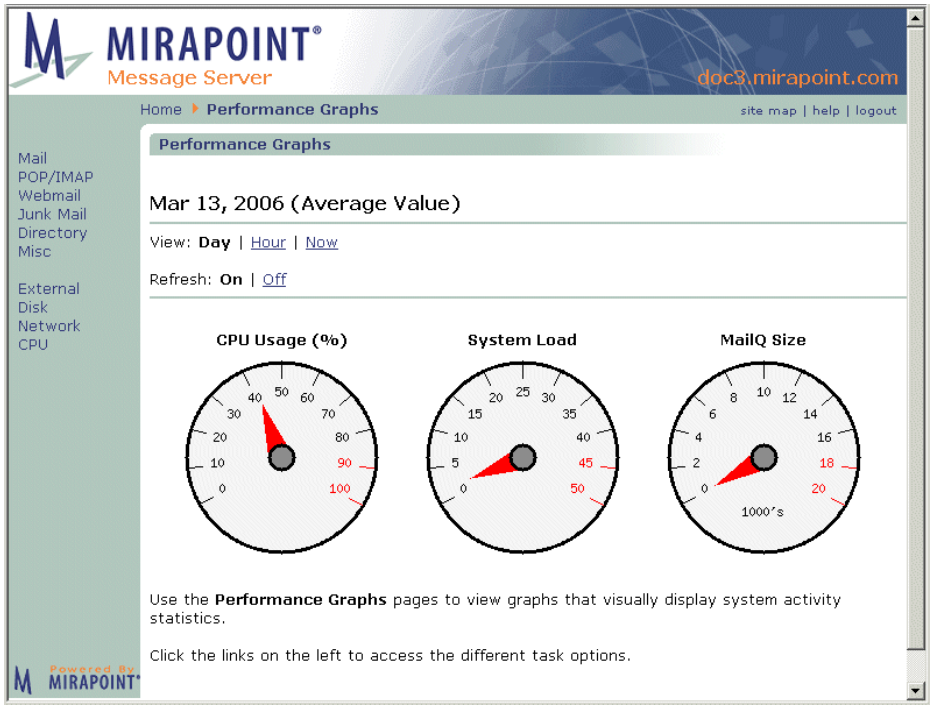


Figure 6 Performance Graphs: Gauges

CPU Usage

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.

System Load

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.

On a Mirapoint system, high system load is usually caused by a large number of messages in the queue, so first look at **Performance Graphs > Mail**. On a RazorGate system, high system load could be caused by a spam or virus attack, so check **Performance Graphs > Junk Mail**. Network connections or degraded RAID disk could be the cause, so check all those pages, then everything else

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.

Mailq Size

The size of the queue will vary from customer to customer. Administrators should monitor the queue size to determine what is appropriate for their installation. In general, you want a consistent value (a few hundred or less) over time. If you find your mailq size is slowly growing over time, this could be an artifact of changes in your company's mail usage. You might want to consider purchasing additional resources. Some times, you will find a spike (rapid and short increase) in the mailq size. This can mean several things.

1. You are the victim of a spammer.
2. A common recipient domain is temporarily down. Your company might send a large number of messages to a domain outside your control requiring you to queue messages for your users until the destination site is running again. 3. Network failures. Runtime services, such as DNS or LDAP, are not accessible.

Mirapoint appliances offer commands to further interrogate your mailq to determine root cause for these spikes. For details see **Help About Mailq** in the CLI.

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.

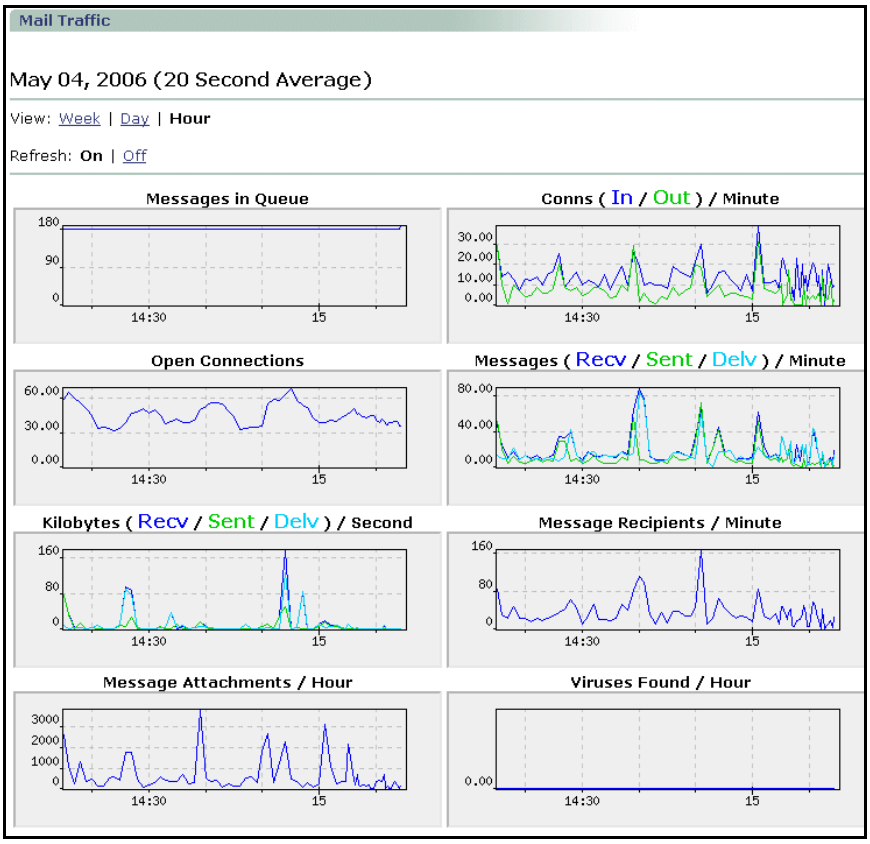


Figure 7 Mail Performance Graphs

Table 7 Mail Traffic Graphs

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.

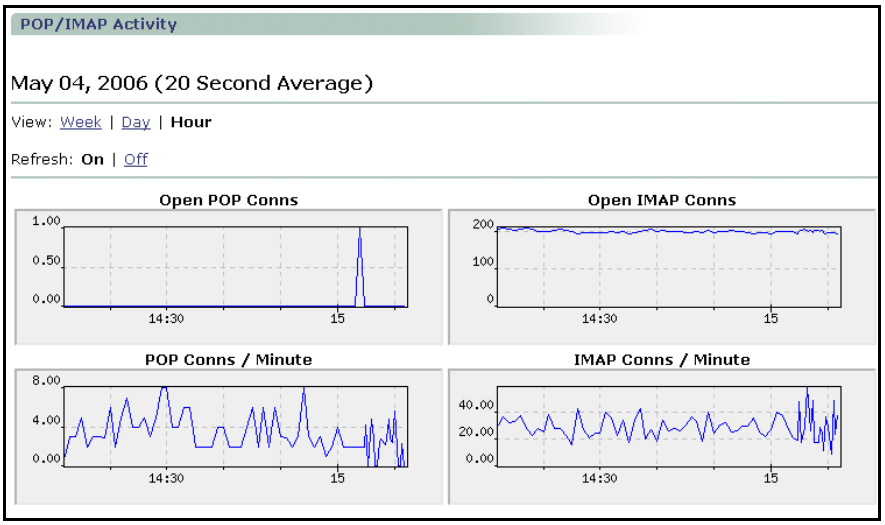


Figure 8 POP/IMAP Performance Graphs

Table 8 POP/IMAP Activity Graphs

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 Activitiy** 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.

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.)

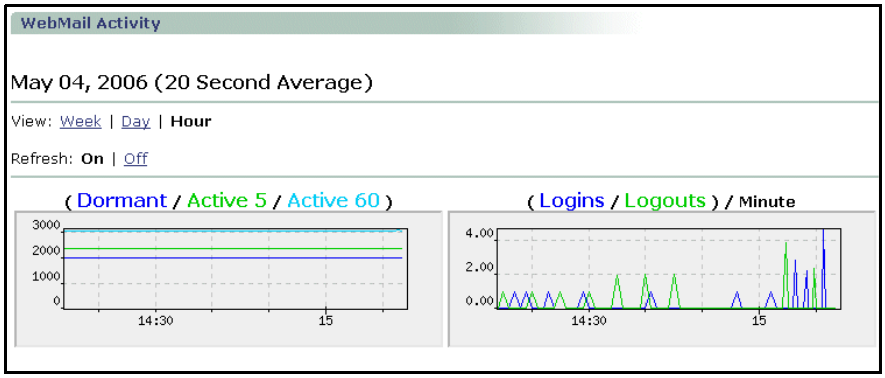


Figure 9 WebMail Performance Graphs

WebMail graphs are a good way to get a baseline understanding of how users on your system are using WebMail.

Table 9 WebMail Activity Graphs

Graph	Description
(**Dormant** / **Active 5** / Active 60)	Dormant: The number of sessions that have been idle for more than 60 minutes and less than the WebMail timeout setting, usually 360 minutes. Active 5: The number of sessions that were active within the last 5 minutes. 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.

Table 9 WebMail Activity Graphs (Continued)

Graph	Description
(**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.

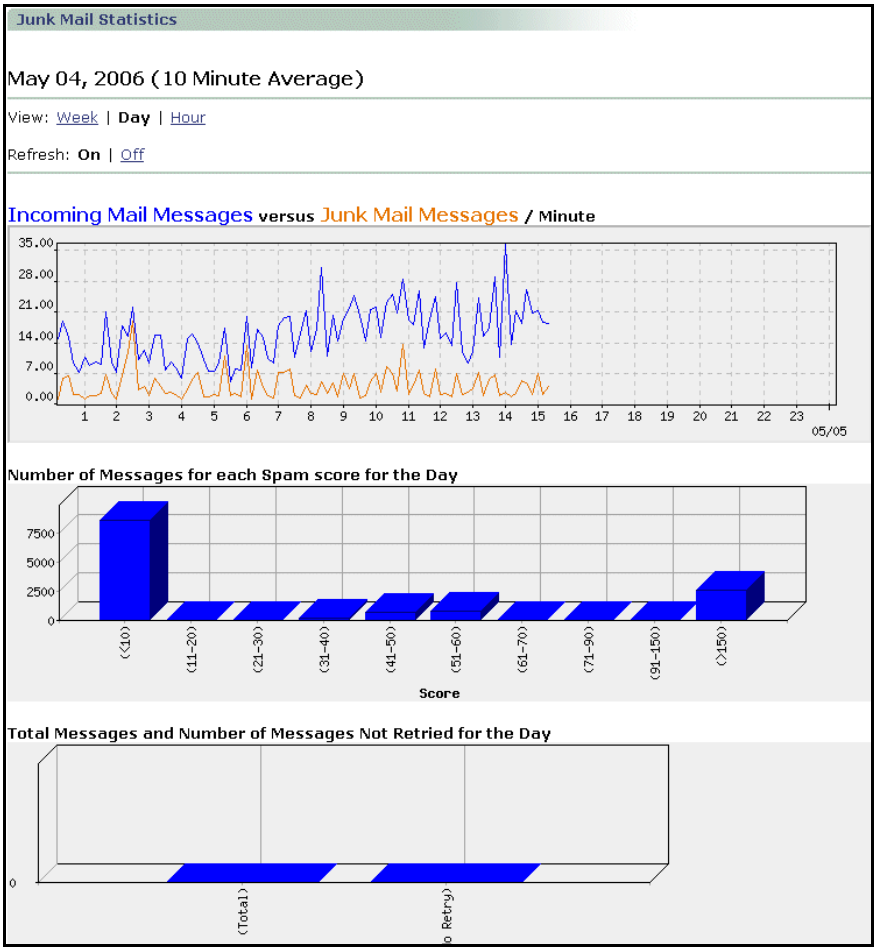


Figure 10 Junkmail Performance Graphs, Detail

Table 10 Junkmail Statistics Graphs

Graph	Description
Incoming Mail Messages versus Junk Mail Messages	This graph shows: ❖ 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 240.
Total Messages and Number of Messages Not Retried 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 282.

In the **Total Messages and Number of Messages Not Retried 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 236.

You can also look for spam attacks in the junk mail 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.

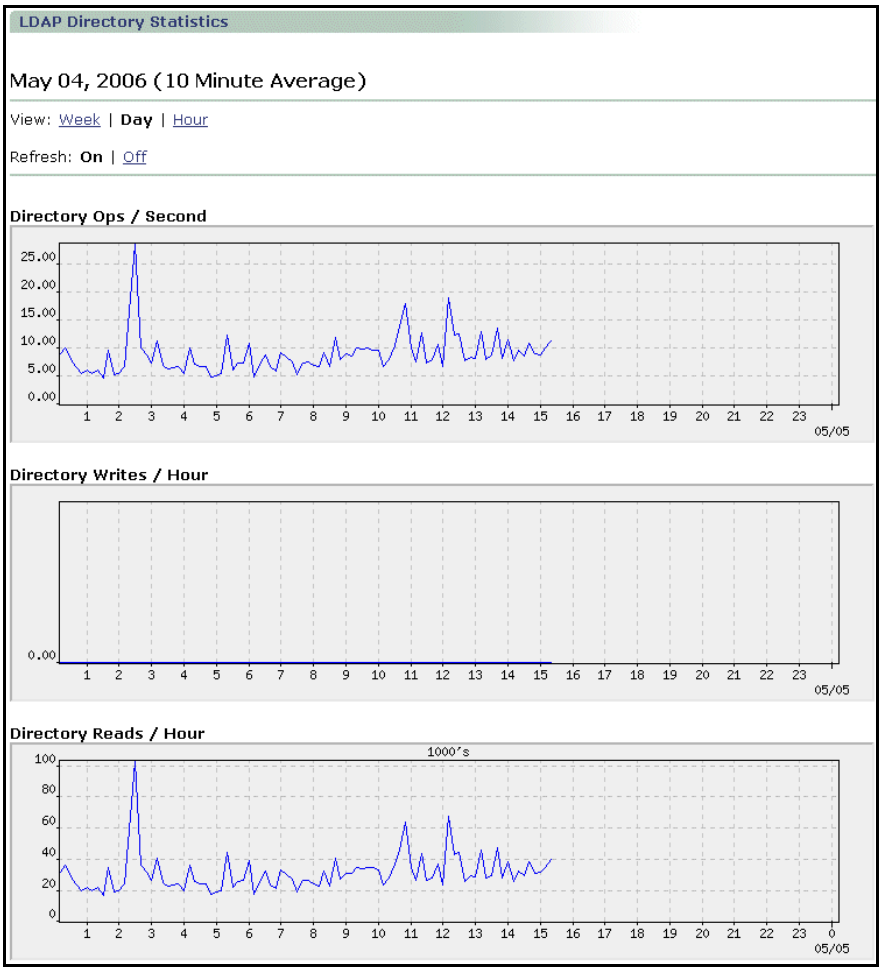


Figure 11 Directory Performance Graphs

Table 11 LDAP Directory Statistics Graphs

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
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 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 (for example, 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.

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 12 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. These 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 server

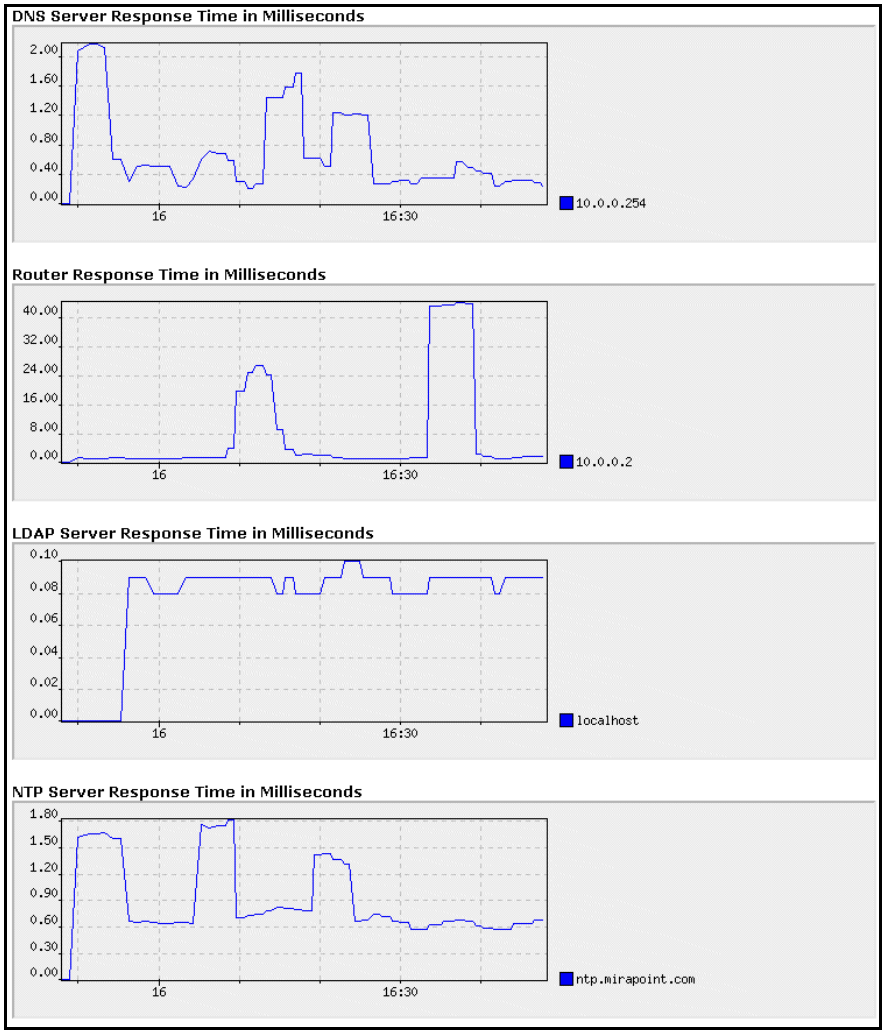


Figure 12 External Performance Graphs (Detail)

Table 13 External Server Monitoring Graphs

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 mail store 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.
LDAP Server Response Time in Milliseconds	Response time of each external Lightweight Directory Access Protocol (LDAP) server.
NIS Server Response Time in Milliseconds	(MOS 3 ONLY) Response time of each Network Information Service (NIS) server.
RBL Server Response Time in Milliseconds	Response time of each Real-time Blackhole List (RBL) server.
Kerb4 Server Response Time in Milliseconds	Response time of each Kerberos 4 authentication server.
Kerb5 Server Response Time in Milliseconds	Response time of each Kerberos 5 authentication server.
Radius Server Response Time in Milliseconds	Response time of each Radius authentication server.
OMR Response Time in Milliseconds	Response time of each outbound message router (OMR).
LMR Response Time in Milliseconds	Response time of each local message router (LMR).

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 network monitoring (**Mon Disable Netmonping**), all response times in the external servers area go flat-lined. For details, see **Help Mon Disable** 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.

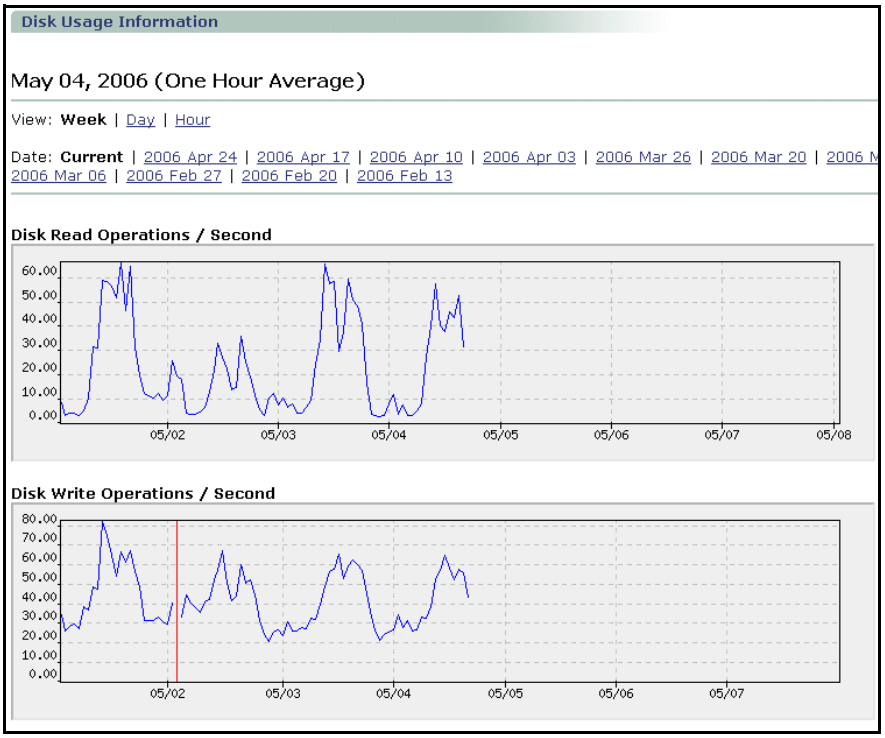


Figure 13 Disk Performance Graphs

Table 14 Disk Usage Information Graphs

Graph	Description
Disk Read Operations/ Second	Number of disk read operations per second for one day. Measures block transfers.

Table 14 Disk Usage Information Graphs (Continued)

Graph	Description
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 14. For explanations of the possible pie chart categories, see Pie-Chart Categories on page 139.

Figure 14 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.

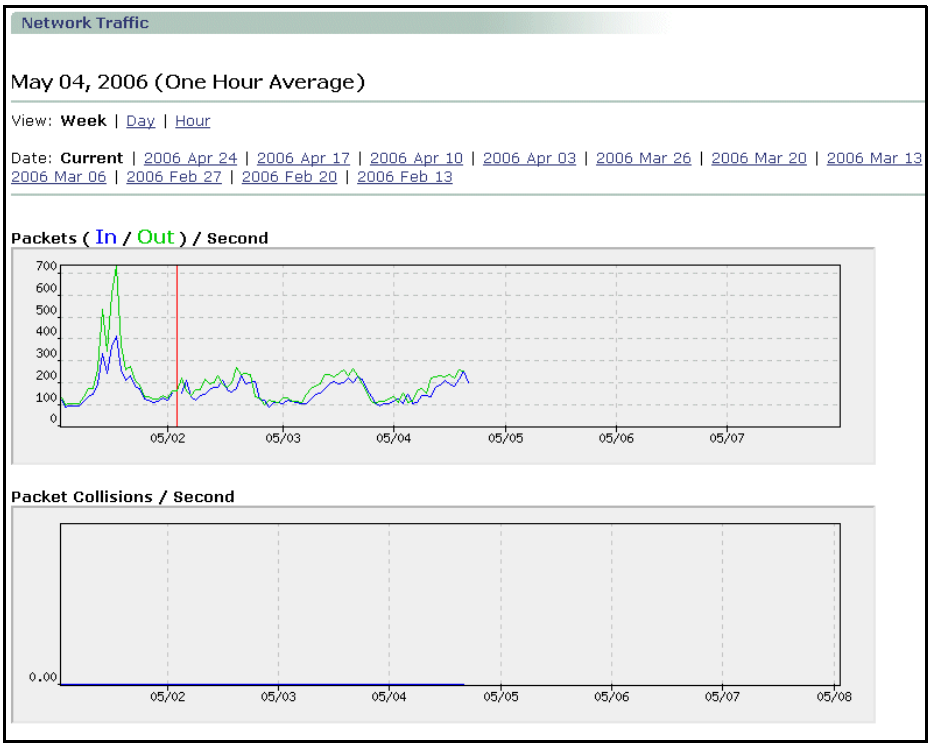


Figure 15 Network Performance Graphs Detail

Table 15 Network Traffic Graphs

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.

Table 15 Network Traffic Graphs (Continued)

Graph	Description
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 139.

The **Network Traffic** pie charts give you information about what's using up network traffic. These charts are shown in Figure 16. For explanations of the possible pie chart categories, see Pie-Chart Categories on page 139.

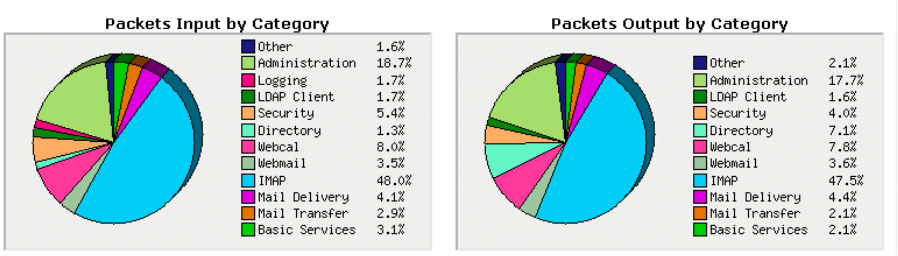


Figure 16 Network Traffic Pie Charts

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. For information on setting the NIC speed or duplex, see **Help Netif Set** in the CLI online Help.

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 139.

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.

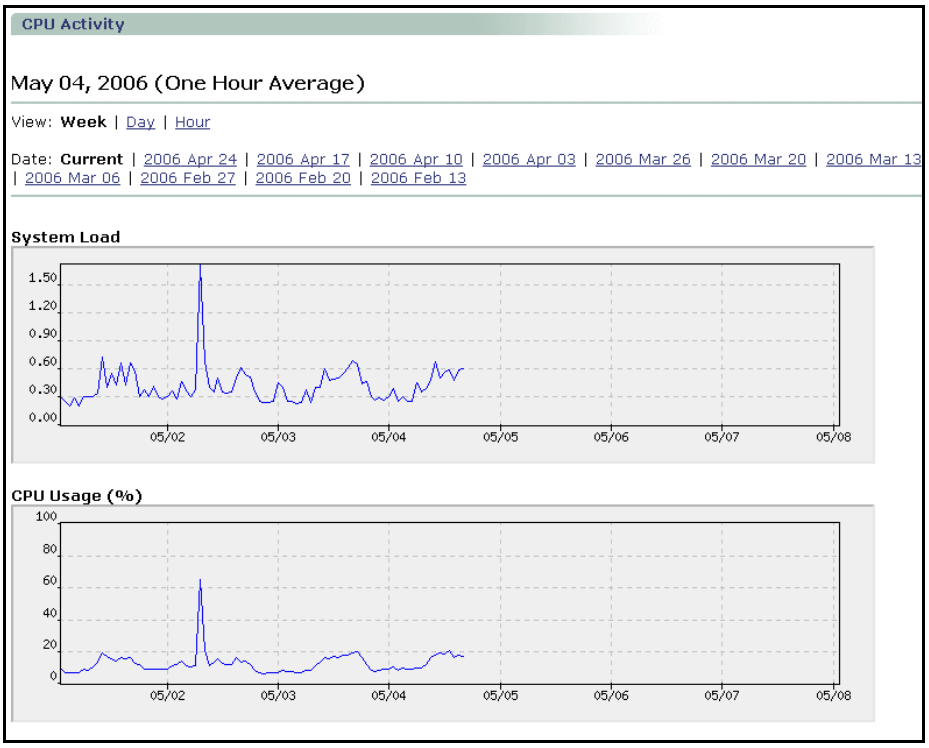


Figure 17 CPU Performance Graphs Detail

Table 16 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 139

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 139.

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 159.
- Sorting messages in the queue; see Sorting Messages in the Queue on page 160.
- Searching for messages in the queue; see Searching the Queue on page 165.

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 158.

About the Queue

Mail systems route mail through a Message Transfer Agent (MTA). MTA's accept messages from mail clients, mail enabled applications, and other MTA's. 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/Qtnbox 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 167 and Deleting the Queue for a Domain on page 167 for details.

Common Reasons Found in the Queue

When viewing a queue, especially a large queue, you will 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 162.)
- **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 will 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 18) 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 18 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 will 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 will 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.

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 160 and Searching the Queue on page 165.

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.

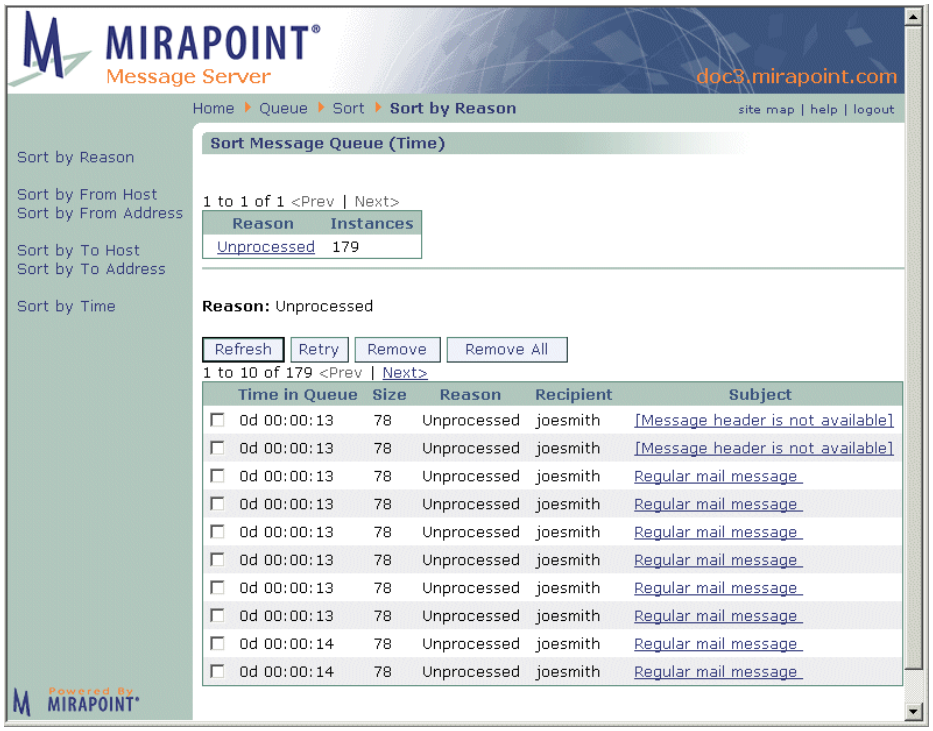


Figure 19 Queue Sort Page

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 162 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 generally, they provide additional information about the message. Mirapoint uses the following **X** headers as indicated:

- During antispam and antivirus scanning,:
  - **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.
  - **X-Junkmail**: The UCE score that the message was given by the antispam scanner that categorized it as junk mail. Example:
    `X-Junkmail: UCE(190)`
  - **X-Junkmail-Loop-ID**: Inserted by a number of different subsystems to ensure that the specific subsystem does not cause a mail loop.
  - **X-Junkmail:RBL**: The message matched an RBL host list.
  - **X-Junkmail-Info**: Provides coded explanations of why the message was categorized as spam (junk mail). This header can be disabled by your system administrator. This header only applies to the **Principal Edition** antispam scanner; to understand the codes, see The Apache SpamAssasin Project. Example:
    `X-Junkmail-Info: FORGED_RCVD_HELO,HTML_80_90,CLICK_BELOW`
  - **X-Junkmail-SD-Raw**: Indicates that the **Signature** edition antispam scanner using RAPID® technology was used.
  - **X-Junkmail-Status**: The UCE score shown over the configured default UCE threshold (see About the Antispam Scanning Rules and Threshold on page 240 for information on adjusting the default threshold) and

what host performed the scanning. Example:
`X-Junkmail-Status: score=0/50, host=mirapoint.com`

- **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-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-Virus**: Tracks the state of the virus cleaning done on a message.
- **X-old-subject**: Keeps the original subject (when the subject line has been modified).

❖ 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 whitelistto 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 antispam 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 whitelistto 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 antispam 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.

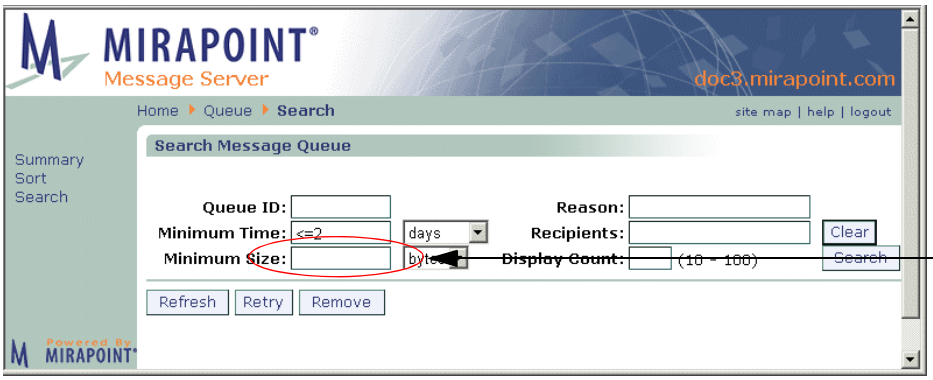


Figure 20 Queue Search Page

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 (**>=**) operator. Default Boolean operators can be overridden by prefixing the field entry with one of the other operators, such as the less than/equals (**<=**) 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 166, 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 menu 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 166.
   - **Minimum Size**—The minimum size of the message. Enter an integer and select a size unit from the drop-down menu 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 166.
   - **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 160 for more information.

Operators for Search Parameters

Definitions:

= (equals), >= (greater than or equals), <= (lesser than or equals)

Table 17 Boolean Operators

Edit Field	Default Boolean Operator	Allowable Boolean Operators
Queue ID	=	Cannot override
Minimum Time	>=	>= <= =
Minimum Size	>=	>= <= =

Table 17 Boolean Operators (Continued)

Edit Field	Default Boolean Operator	Allowable Boolean Operators
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.

You can also stop inbound mail without stopping the processing of the queue by altering the **SMTP Listen Port**. 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 19) 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. 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.

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.

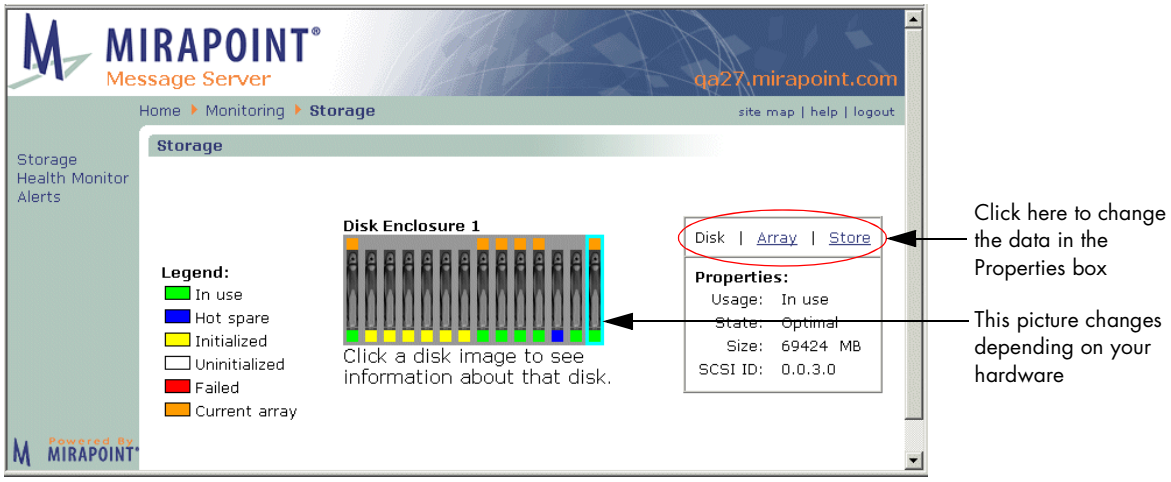


Figure 21 Monitoring > Storage Page Disk View

If your system has IDE (integrated drive electronics) storage, then the **Storage** page displays only the **Properties** data box, as shown in Figure 22.

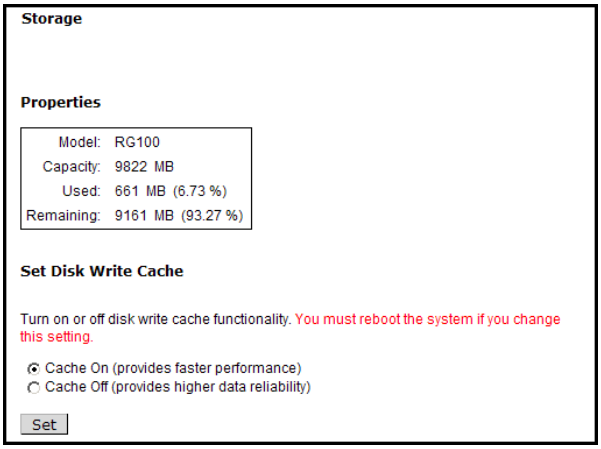


Figure 22 Monitoring IDE Storage

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.

6-Series hardware and MOS 4.x do not support direct-attach disk shelf hardware.

- 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 169 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 170 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 172 for details.

Storage Disk Data View

Each Disk Enclosure or Disk Shelf (5-Series MOS 3.x only) 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.

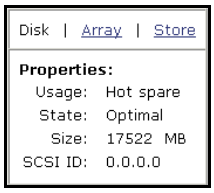


Figure 23 Monitoring > Storage Page Disk View Properties Box Detail

The following table explains the terms in the **Properties** data box for **Disk** view; see Figure 21.

A message displays if a disk has failed, or is in a missing state.

Table 18 Disk View Properties Data Box Items

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.

Table 18 Disk View Properties Data Box Items (Continued)

Item	Description
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.

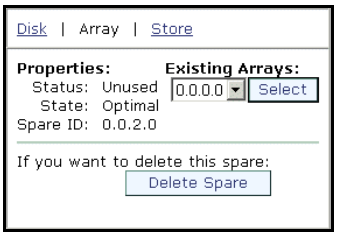


Figure 24 Monitoring > Storage Page Array View Properties Box Detail

The following table explains the terms in the **Properties** data box for the **Array** view; see Figure 21.

Table 19 Array View Properties Data Box Items

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. 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 email 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.

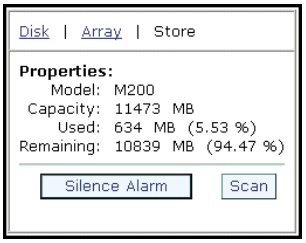


Figure 25 Monitoring > Storage Page Store View Properties Box Detail

The following table explains the terms in the **Properties** data box for the **Store** view; see Figure 21.

Table 20 Store View Properties Data Box Items

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.

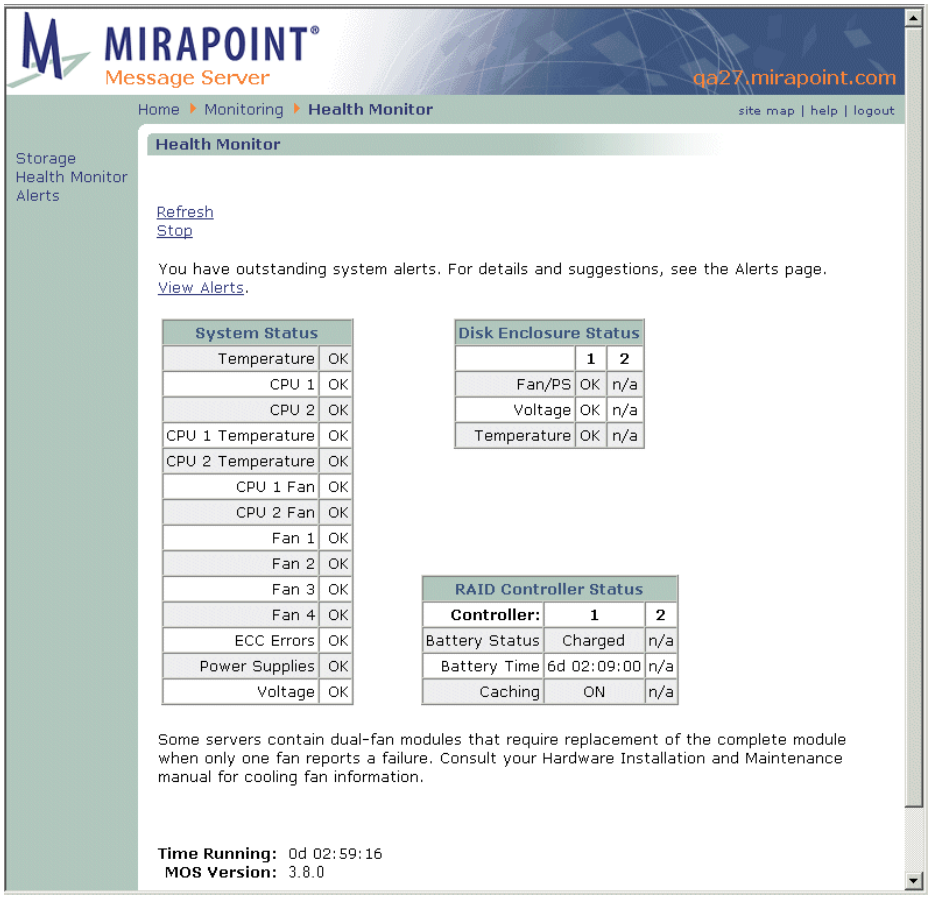


Figure 26 Monitoring > Health Monitor Page

To verify the health of computer components using the Administration Suite, go to the **Monitoring > Health Monitor** page (see Figure 21).

The table on the left represents the computer chassis, while the table on the right represents the disk enclosure. Reported statistics vary per appliance.

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 27).

Figure 27 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 21 Admin Audit Trail Report

Field	Description
user	The login name of the user performing the action; for delegated domain users, this includes the domain name

Table 21 Admin Audit Trail Report (Continued)

Field	Description
id	The unique identifier for the administration service connection (session) in which the event occurred
action	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.

SNMP MIBs are periodically updated. If you use SNMP to monitor your system, Mirapoint recommends downloading the MIB files from the system after upgrading Mirapoint software to ensure you are using the latest MIBs. MIBs can be upgraded by any release. They are available at http://*hostname*/help/snmp-mibs.

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  .
   Result: The add traps page opens, see step 1 for options.

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.

6 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.

If you intend to use Classes of Service (COS), it is better to set up you COS first (described in Managing Classes of Service on page 225) and then create your delegated domains and users; in that way, you can assign a COS to an entire domain or to individual users.

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 it's 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 28 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.

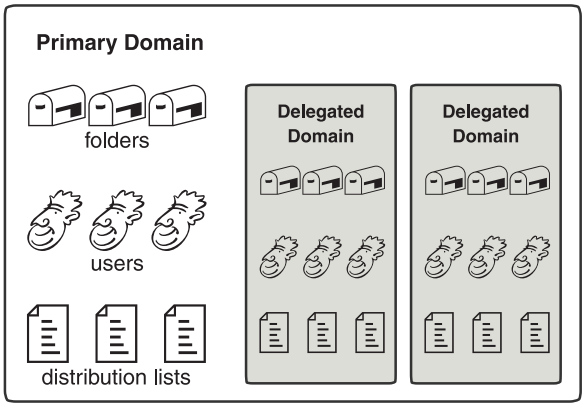


Figure 28 Primary Domain and Delegated Domains

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 are 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 43.”

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.) The **Domains > Administration** and **Class of Service** pages require special licenses to display. See Setting Up a User Directory Service on page 50 for details on configuring your system to enable this LDAP feature.

There is a limit of 32,000 delegated domains.

Domain Sensitivity

Some commands behave differently if a delegated domain is selected see Selecting a Domain on page 185 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 183.
3. Assign the domain administrator to the postmaster distribution list. This is discussed in Adding Delegated Domain Administrators to the Postmaster DL on page 184.
4. Configure settings for policy management, calendar defaults, and customization as needed. These options are discussed in Editing Delegated Domains on page 186 and Configuring Calendar Options for Domains on page 192.

Use the **Domains > Administer Domains** page shown in Figure 31 on page 188 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.

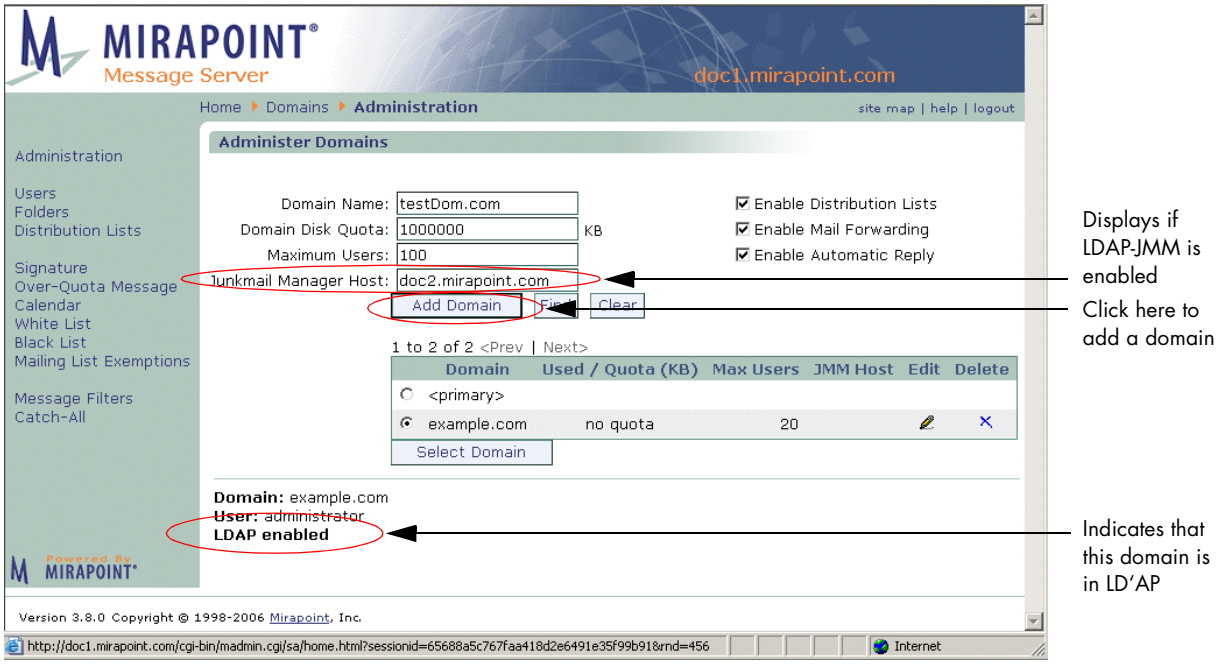


Figure 29 Domains > Administer Domains Page, Add a Domain

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.

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 225.

- **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 85 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 203 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 225 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 203.

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.

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 219.

Finding a Delegated Domain

If have a large number of delegated domains, you can search for the domain you are 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 32 on page 189).

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 on page 184."
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.

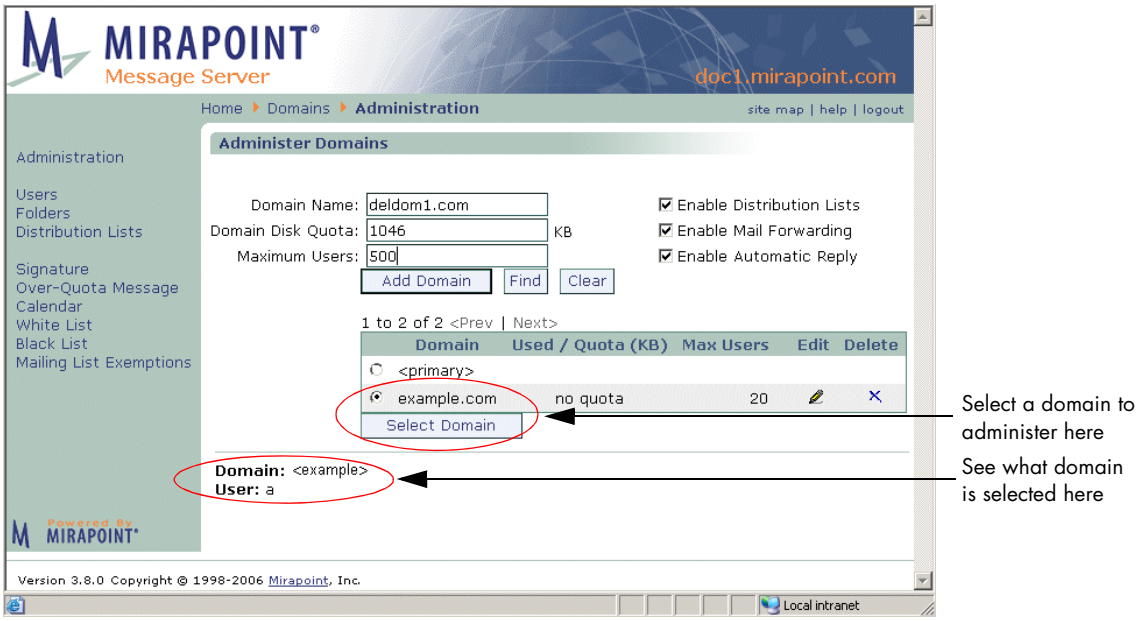


Figure 30 Domains > Administer Domains Page, Select a Domain

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.

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 206 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 183 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 216 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 185 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 225.

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 31 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 211 for details. See Folder Access Control Lists on page 212 for details on folder access control.

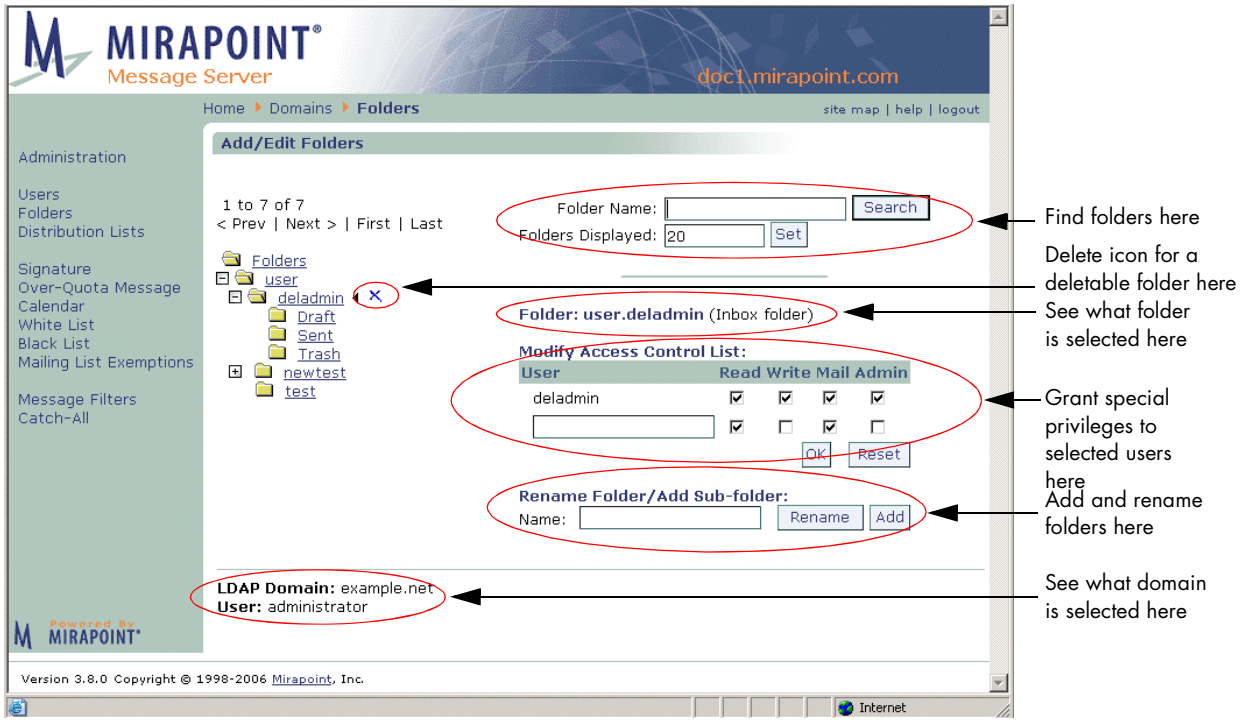


Figure 31 Delegated Domains Folders Page

Creating Distribution Lists for a Delegated Domain

Use the **Domains > Distribution Lists** page (see Figure 32 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 219 for details.

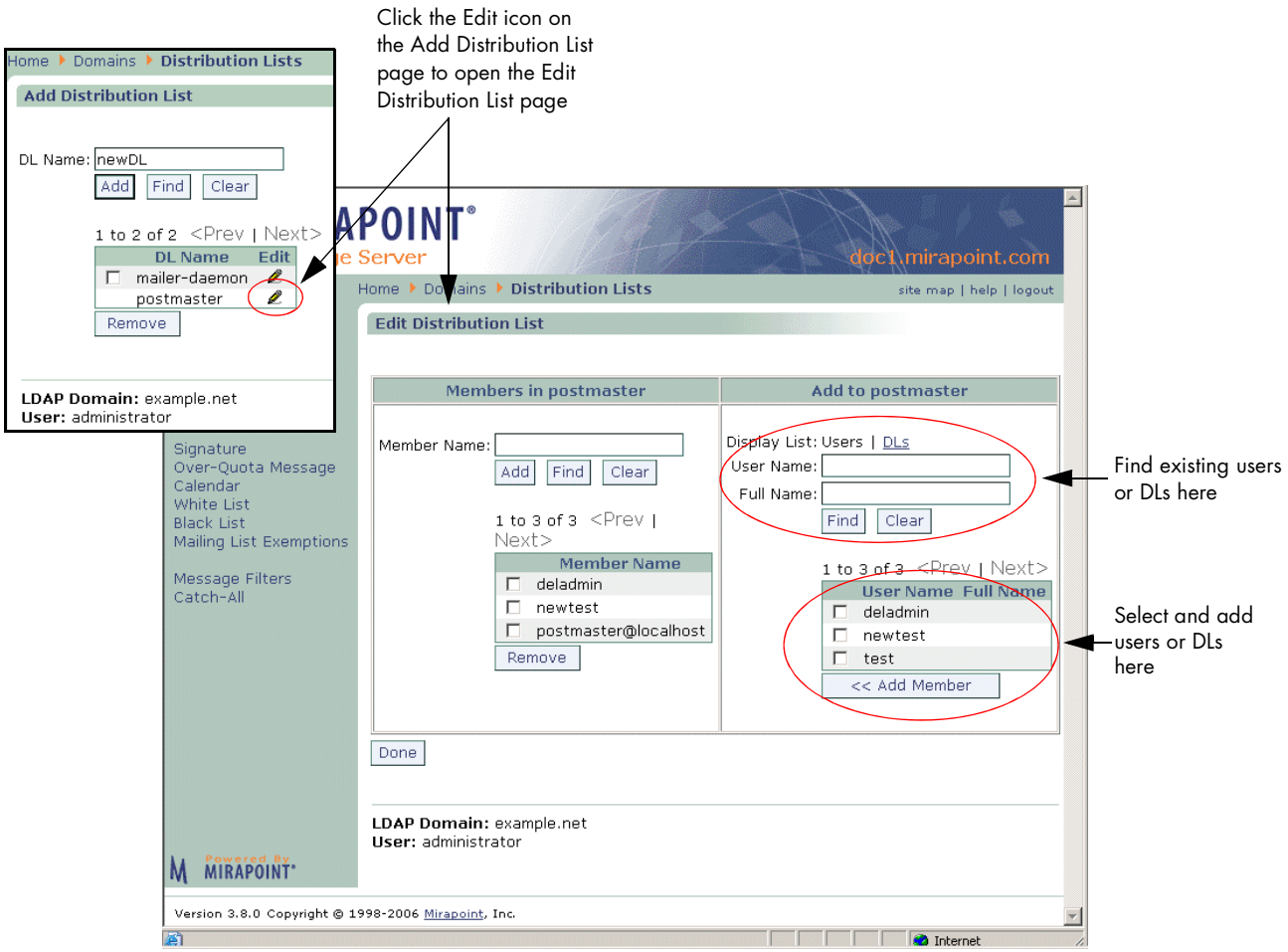


Figure 32 Delegated Domains Distribution List Page

Creating a Signature for a Delegated Domain

The **Domain > Set Signature** page (see Figure 41 on page 214) 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.

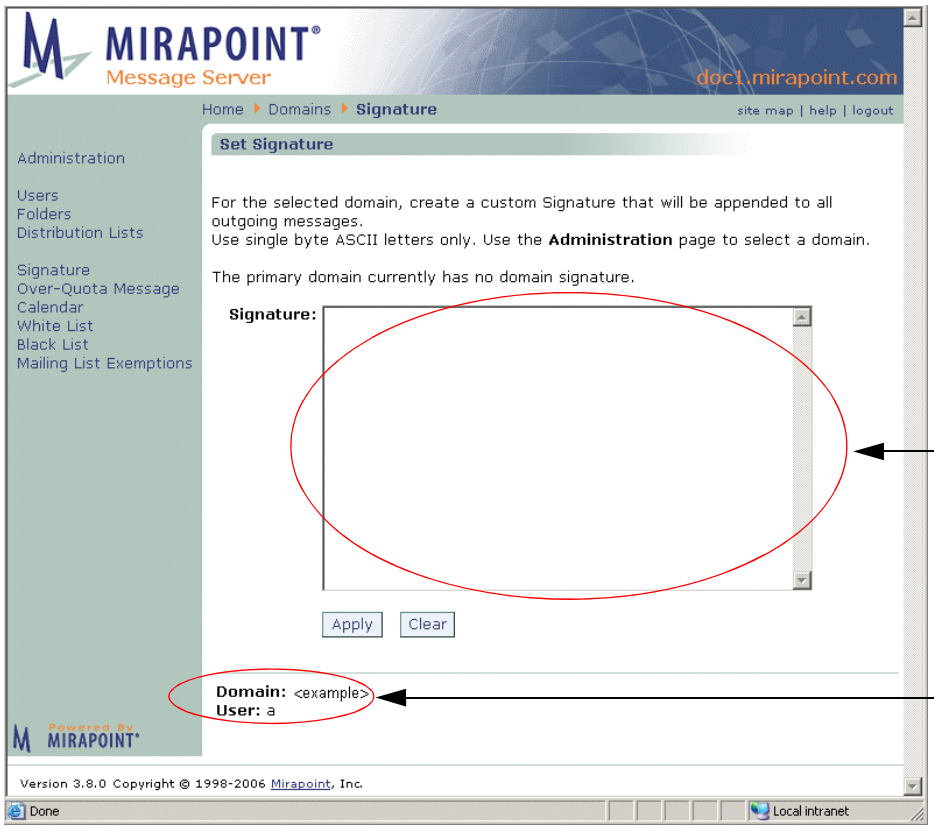


Figure 33 Domains > Signature Page

Customizing the Over-Quota Message

Use the **Domains > Over-Quota Message** page (see Figure 34 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.

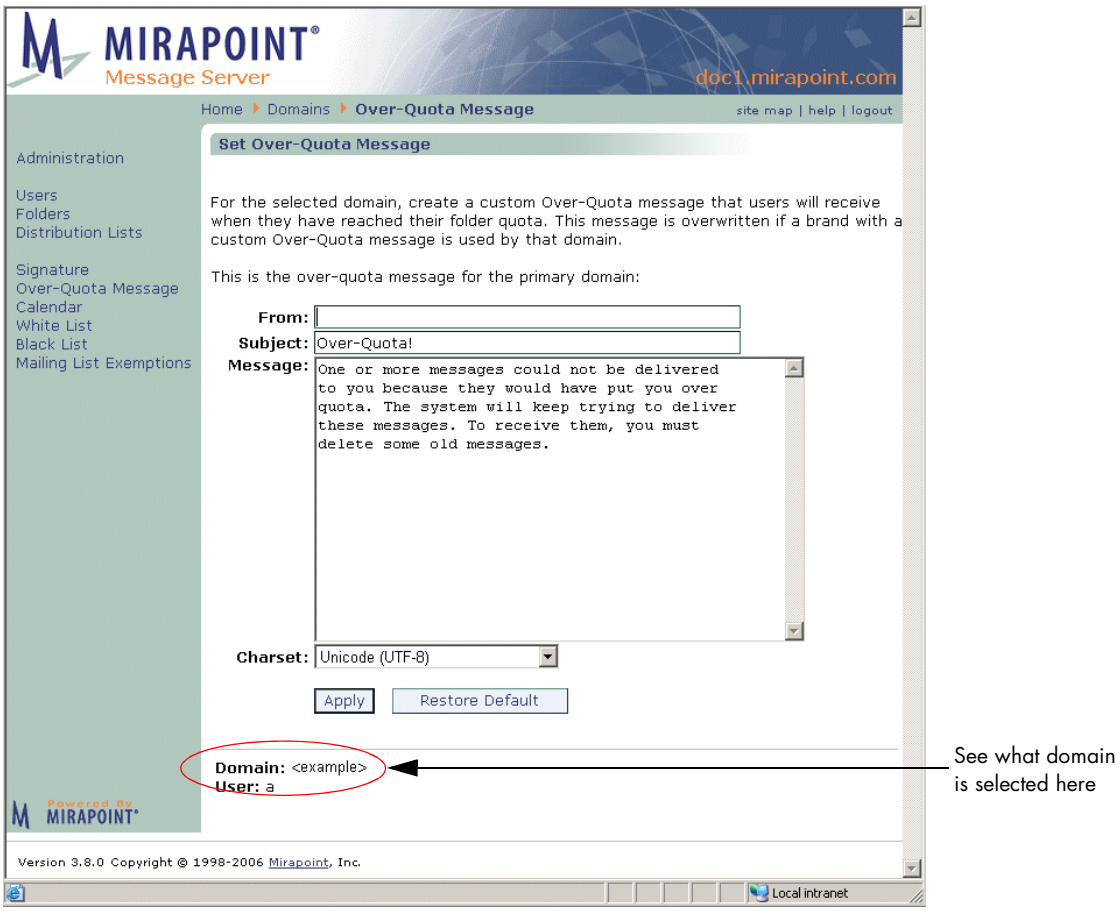


Figure 34 Domains > Over-Quota Message Page

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 7, 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 31 on page 188). 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 225.

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 181.
2. Include LDAP records with the appropriate mailhost for each user. For more information, see Managing Delegated Domains on page 179.
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 179.

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 198.

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 3.10 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. 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?(&(|(objectc
   lass=person)(objectclass=inetorgperson)(objectclass=mirapointUser))(|(uid=
   $(cn)*)(miloginid=$(cn)*)(sn=$(cn)*)(givenname=$(cn)*)))"
   "(uidalias=miloginid)"
   OK Completed
   ```

   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 *delDomName* to the name of the current delegated domain. 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=delDomName,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
```

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 43 on page 215 for an example) to set basic calendar defaults.

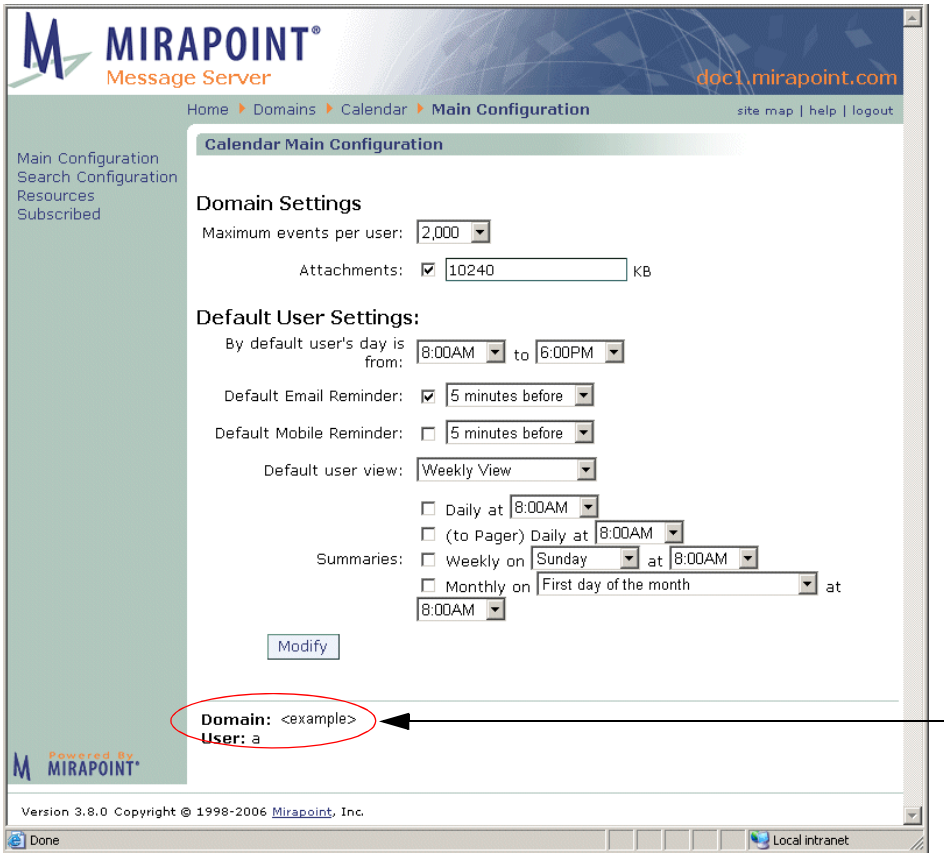


Figure 35 Domains > Calendar > Main Configuration Page

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 drop-down menu 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. 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 44 on page 219 for an example) to set up default search parameters.

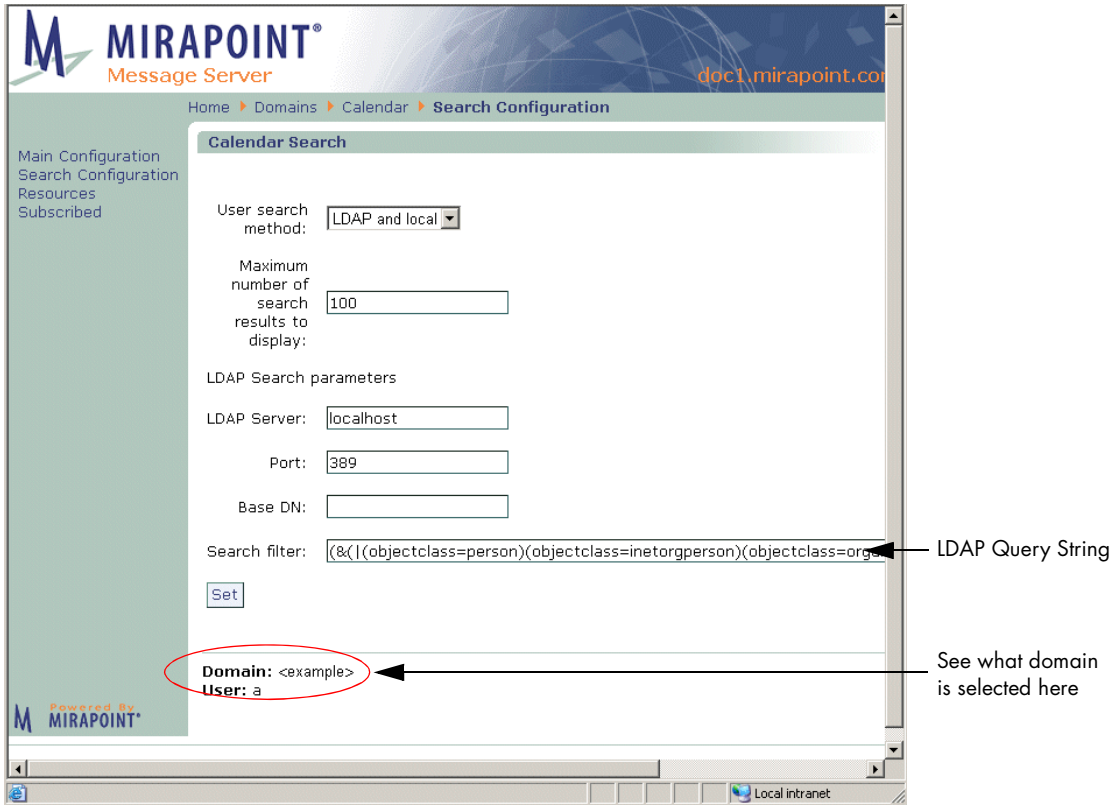


Figure 36 Domains > Calendar > Search Configuration Page

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 45 on page 221 for an example) to add resources such as meeting rooms and projectors. Be sure to select the desired delegated domain first.

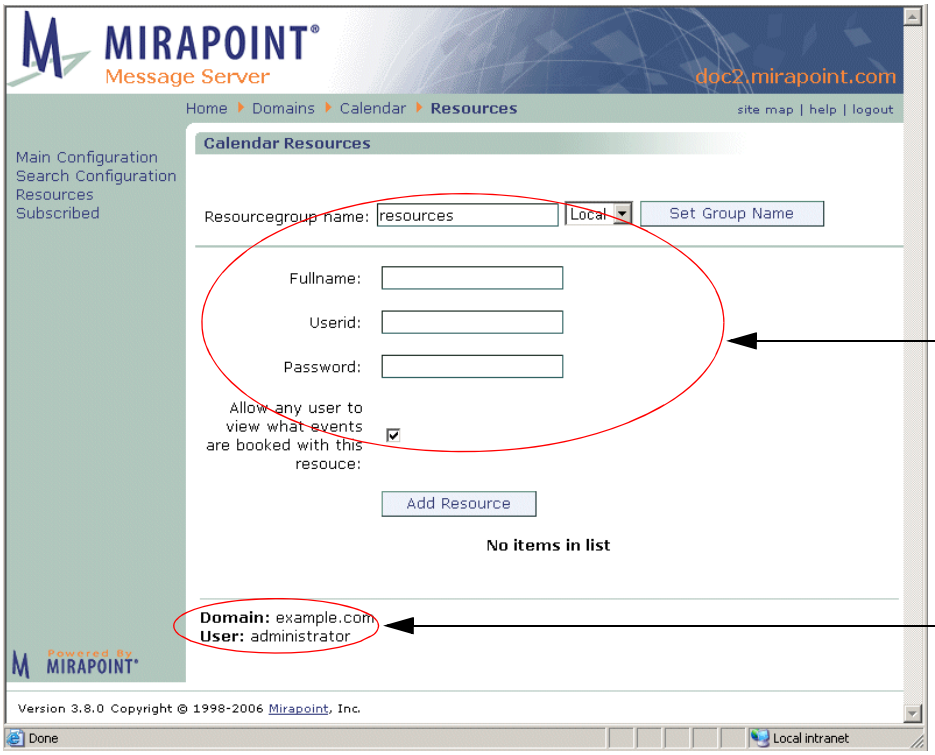


Figure 37 Domains > Calendar > Resources Page

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.

Resources show up in address book as users.

Calendar—Setting Up Calendar Subscriptions

Use the **Domains > Calendar > Subscribed** page (see Figure 46 on page 222 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.” 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.

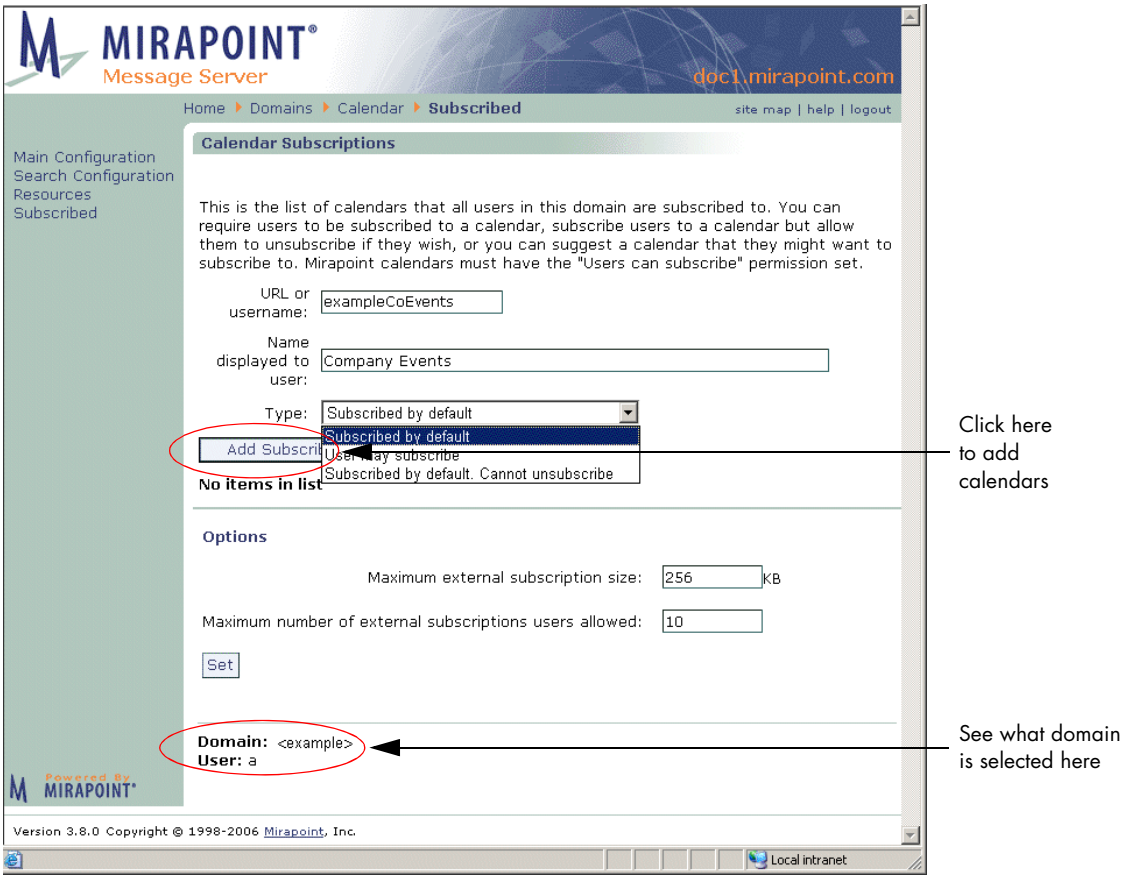


Figure 38 Domains > Calendar > Subscribed Page

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 198 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 admind 3.10 server ready
User: Administrator
Password:
OK User logged in
```

2. 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.

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?(&(objectclass=mirap
ointmailuser)(|(sn=$(cn))(givenname=$(cn))(cn=$(cn))(mail=$(mail)*)(maillo
caladdress=$(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,D
C=com)(bindpasswd=password)"
OK Completed
```

This example is 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 31 on page 188) 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 deleted 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 184."
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.

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 221.

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 241.

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 205.

  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 Address Restrictions

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) and) (close parenthesis)
- , (comma)
- : (colon)
- ; (semi-colon)
- < (less than)
- > (greater than)
- @ (at sign)
- [(open bracket) and] (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) and } (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 39 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.

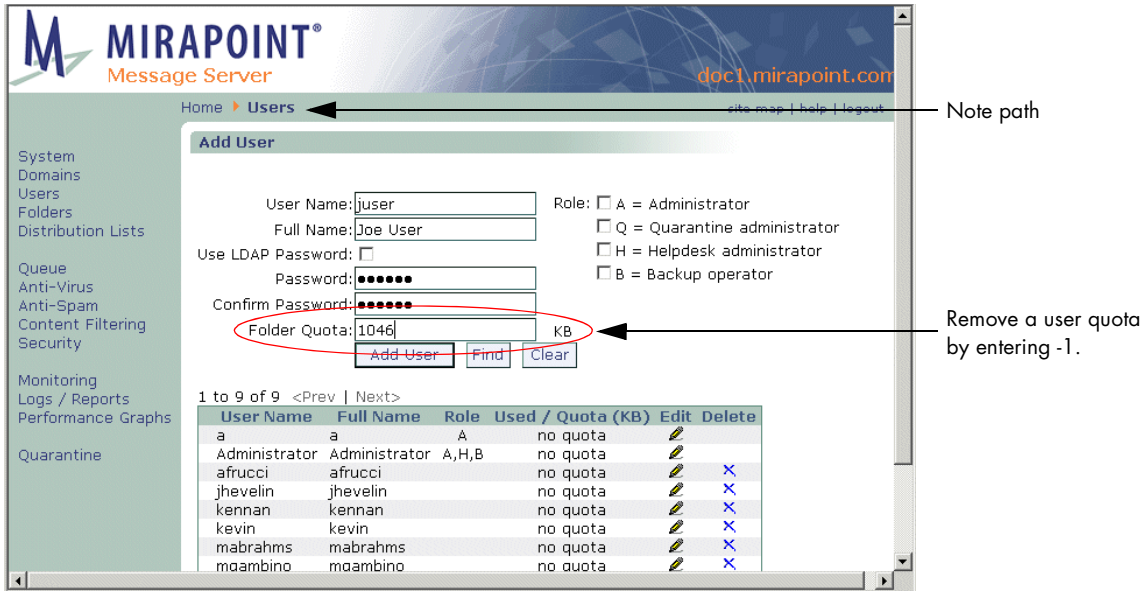


Figure 39 Mirapoint Add User Page

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 183 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 203.
- **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). 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 50 for details): Use this option to set up alias email addresses for your users, the alias's domain must exist in LDAP.

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 211 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 208.

Finding a User

If have a large number of users, you can search for the user you are 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).

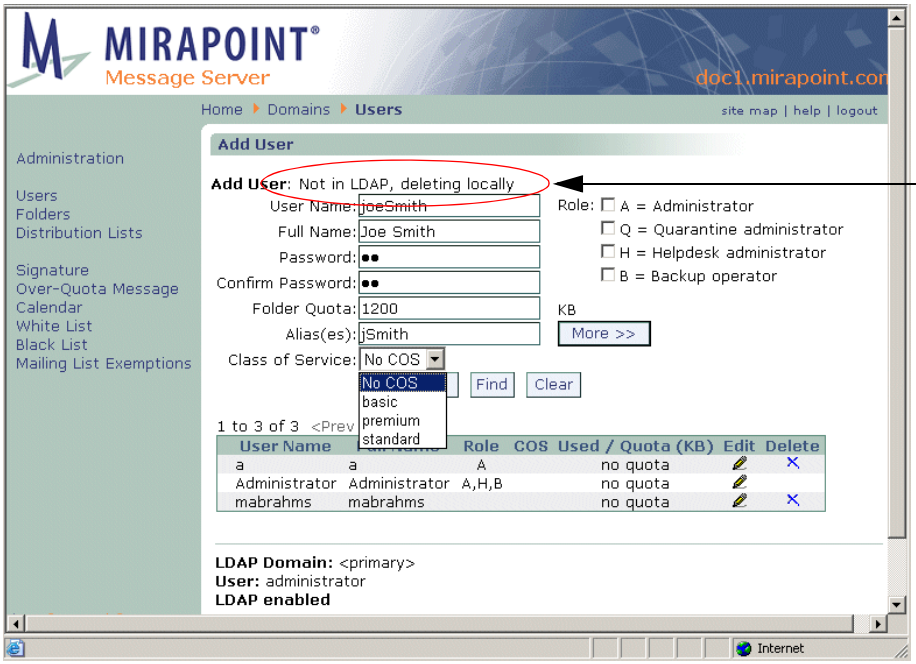
Editing Users

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 confirmation message. 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 40.



This message displays if the user you are deleting was added locally, not with the LDAP-enabled page

Figure 40 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 175.

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 7, 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:

```
Start > Run: telnet hostname.domain.com
OK hostname.domain.com admind 3.10 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 email 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 email 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 email 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 email 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 41 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 43 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. The following characters are allowed:

- Letters (A through Z and a through z)
- Numbers (0 through 9)
- Space ( )
- Minus (-)
- Underscore (_)

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
```

Special Characters Not Allowed

You cannot use the following characters in folder names because they have special meanings:

- Period/Full Stop (.) (U+002E) and Fullwidth Full Stop (U+FF0E)—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/Solidus (/) (U+002F) and Fullwidth Solidus (U+FF0F)—Reserved for the system.
- Plus (+) (U+002B) and Fullwidth Plus (U+FF0B)—Used to address subfolders of user Inboxes or shared folders that do not belong to a particular user.
- Limited by IMAP:
  - Asterisk (*) (U+002A) and Fullwidth Asterisk (U+FF0A)
  - Percent sign (%) (U+0025) and Fullwidth Percent Sign (U+FF05)
  - Quotation Marks (") (U+0022) and Fullwidth Quotation Marks (U+FF02)

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 22, 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 22 describes what the access control permissions mean.

Table 22 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.)

Table 22 Access Control Permissions (Continued)

Field	Description
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 41 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.

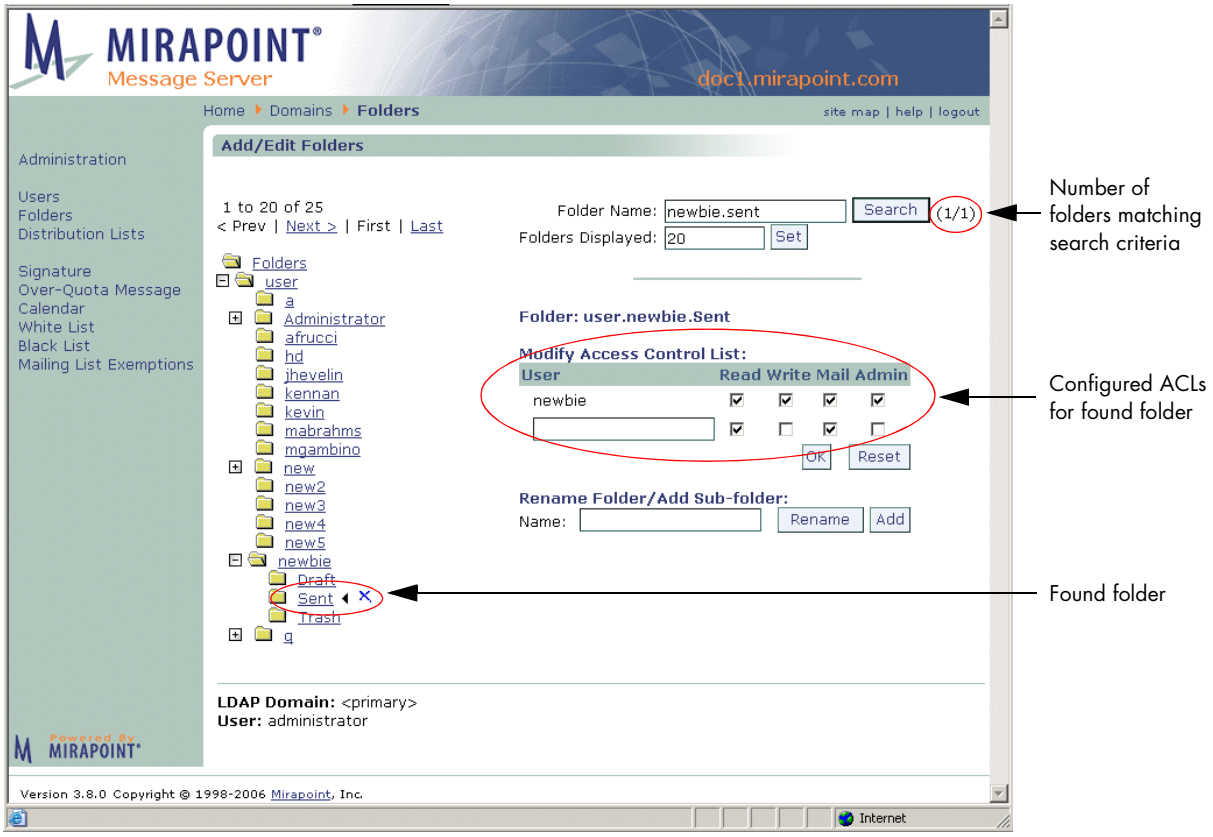


Figure 41 Mirapoint Folders Page—Find Folder Search Result

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 42 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 211 for details. The new folder displays the **Selected** icon and the **Delete** icon that you can use to remove the folder.

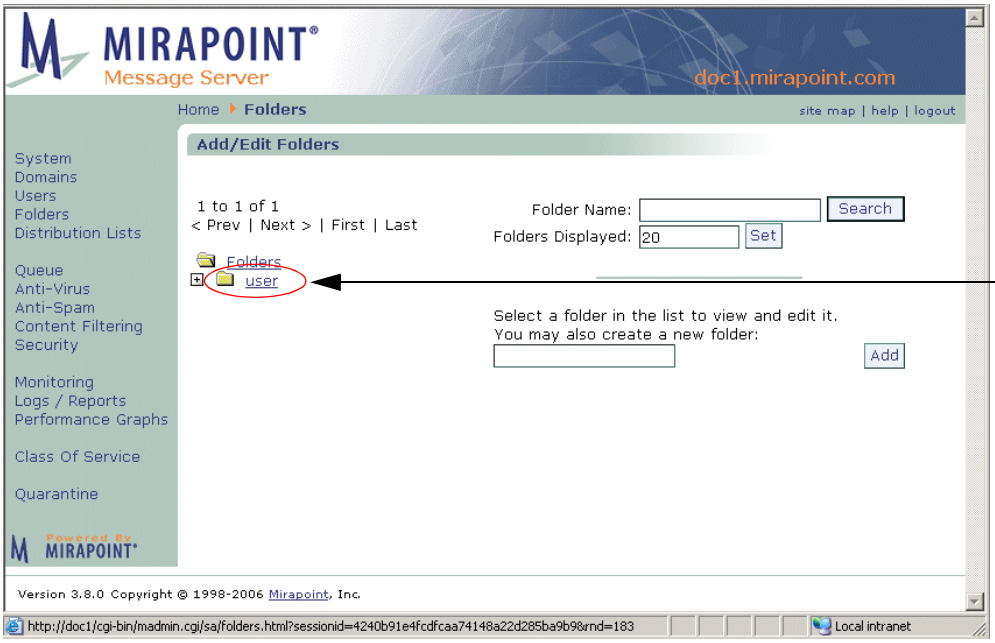


Figure 42 Mirapoint Folders Page—Collapsed View

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 216.

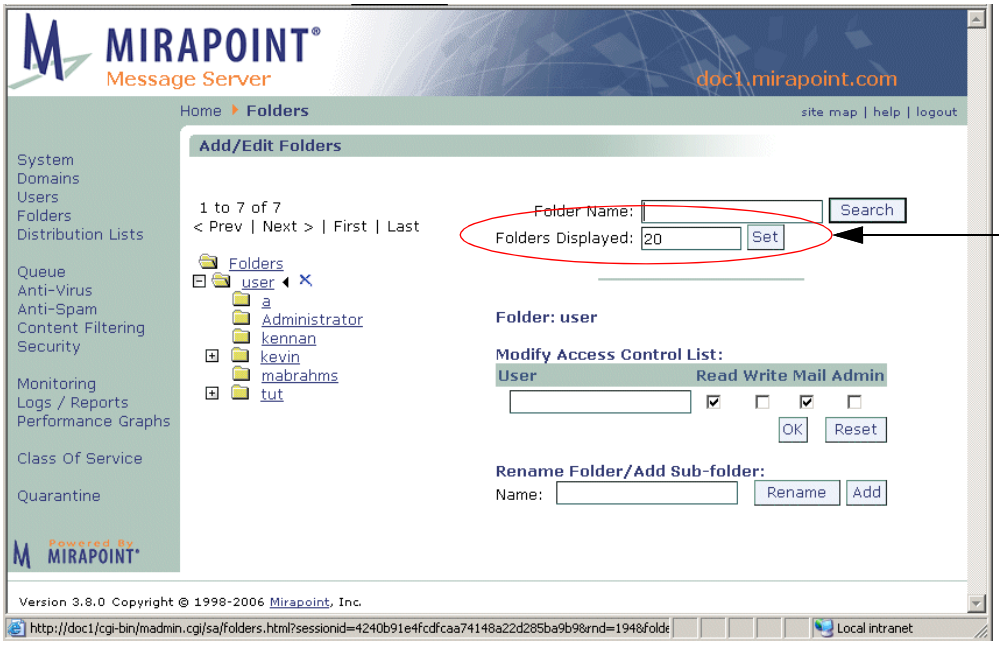


Figure 43 Mirapoint Folders Page—Expanded View

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 **Mail** 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 213).
   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.

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 213).

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 213).
   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 are 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 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.

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 213).
   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.

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 44.

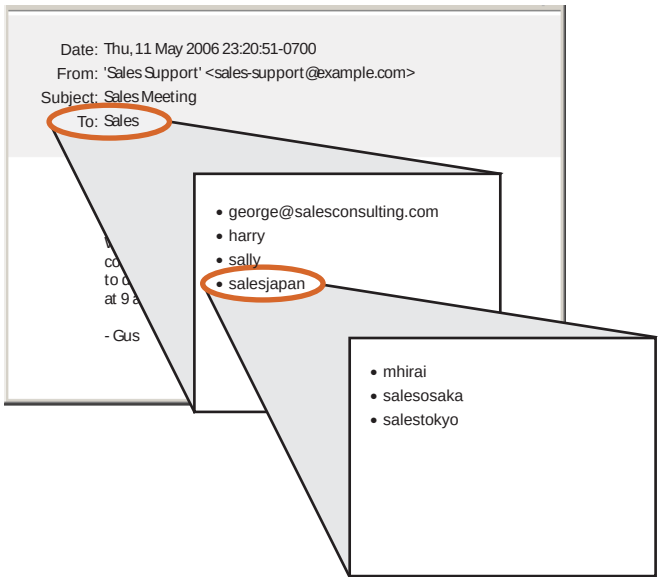


Figure 44 Example of Distribution List Named Sales

In Figure 44, **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 137.

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 45 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.

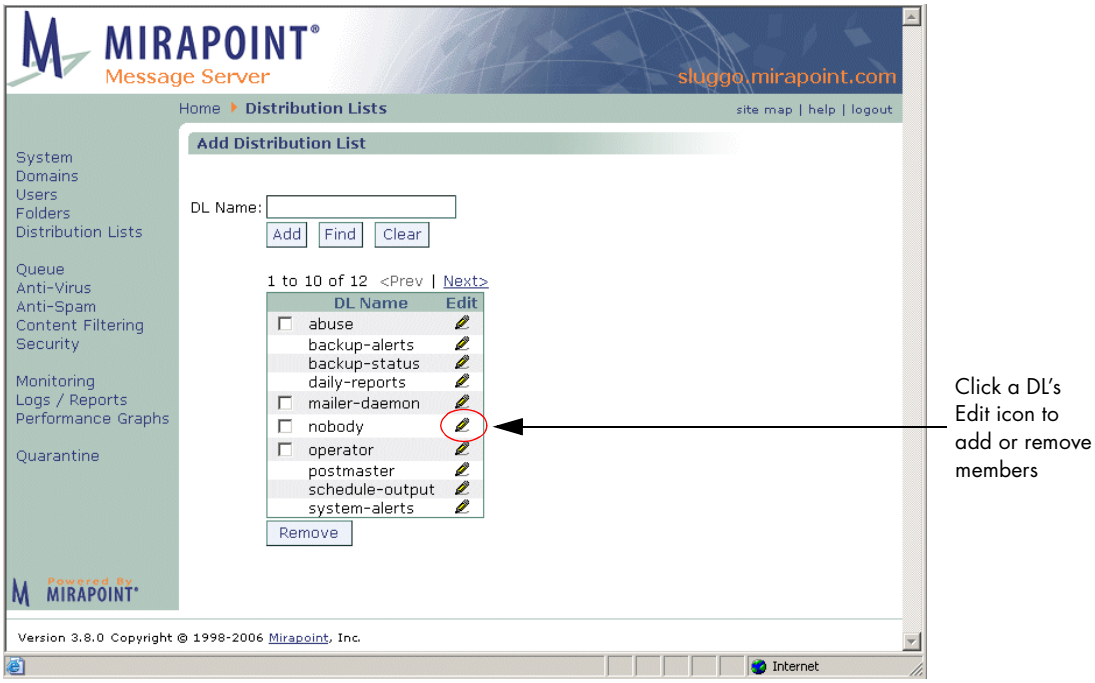


Figure 45 Add Distribution List Page

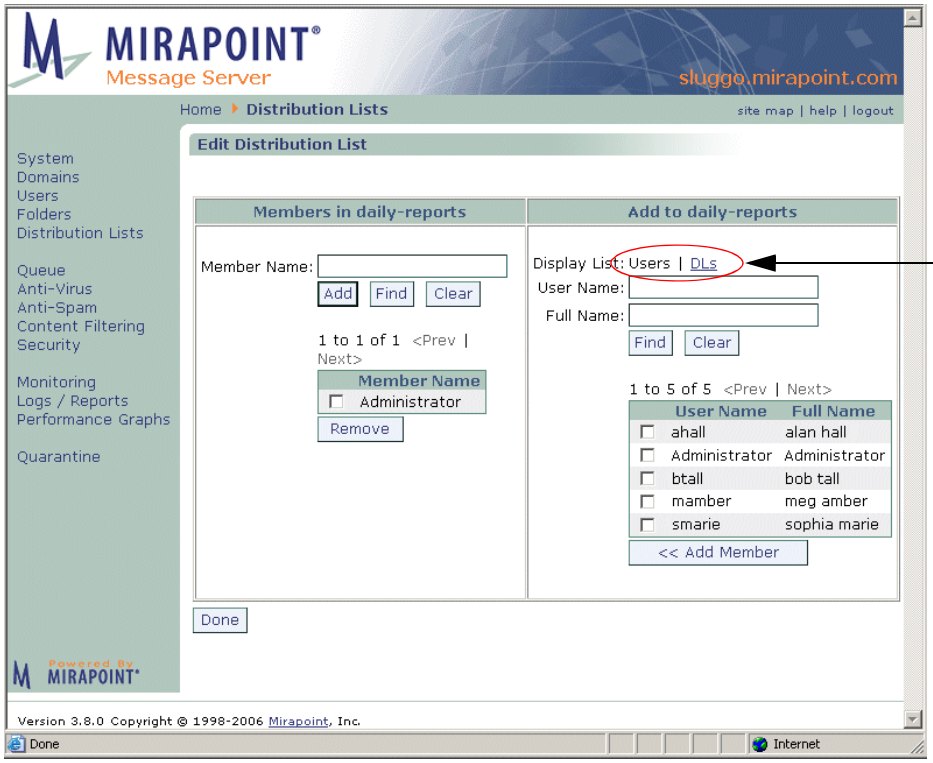


Figure 46 Edit Distribution List Page

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 46 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.

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 45 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 46 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 45 for an example), find the DL that you want to edit and click its **Edit** icon  .

Non-deletable, system-created distribution lists do not have a checkbox by their name.

Result: The **Edit Distribution List** page (see Figure 46 for an example) for that DL displays.

2. Make changes to the members as needed, see Adding and Populating Distribution Lists on page 221 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 45 for an example), find the DL that you want to remove, select it and click **Remove**.

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.

7 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 **LDAP Class of Service Editor** 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 folder settings by domain or user through Classes of Service. A "Class of Service" (COS) is a named set of services and limits, configured as an LDAP attribute, 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 LDAP-enabled **LDAP Class of Service Editor** pages.

To control access to a particular service, you need to enable Class of Service LDAP checking for that service—otherwise, all users can access the service (as long as the service is licensed and enabled).

The COS mechanism can be used to make different levels of service available to your users. For example, the "Gold" COS service might include all available services, while the "Silver" service might include a subset. You can name the classes of service that you create what you want.

User and domain information, including COS attributes, are stored in your LDAP database. If COS checking is enabled for a service, LDAP lookups 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). COS requires a complete LDAP infrastructure in order to be used.

Not all services should be COS enabled on every appliance. For example, **Sender Anti-spam** and **Sender Anti-virus** would only be enabled on an appliance acting as an outbound message router. Similarly, many services only make sense on an appliance acting as a message store, and the antivirus and antispam services apply to appliances acting as message screeners or inbound message routers.

If a user is created in a domain that has a COS attribute, that user automatically inherits that domain's COS. You can assign a different COS to a user in the domain and that assignation overrides the domain's COS. If you remove from a user any COS assignation (assign them "No COS") they will still inherit the COS of their domain. If you change the COS for a domain, that change affects all users in that domain that are not already specifically assigned a different COS, including any users from whom a COS attribute was removed.

Class of Service Features and Configuration Options

COS must be enabled using the command line interface (CLI); how to do this is described in Chapter 2, All-In-One Message Server Deployment page 54 and Chapter 3, Message Server Setup for Multi-Tier Deployments page 90 as part of the setting up of the Internal Directory service (an LDAP directory service is required for COS).

Once COS has been enabled, and your LDAP is set up (along with LDAP GUI), the **Class of Service** link displays in the top-level left menu. The services displayed on the **LDAP Class of Service Editor** 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 Site Planning Guide*. These are the service choices displayed on the **Class of Service** page.

- **Anti-Spam**—Inbound antispam scanning
- **Anti-Virus**—Inbound antivirus
- **Automatic Reply**—WebMail auto-reply
- **Calendar**—WebCal Direct Standard Edition (Personal)
- **Corporate Edition**—WebMail/Group Calendar Corporate Edition
- **Message Filters**—WebMail message filters
- **Forwarding**—WebMail mail forwarding (vacation mail)
- **External Mail**—WebMail External POP mail
- **Group Calendar**—WebCal Direct Standard Edition (Group)
- **IMAP**—Message sending and receiving
- **Junkmail Manager (JMM)**—Spam mail management
- **Message Expiration**—Automatic message deletion
- **Message Undelete**—Deleted messages retrieval
- **POP**—Message sending and receiving

- **Quota for Mailbox**—Quota setting
- **Sender Anti-Spam**—Outbound antispam scanning
- **Sender Anti-Virus**—Outbound antivirus scanning
- **SSL**—HTTPS secure connections
- **WebMail**—WebMail Direct Standard Edition

Services Requiring Additional Configuration

Some of the COS services listed above require additional configuring:

- **Folder Quota**—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)—Duration a message can remain in the user's **Junk Mail** folder before expiring and deleting. For users without Junk Mail Manager.
- **Trash Message Expire** (**Message Expiration** configuration)—How long a message can remain in the **Trash** mail folder before expiring and deleting.
- **JMM Message Expire** (**Junk Mail Manager** configuration)—Duration a message can remain in the Junk Mail Manager quarantine before being expired and deleted.
- **JMM Mailbox Quota** (**Junk Mail Manager** configuration)—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)—Two-step message retrieval hierarchy. Provides a **deletedmessages** folder hierarchy where messages deleted from user folders 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 (junk mail) by the antispam scanner. Useful for POP users who lack a **Junkmail** folder.

If you create a COS and do not select any services, the COS is endowed with ALL services.

Any folder can be set up for expiry (automatic message deletion) by editing LDAP attributes directly (see **Help Mailbox Msgexpirenow** in the CLI); however, only the **Junk Mail** and **Trash** folders can be set up so using the LDAP enabled **Class of Service** pages.

The **Class of Service** page link only displays if you have COS enabled for your system. Clicking the **Class of Service** link in the left menu opens the **LDAP Class of Service Editor** page as shown in Figure 47, Class of Service Edit Page, next.

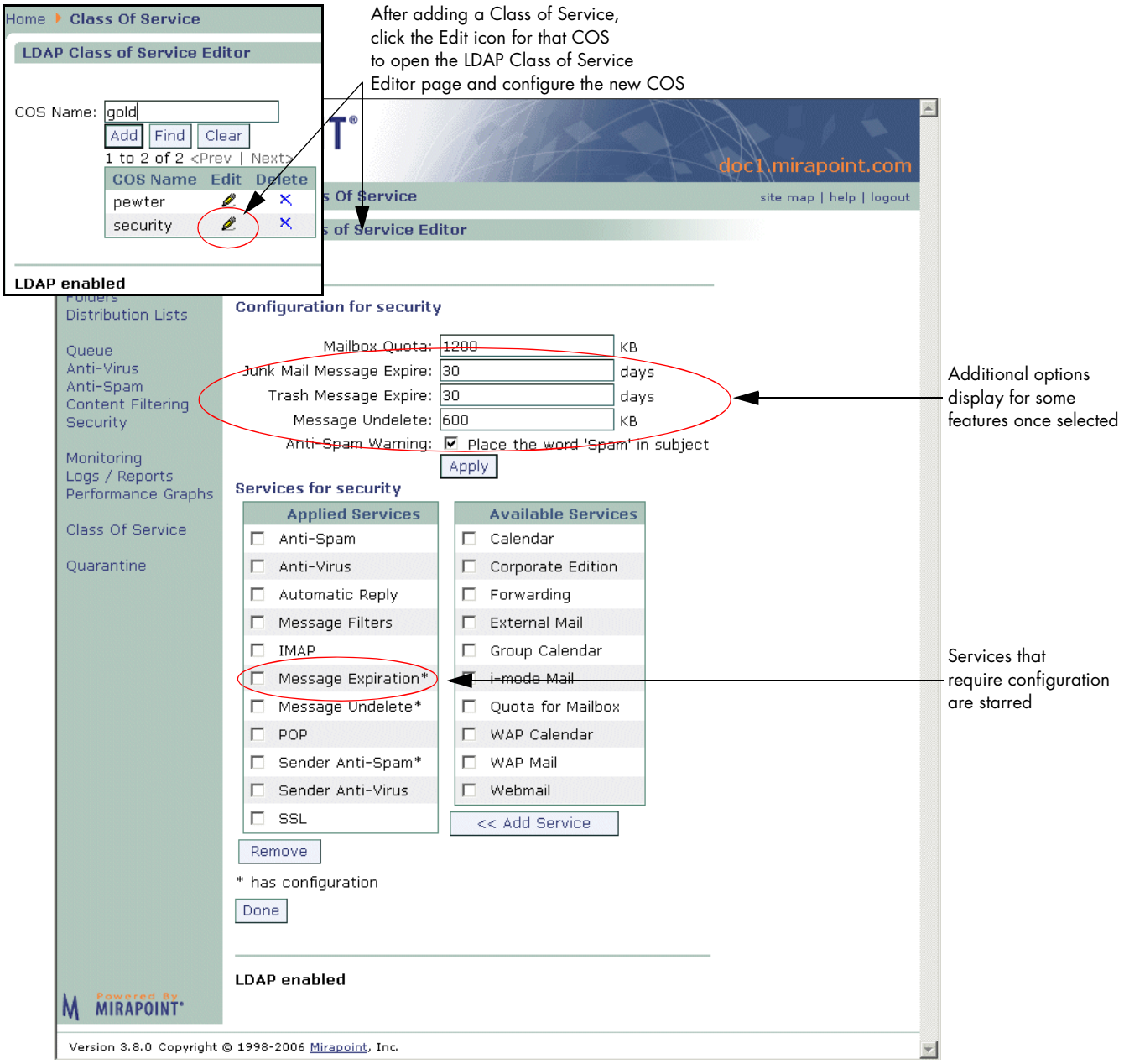


Figure 47 Class of Service Edit Page

Adding and Populating a Class of Service

The **Class of Service** page (see Figure 47 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.

1. Click **Class of Service** in the left menu to open the **LDAP Class of Service Editor** page. Enter a **COS Name** 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 **LDAP Class of Service Editor** page refreshes with service options. Initially, all available services display in a table to the right.
3. Select the services that you want to make available to users of this class of service; choose services that you have enabled. To add a selected service, click **Add Service**.

The COS is added to your LDAP database. Services that aren't available on this machine can be added to the COS as long as they are licensed and enabled in your LDAP directory.

Result: The selected services are added to the new COS and display in a table. Additional service configuration options display at the top of the page.

4. Depending on which services you added to the new COS, you might have to enter configuration data; see Services Requiring Additional Configuration on page 227 for details. Click **Apply**
   Result: The conditions for the COS are entered into the system.
5. To remove an added service, click **Remove Service**.
6. When you finish, click **Done**.
   Result: You return to the top-level **LDAP Class of Service Editor** 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 the Forwarding option does not display when they use WebMail.

Assigning a COS to a particular user overrides the COS assigned to the domain to which the user belongs. If no COS is assigned to the user or the user's domain, the primary COS is used if there is one. Otherwise, all enabled services are available.

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 overriden 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 below, the pattern **ann?** used to find a user, would match the former user names, and the pattern **jo***, used to find a folder, would match the latter folder names:

```
anna anne

jo joe john jon jon.bulk jon.personal
```

Editing Classes of Service

To edit a class of service, follow these steps.

1. On the **LDAP Class of Service Editor** page, find the COS that you want to change and click its **Edit** icon  .
   Result: The LDAP **Class of Service Editor** page opens.
2. Make your changes, adding or removing features; when you are finished, click **Done**. Click **Apply** before clicking **Done**.
   Result: 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.

1. On the **LDAP Class of Service Editor** page, find the COS that you want to delete and click its **Delete** icon ✕.
   Result: A confirmation page displays.
2. Click **OK** to confirm or **Cancel** to terminate the delete operation.
   Result: If you click **OK**, the selected COS disappears from the **Class of Service** list. If you click **Cancel**, the Class of Service is not deleted. Both options return you to the top-level **LDAP 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; examples of the pages used to implement these quotas are shown in Figure 48, Domains > Administer Domains Page, Domain Quotas," and Figure 49, Mirapoint Add User Page, Quota and COS Included," next.

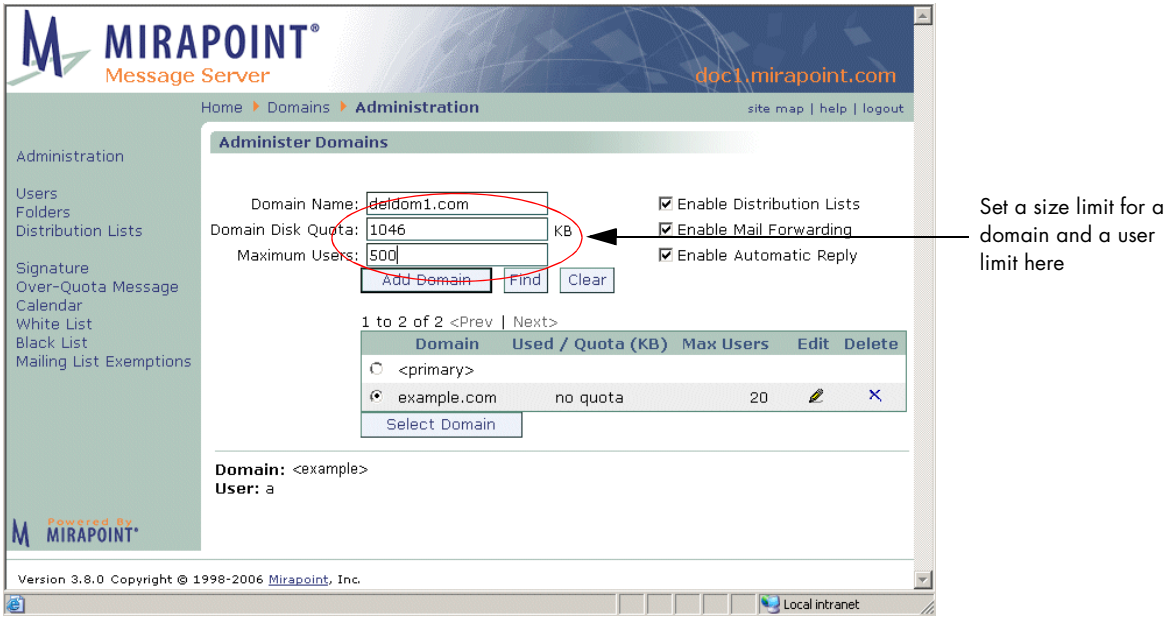


Figure 48 Domains > Administer Domains Page, Domain Quotas

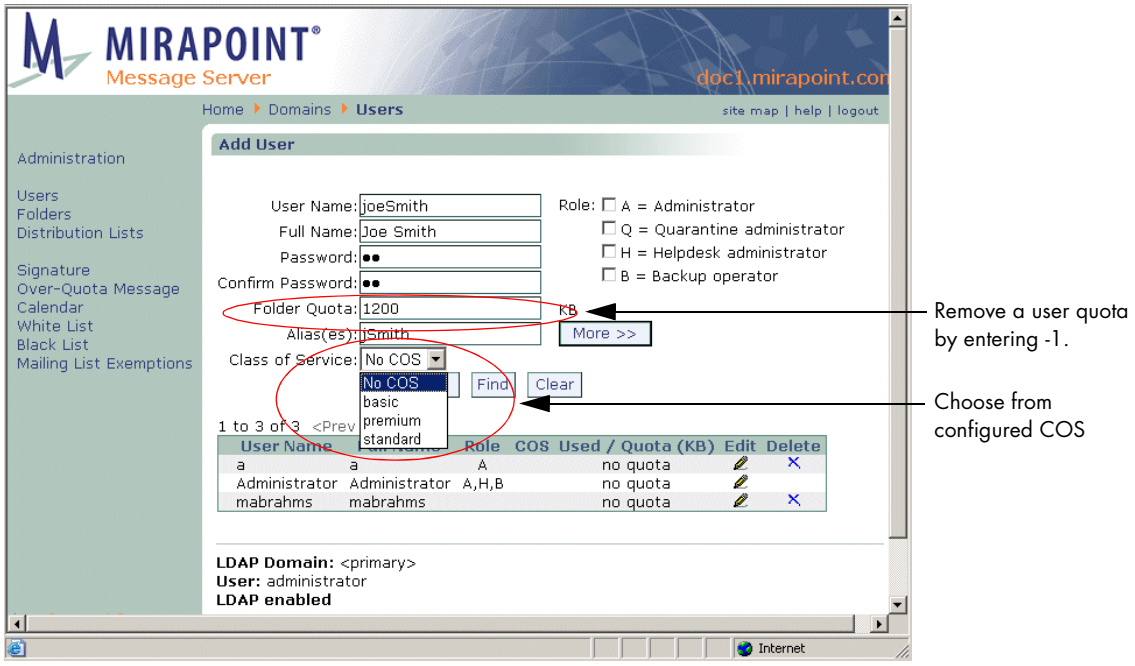


Figure 49 Mirapoint Add User Page, Quota and COS Included

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.

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**—Automatic message deletion. Selecting this COS feature requires the specification of **Trash Message Expire** (when the user's **Trash** mail is deleted).
- **Message Undelete**—Message Retrieval. Selecting this feature requires the specification of a **deletedmessages** folder where messages deleted from user folders can be retrieved by an administrator. Some IMAP clients allow users to access the **deletedmessages** folder and retrieve messages themselves.
- **Quota for Mailbox**—Quota setting on user folders.
- **Junk Mail Message Expire** (**Message Expiration** configuration)—Duration 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)—Duration a message can remain in the JMM quarantine before being expired and deleted.
- **JMM Mailbox Quota** (**Junk Mail Manager** configuration)—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 move 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, connect to your appliance using telnet in a command window, and log in as the Administrator:

```
Start > Run: telnet hostname.domain.com
OK hostname.domain.com admind 3.10 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. The namespace (Cyrus or UW) is box-wide, applies to IMAP only, and can be switched at any time, although switching will cause disruption to the user community including significantly longer login times the first time each user connects to IMAP following the namespace change. This is because the client caches must be refreshed and users must download their entire folder again.

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, connect to your appliance using telnet in a command window, and log in as the Administrator:

```
Start > Run: telnet hostname.domain.com
OK hostname.domain.com admind 3.10 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
```

Set the expiration schedule with the **Schedule Add** command; this command schedules message expiration daily at 3 AM for all users in the current domain, or top-level domain if none is current:

```
Schedule Add aging daily 3 "Mailbox Msgexpirenow (users=*) 0"
```

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 are 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.

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.

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. Additionally, you can set up content policies on a box-wide basis for all, local, or non-local email.

Creating Content Policies

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.

The message filters functionality is broad in scope and can be used 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.

Top Email Content Concerns

Studies show the top enterprise employee email concerns include:

- Protecting identity and financial privacy—Employee's social security number, paycheck information, etc. must be kept confidential.
- Guarding against leaks of confidential memos—Internal memos must stay internal.
- Complying with internal email policies—Confidentiality agreements specifying that confidential material will only be shared with other company employees must be honored.
- Complying with health care privacy regulations and guidelines—Employee health care benefit records must be kept confidential.
- Guarding against leaks of valuable IP (intellectual property) and trade secret—Outgoing email must not contain intellectual property or trade secrets.
- Guarding against inappropriate content and attachments—Offensive or inappropriate email content and attachments must be controlled.
- Signatures and disclaimers—Domain-wide signatures or disclaimers for all mail outgoing from a particular domain. For details, see Attaching a Signature to All Messages From a Domain.
- Restrictions—Maximum message size and maximum number of recipients and/or attachments restrictions. Often, the allowable attachment types are also restricted.
- Encryption—Employees in highly sensitive areas of a company may be required to have all mail encrypted for additional security.

Example Policy Enforcement Filters on page 250 are given after the Creating a Message Filter section on page page 243. It's best to read the following sections providing important background information, before creating filters.

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 243.

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.

Figure 50 Destination Domain Filter Options

The **Destination Domain** options (see Figure 50 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.

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; this is also true of delegated domain

filters. Multiple filters at the same priority are executed at that "priority level," then the filters at the next priority level are executed.

Filters are executed in the following priority order by default:

100 (High Priority) filters **Any** Destination Domain
100 (High Priority) filters **Primary** Destination Domain
100 (High Priority) filters **Local/Nonlocal** Destination Domain
100 (High Priority) delegated domain filters
antivirus scanning
antispam scanning
450 filters **Any** Destination Domain
450 filters **Primary** Destination Domain
450 filters **Local/Nonlocal** Destination Domain
450 filters delegated domain filters
500 filters **Any** Destination Domain
500 filters **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

The **Content Filtering > Advanced** page indicates the order in which configured filters are executed. 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.

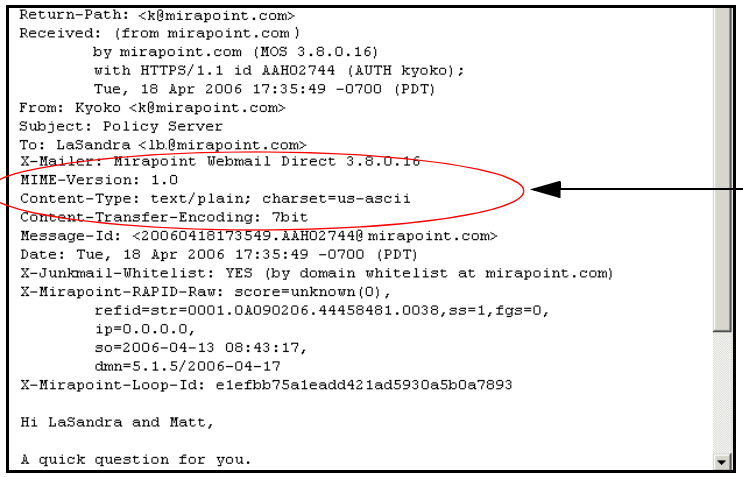


Figure 51 Example Message Source, MIME Type Indicated

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**).

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 (for Outlook 2003)

http://technet.microsoft.com/en-us/library/cc179163.aspx (for Outlook 2007)

About the Antispam Scanning Rules and Threshold

The antispam scanner uses one of two techniques to categorize mail as junk mail (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 junk mail. The more rule matches, the higher the

UCE score; a score over 50 classifies the mail as junk mail; 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.

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 **Anti-Virus > Configuration** page **E-mail address** 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 243 for more information about setting filter options.

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 290. For information on the Junk Mail Manager quarantine, see How Junk Mail Manager Quarantine Works on page 242.

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 **Antivirus Set Quarantinedelay** command. For more information, see the *Mirapoint Administration Protocol Reference*.

Creating a Message Filter

To create domain-level content filters, use the **Domains > Message Filters** pages (you must select a delegated domain for the **Message Filters** link to display).

To create system-wide antispam filters, use the **Content Filtering > Advanced** pages. System-wide antispam filters are created in the same way as domain-level content filters only there is the additional option of choosing the **Destination Domain**, that specifies a scope for the filter. Creating system-wide, antispam filters is discussed in detail in the See Figure 52 and Figure 53 for examples.

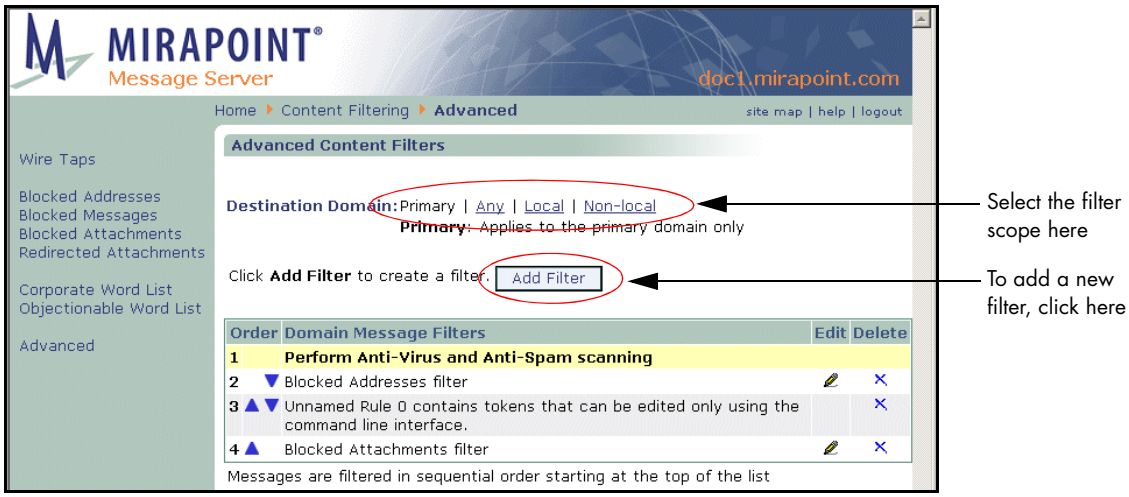


Figure 52 Advanced Content Filters Page, Add Filter

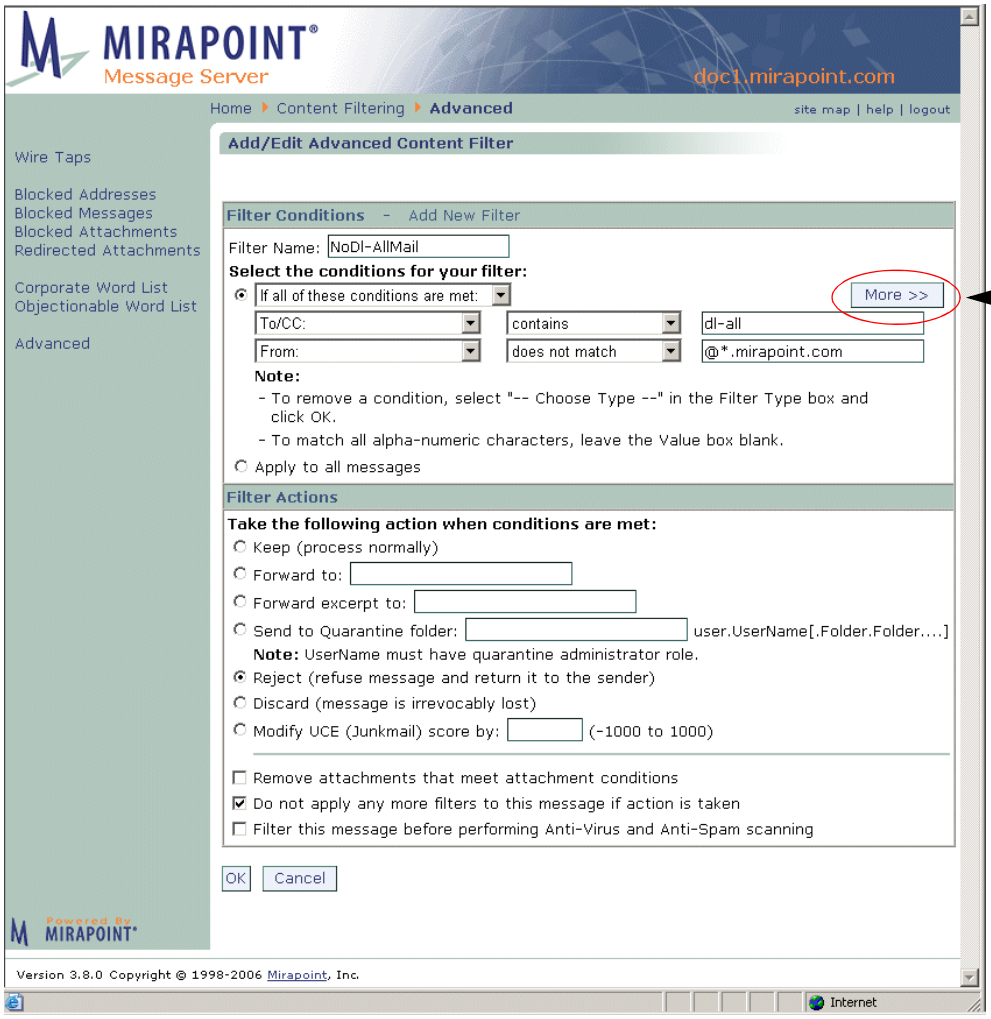


Figure 53 Add/Edit Advanced Content Filter Page

To create a message filter follow these steps.

1. On the **Add Advanced Filter** page (see Figure 52), in the **Destination Domain** area specify the scope for the filter you are creating.

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 processes only mail addressed to the selected user group. See About the Destination Domain Options on page 238 for details on this option.

2. Click **Add Filter.**
   Result: The **Add/Edit Filter** page displays (see Figure 53).
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**: What the mail recipient sees as the **From** line.
   - **To/CC**: What the mail recipient sees as the **To** line (does not include BCC recipients).
   - **Subject**: The subject line.
   - **Body**: The message body; text and text attachments including Plain text, HTML text, and Rich Text. This is the same as choosing **bodydecoded** (the decoded form of all MIME parts of the message) in the CLI (command line interface). If you are looking for an 8-bit string, or an encoded Word document, this option might be best.

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.

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. This is the same as choosing **body** (the raw RFC822 text) in the CLI. If you are looking for a word (ASCII text), or MIME data, in a message, this option might be best.
- **Body (binary)**: Use this to find the binary value of an alphanumeric string in the message. This is the same as choosing **bodydecodedbinary** (unrolls all the MIME parts and allows binary searches) in the CLI. For example, to use this option to find the “Yen” character (hex A5), you would enter **\xA5**.

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 322.

- **To (message envelope)**: What the routing believes is the recipient, includes Bcc; 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. Administrator-only option.
- **From (message envelope)**: What the routing believes is the sender; 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. Administrator-only option.
- **Return-path**: The return-path address; not useful with domain filters as the return path might be re-written, use **From (message envelope)** instead. End-users could use this if they think they are being spoofed.
- **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 162.
- **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 321.
- **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. Administrator-only option.
- **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**. Administrator-only options.
- **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 239. If you are looking for a single attachment MIME type, this option might be best; if you are looking for many, the Attachment Word Lists are better filters.
- **Attachment file name**: The attachment name. You can use the asterisk wildcard; for example, *.vbs.
- **Attachment size (bytes)**: The value must be an integer. Administrator-only option.
- **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 240. Using this option is highly discouraged; every time

the UCE score is modified, the entire message is re-written which can cause other problems.

- **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.

Use the asterisk (*) wildcard and the **does not contain** 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.
   - **does not regex-match**: The object must not match the regular expression you enter; use with regular expressions only.
   - **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?**"

   Example: "starts with something:" ***something***, or "ends with something:" ****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 kept through the end of that filter priority level. This option is useful in conjunction with other filters or options; see Filtering "Keep" Use Examples on page 257.
   - **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 241. For information on the Quarantine Administrator user, see About the Quarantine Administrator User on page 203.

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 only if the **Send Recipient(s) the following message** option (described below) is selected.
- **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 antispam 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.

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 in order below this filter (within that filter priority level) are not applied to the message.
- **Filter this message before performing Anti-Virus and Anti-Spam scanning** (deselected by default): The message will be passed to antivirus and antispam scanning after it has been filtered by the preceding filters.
- **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.

Example Policy Enforcement Filters are given on page 250; Example System-Wide Antispam Filters are given on page 320.

Reordering a List of Filters

Before and during message acceptance on the system, SMTP authentication, relay and blocked domains, and RBLs (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).

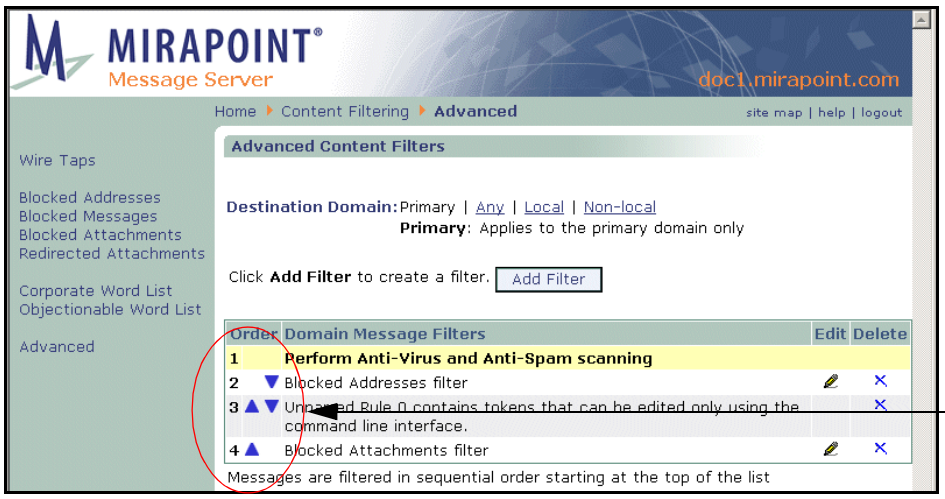


Figure 54 Advanced Content Filters Page, Reordering Filters

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 238 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 238 for more information on filtering ordering.

Example Policy Enforcement Filters

You set policy content limitations using domain-wide message filters. Most content policy filters are on outgoing email, so you must set **Destination Domain = Non Local** for each filter you create. If you set **Destination Domain = Any**, mail incoming and outgoing is filtered.

Some message filters that can be used to implement policies are described in this section. Create these filters on the **System > Content Filtering > Advanced** page, unless otherwise noted. See Content Filtering Options on page 238 for details.

Filtering on Social Security Numbers

This filter quarantines outgoing mail containing a series of numbers in the configuration used for social security numbers.

Destination Domain = Non Local
Filter Name: QuarantineSocSecNums
If all of these conditions are met
Body
regex matches
[0-9][0-9]-[0-9][0-9]-[0-9][0-9][0-9][0-9]
Send to Quarantine folder: user.QA.socsecnums

Filtering on Specific Words

To filter certain words in either the **Subject** header or the message body, use the **Corporate Word List** or **Objectionable Word List** filter pages. For details, see Using Corporate Word Lists, and/or Using Objectionable Word Lists. Words that might be used in a **Corporate Word List** filter include:

- Proprietary
- Confidential
- Internal

Filtering on Mail Sent to Competitors

This filter scans the **To envelope** (includes BCC recipients) and quarantines messages that are sent to competitors. To do this, you must first compile a list of competitors. An example of this filter:

Destination Domain = Non Local
Filter Name: QuarantineCompetitorRecipients
If any of these conditions are met
To (message envelope)
matches
competitor A

OR (use **More>>** to add another condition)
To (message envelope)
matches
competitor B
(add as many rules as needed)

Send to Quarantine folder: user.QA.socsecnums

Filtering All Mail Outgoing From a Certain Address

This filter "wire taps" an address; use the **Home > Content Filtering > Wire Taps** page. If you select **Destination Domain = Non Local**, all mail outgoing from the specified address is sent to the specified **Forward to** address where it can be examined. Using the CLI (command line interface) you can create a more specific wire tap filter to wire tap mail based on advanced filter criteria; for details, see **Help About Filter** in the CLI.

Filtering Outgoing Mail with Too Many Recipients

To filter out (bounce) all outgoing email messages with more than 50 recipients, use the SMTP Maximum Recipients per message option on the **System > Services > SMTP > Main Configuration** page. The default maximum number of recipients is 50000.

Filtering Over-sized Messages

This filter restricts the maximum size of outgoing messages to 128 MB:

Filter Name: BounceMessageTooLarge
If all of these conditions are met
Message size (bytes)
is more than
31457280
Reject
Send the recipient(s) the following notification message:
To: $(sender)
From: Administrator
Subject: Your mail has been filtered
Message: Your mail with subject $(subject) has been $(action) by $(filtername) filter.

An alternate method of restricting message size is to use the Maximum Message Size option on the **System > Services > SMTP > Main Configuration** page. The default maximum message size is 31457280 in bytes. The advantage to doing this with a filter is that you can send a notification message.

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 189.

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.

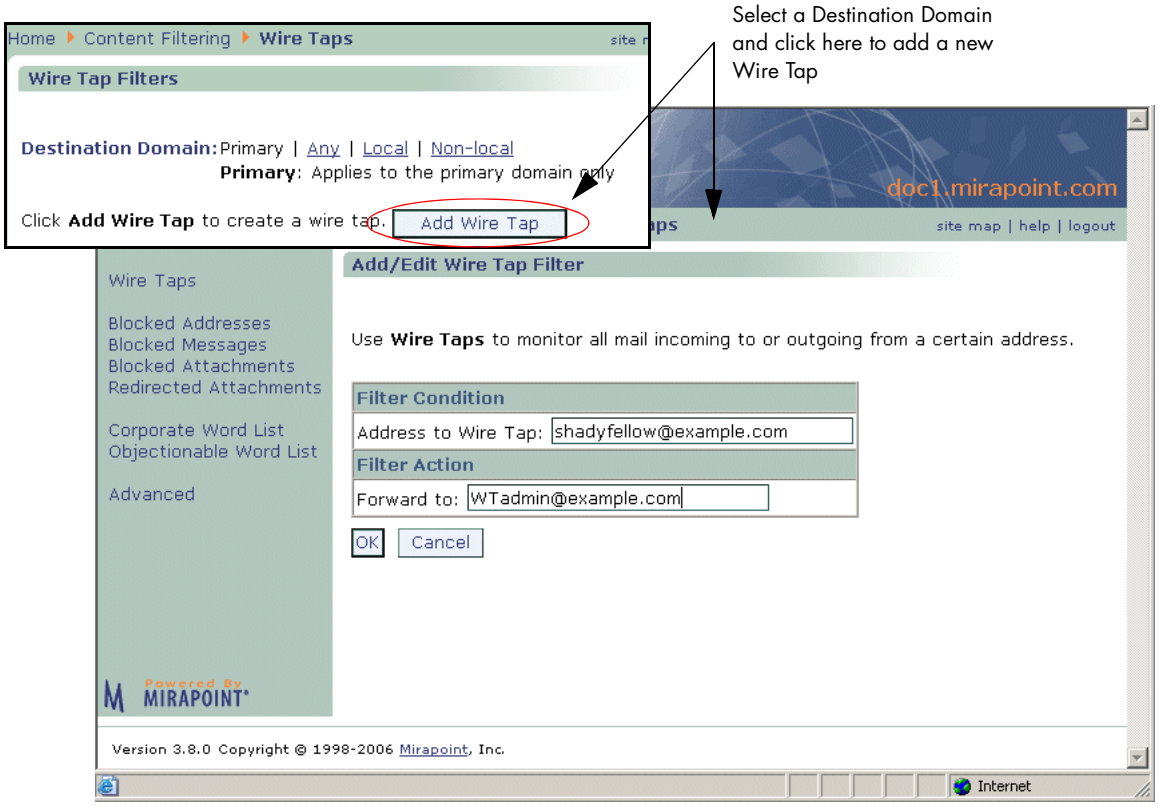


Figure 55 Content Filtering > Wire Tap Page

To create, edit, or delete a Wire Tap follow these steps on the **Content Filtering > Wire Taps** page (see Figure 55 for an example).

1. In the **Destination Domain** area specify the scope for the filter you are creating. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 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 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.

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 a delimiter.

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.

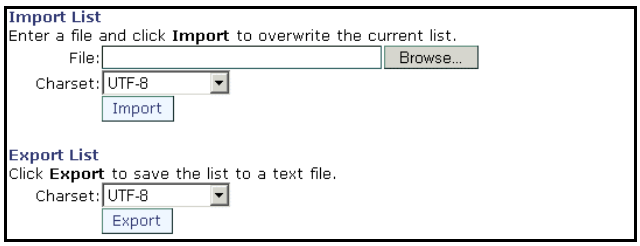
Managing a Filter List

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.

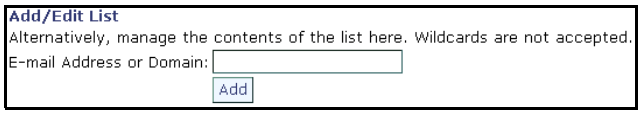
You cannot separate entries with spaces or semi-colons; each entry must be on a separate line. Therefore, you must make your entries one at a time. Wildcards are not accepted.

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**".

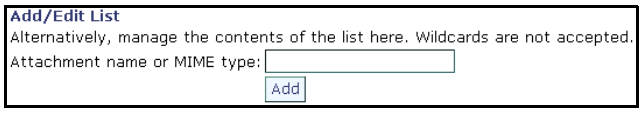


Import a word list you have created here

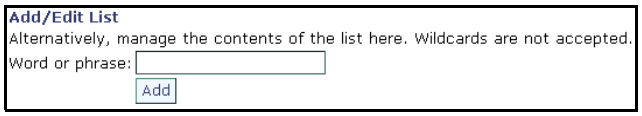
Export a word list you have created here; you can then import that word list to other word list filters



Word List editor for Blocked Addresses



Word List editor for Blocked and Redirected Attachments



Word List editor for Corporate and Objectionable Word Lists

Figure 56 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 56 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 239.

   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**.

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.

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.

Integrating a New Word List

Often word lists are used to filter out unacceptable messages with the action set to discard. In the case where such a word list filter has been operating successfully and there are new words to be added, Mirapoint recommends following this process:

1. Set up a new wordlist that contains only the new entries.
2. Create a quarantine folder for the new wordlist.
3. Create a new filter using the new wordlist and set the action to quarantine to the quarantine folder you created for it.
4. Review the messages that the new wordlist filter catches; release any messages that are mistakenly matched and adjust the wordlist entries accordingly.
5. Once the wordlist is refined; add the new entries to the original wordlist and delete the new wordlist filter.

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 203 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.

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.

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 254.

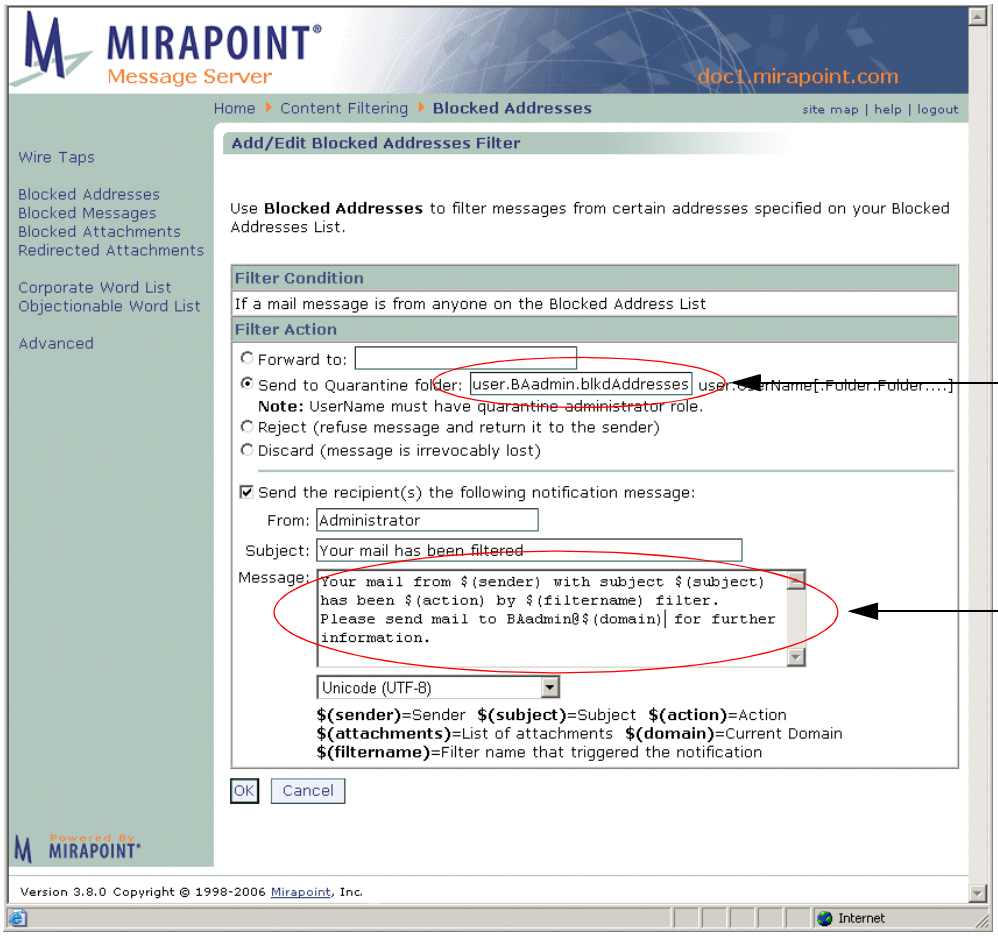


Figure 57 Content Filtering > Blocked Addresses Page

To create, edit, or delete a **Blocked Addresses** filter, follow these steps on the **Content Filtering > Blocked Addresses** page (see Figure 57).

1. In the **Destination Domain** area specify the scope for the filter you are creating. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 for details on this option.
2. Create a **Blocked Addresses** list; to do this, see Managing a Filter List on page 254 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 257.
   - **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 241.
   - **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 254.

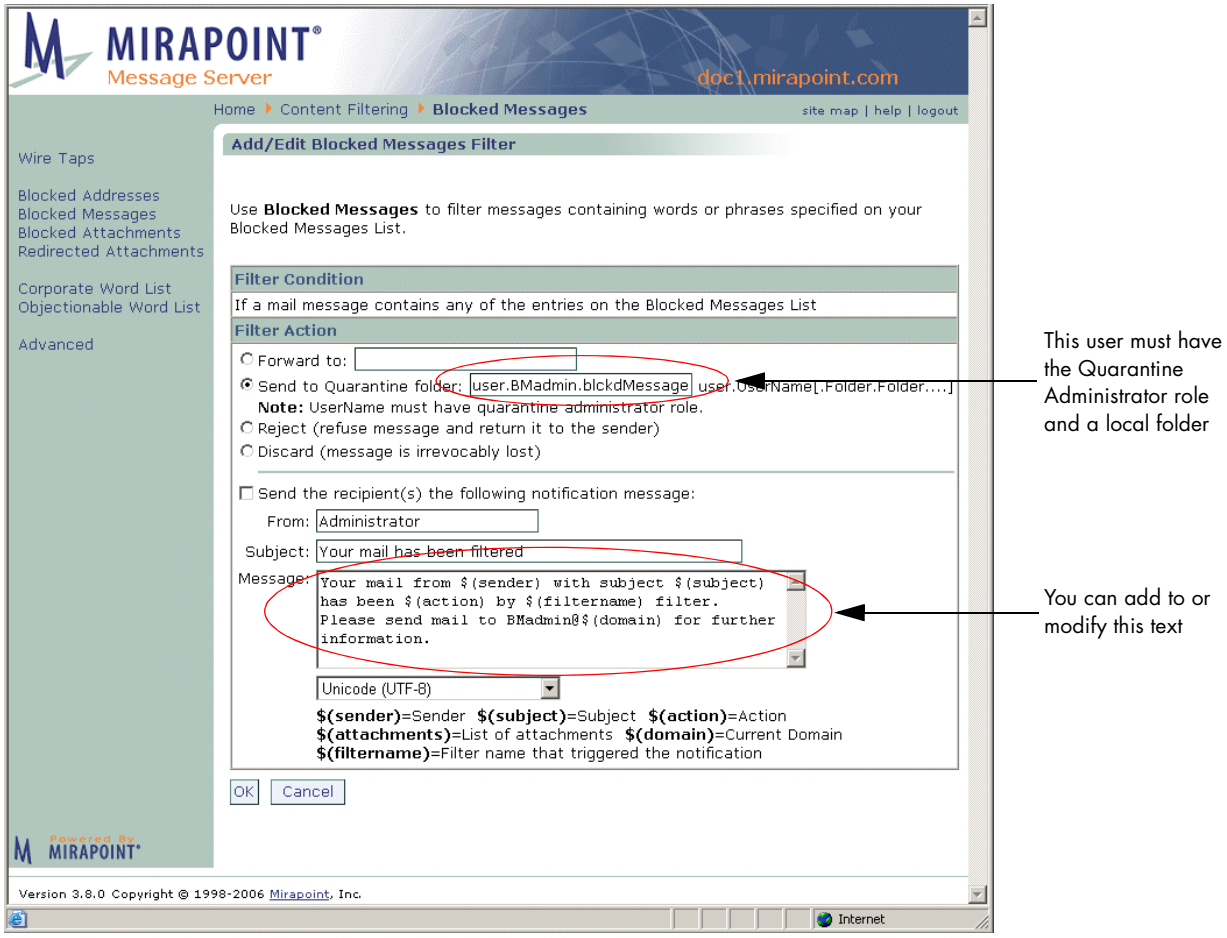


Figure 58 Content Filtering > Blocked Messages Page

To create, edit, or delete a Blocked Messages filter follow these steps on the **Content Filtering > Blocked Messages** page (see Figure 58).

1. In the **Destination Domain** area specify the scope for the filter you are creating. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 for details on this option.

2. Create a **Blocked Messages** list; to do this, see Managing a Filter List on page 254 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 257.
   - **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 241.
   - **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 254. To understand this filter better, see About MIME and Filtering Attachments on page 239.

There is a list of attachments that Microsoft recommends that you block; see: http://office.microsoft.com/en-us/assistance/HA011402971033.aspx

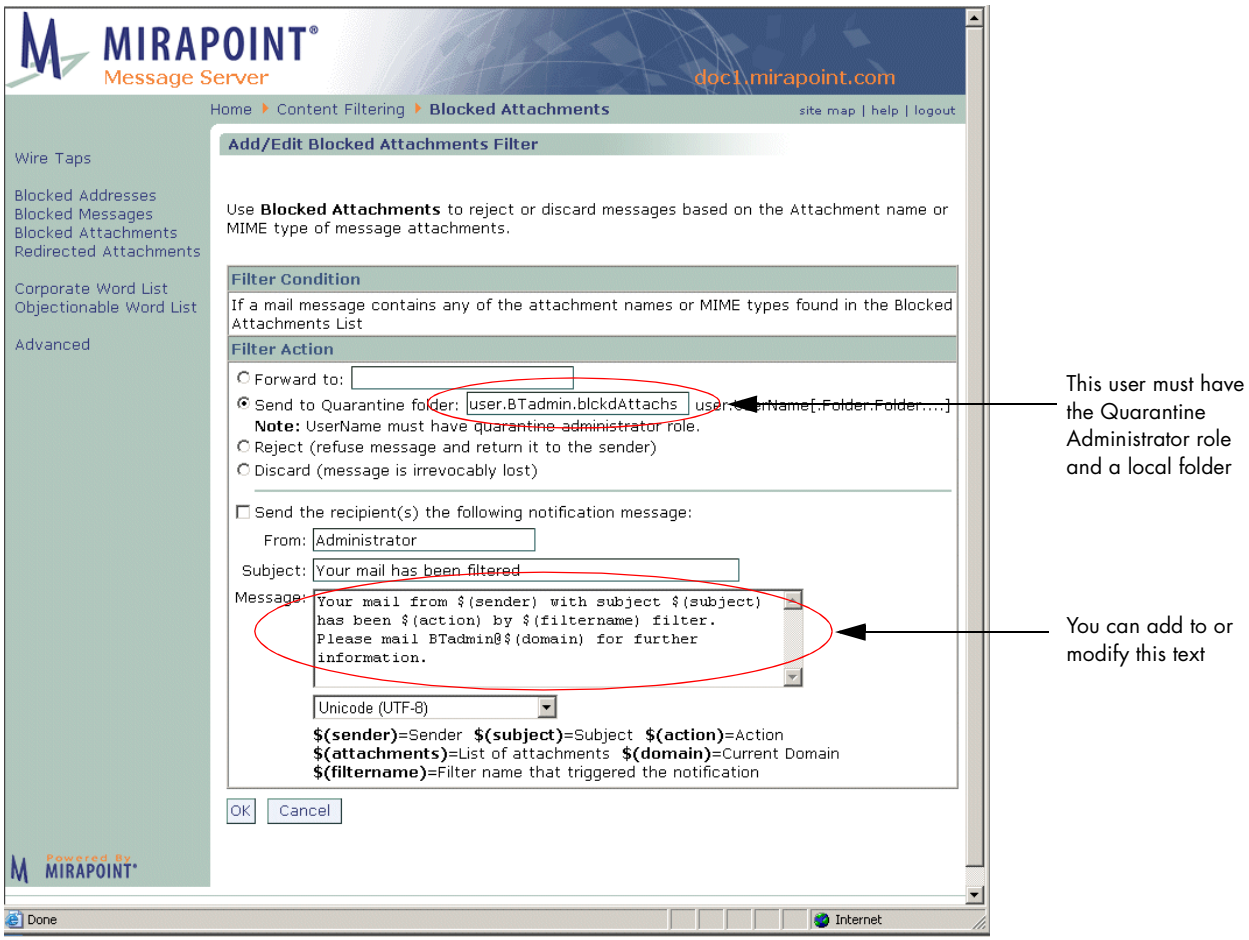


Figure 59 Content Filtering > Blocked Attachments Page

To create, edit, or delete a Blocked Attachments filter follow these steps on the **Content Filtering > Blocked Attachments** page (see Figure 59).

1. In the **Destination Domain** area specify the scope for the filter you are creating. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 for details on this option.

2. Create a **Blocked Attachments** list; to do this, see Managing a Filter List on page 254 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 257.
   - **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 241.
   - **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.
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; the **Blocked Attachments** page displays 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 filter list. Any incoming mail attachment with the name **iloveyou.vbs** is handled according to the selected filter action.

.vbs: Adds the file extension **.vbs** to your filter list. Any incoming mail attachment with a **.vbs** extension is handled according to the selected 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 filter list. Any incoming gif attachments, regardless of the file extension, are handled according to the selected 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 254. To understand this filter better, see About MIME and Filtering Attachments on page 239.

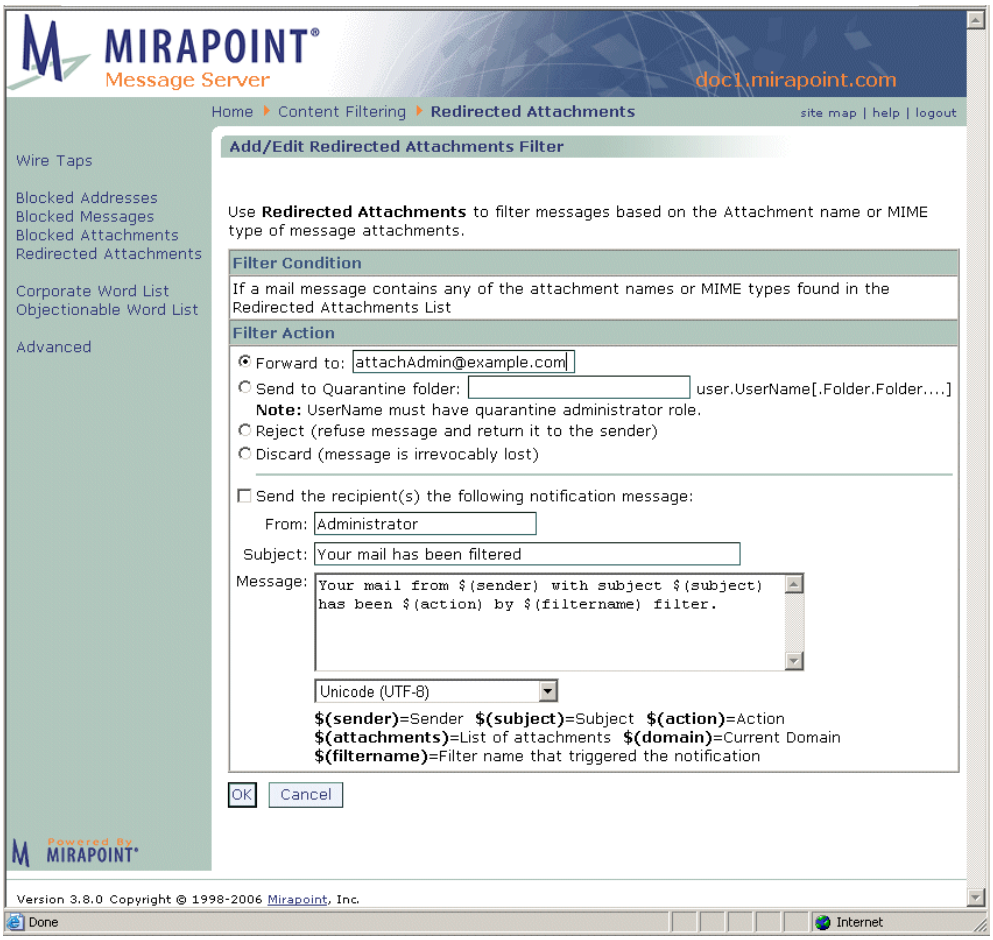


Figure 60 Content Filtering > Redirected Attachments Page

To create, edit, or delete a Redirected Attachments filter follow these steps on the **Content Filtering > Redirected Attachments** page (see Figure 60).

1. In the **Destination Domain** area specify the scope for the filter you are creating. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 for details on this option.
2. Create a **Redirected Attachments** list; to do this, see Managing a Filter List on page 254 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 257.
   - **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 241.
   - **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.

iloveyou.vbs: Adds the attachment file name **iloveyou.vbs** to your filter list. Any incoming mail attachment with the name **iloveyou.vbs** is handled according to the selected filter action.

.vbs: Adds the file extension **.vbs** to your filter list. Any incoming mail attachment with a **.vbs** extension is handled according to the selected 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 filter list. Any incoming gif attachments, regardless of the file extension, are handled according to the selected filter action.

You cannot separate entries with spaces or semi-colons; each entry must be on a separate line. Wildcards are not accepted.

Using Corporate Word Lists

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 254.

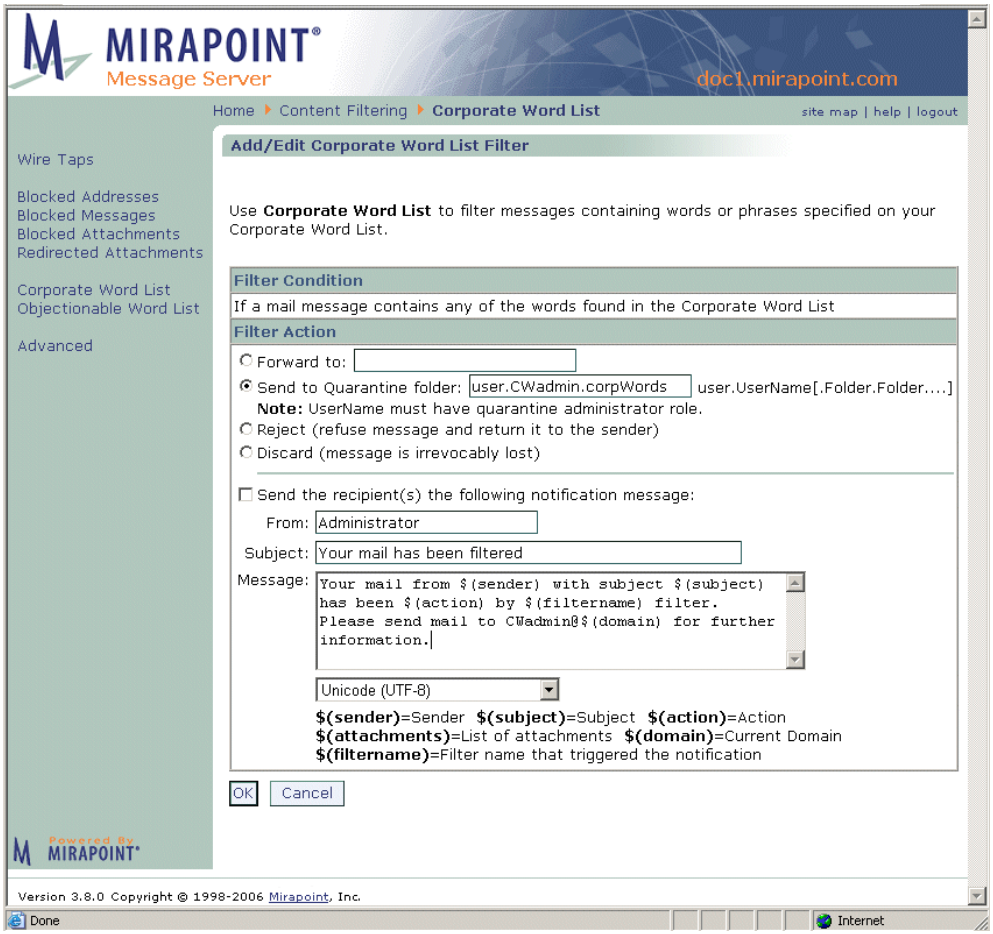


Figure 61 Content Filtering > Corporate Word List Page

To create, edit, or delete a Corporate Word List filter follow these steps on the **Content Filtering > Corporate Word List** page (see Figure 61).

1. In the **Destination Domain** area specify the scope for the filter you are creating. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 for details on this option.

2. Create a **Corporate Word** list; to do this, see Managing a Filter List on page 254 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 257.
   - **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 241.
   - **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 Lists

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 254.

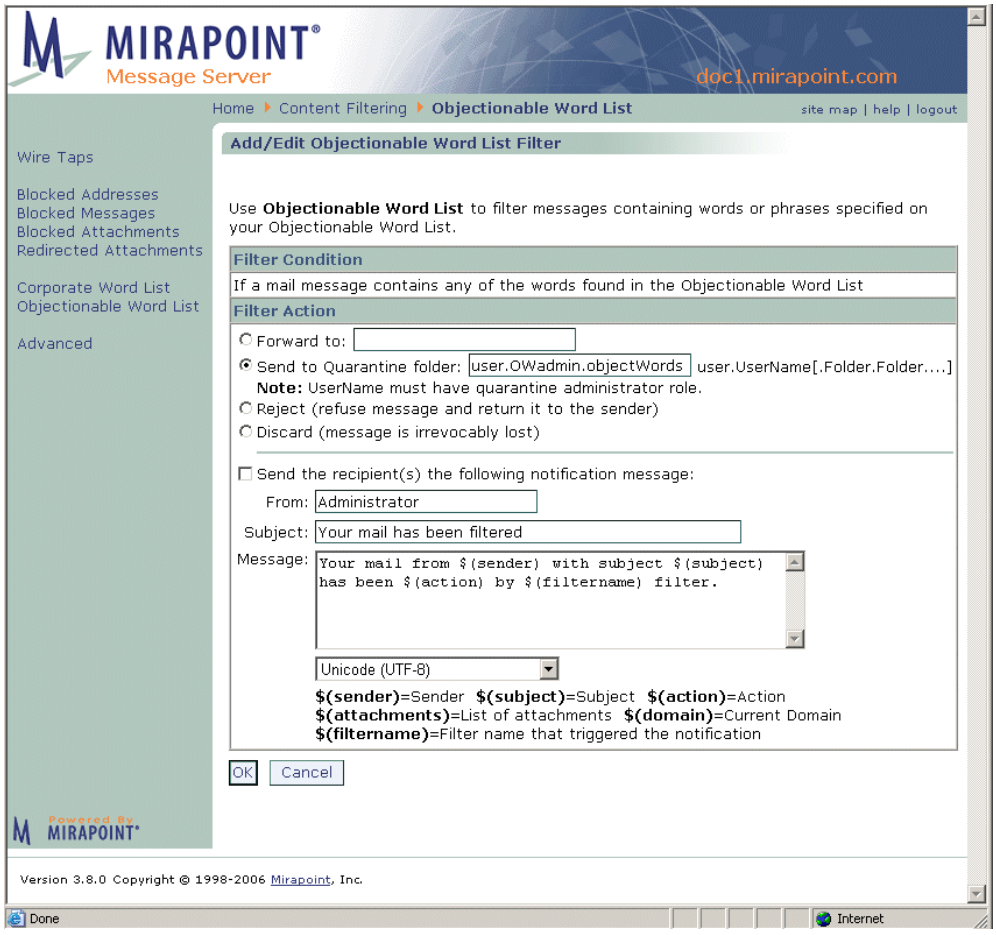


Figure 62 Content Filtering > Objectionable Word List Page

To create, edit, or delete a Objectionable Word List filter follow these steps on the **Content Filtering > Objectionable Word List** page (see Figure 62).

1. In the **Destination Domain** area specify the scope for the filter you are creating. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 for details on this option.

2. Create an **Objectionable Word** list; to do this, see Managing a Filter List on page 254 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 257.
   - **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 241.
   - **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.

8 Security Tasks

This chapter discusses Mirapoint security features, how to use the MailHurdle, Anti-Virus and Anti-Spam options, including Junk Mail Manager. 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. Includes Example System-Wide Antispam Filters.
- Configuring Multi-Listeners—How to add a SMTP multi-listener.
- Configuring NIC Failover—How to allow an appliance to switch seamlessly 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 7, 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 Layer

Figure 63 summarizes the network security layer.

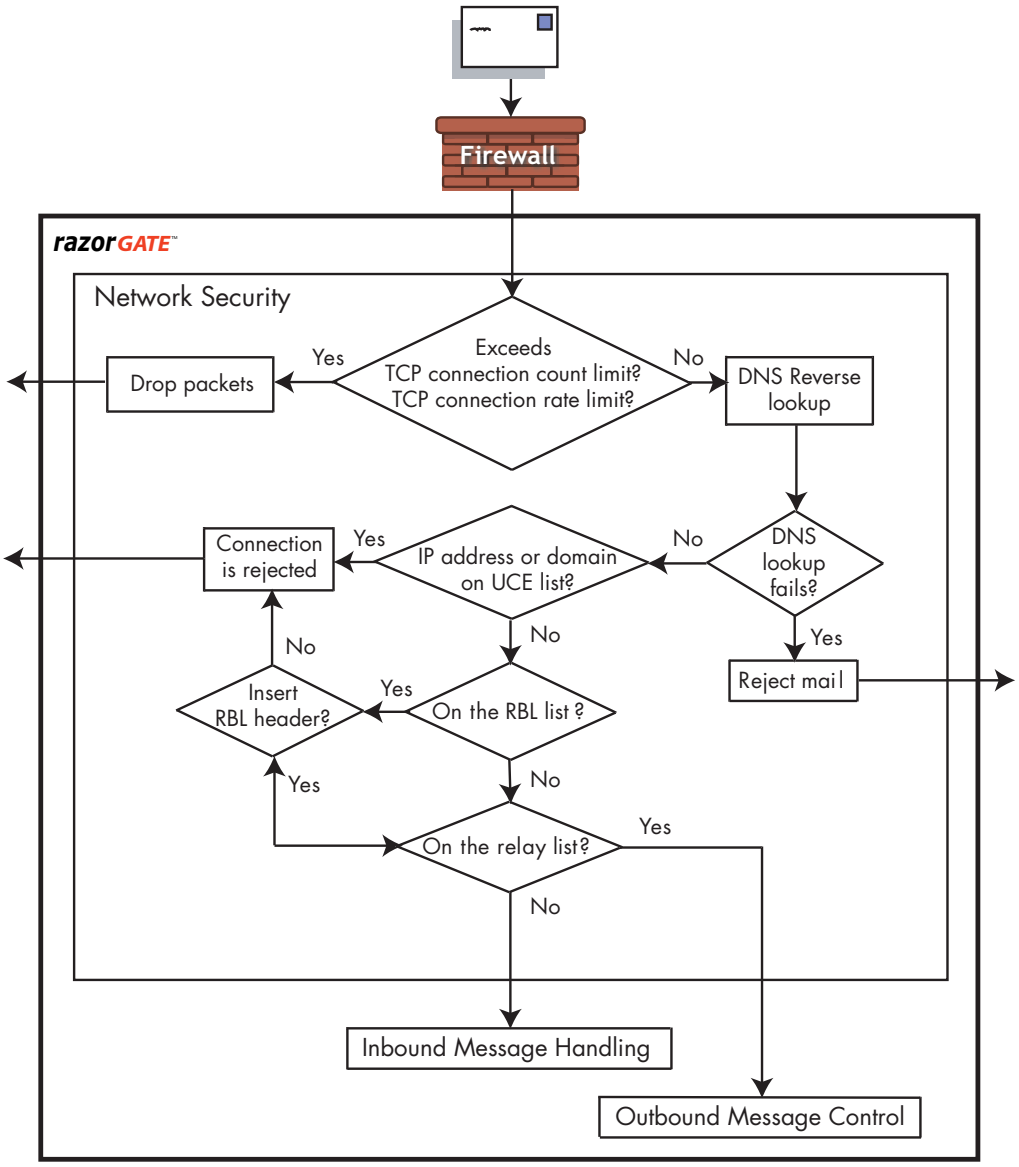


Figure 63 Network Security Layer

The network security layer is the first line of defense against attacks on your messaging system. Limiting TCP connections is done through the CLI (command line interface) only. 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.

Use the CLI (command line interface) to set:

- TCP rate limiting: See Limiting TCP Connections on page 60

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 318 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 317 for details.
- **Real-time Blackhole List** (RBL): You can make use of various services on the Internet keeping track of spamming domains; see Updating Your Real-time Blackhole List (RBL) on page 319 for details.

SMTP Layer Security

This section provides an example of what occurs at the SMTP level when an email transmission is initiated and explains Mirapoint options for security.

Not all possible SMTP actions or Mirapoint options are included. This example uses “Helo” rather than “Ehlo;” the possible responses to “Ehlo” are much longer and more varied.

1. An email is sent to a Mirapoint system: SMTP connection occurs on port 25. RazorGate TCP connection limits can help prevent Denial of Service Attacks; see Limiting TCP Connections on page 60 for details.
2. RazorGate responds with:
   `220 systemname ESMTP Mirapoint mos version; date time`
3. Connecting server responds with:
   `HELO connecting mail.domain.com`
   RazorGate does syntax verification, IP address checks, remembers errors, introduces delays.
4. With a good connection, RazorGate reverse DNS lookup allows this response with the correct connection IP address:
   `250 systemname Hello pc.domain.com[IP address], pleased to meet you`
5. Connecting mail server responds with:
   `MAIL FROM: user@domain.com`
   RazorGate checks the IP address against UCE (unsolicited commercial email) block list (Blocked Addresses), RBL List, SSL enforcement, SMTP Auth enforcement, LDAP masquerade, and Sender Check. These restrictions are set on the **System > Services > SMTP > Main Configuration** and **Anti-Spam > Blocked Senders** and **RBL Host List** pages.
6. If error is found, RazorGate responds with an error message, for example:
   `550 domain is blacklisted, contact your postmaster`
   With no error, RazorGate responds with:
   `250 Sender OK`

7. Connecting server responds with:
   `RCPT TO: user@localdomain.com`
   RazorGate can verify the recipient, check for open relay attempt, and MailHurdle blocking. Set recipient checking on the **System > Services > SMTP > Main Configuration** page, disallow open relays on the **Anti-Spam > Relay List** page, and configure MailHurdle on the **Anti-Spam > MailHurdle** pages.
8. On MailHurdle block, RazorGate responds with:
   `451 user@localdomain.com...Requested action not taken: mailbox unavailable`
   Without MailHurdle block, or other error, RazorGate responds with:
   `250 Recipient OK`
9. Connecting server responds with:
   `DATA`
10. RazorGate responds with:
    `354 Enter message, followed by a "."`
11. Connecting server responds with header and body of message:
    ```
    From: <user@domain.com> Joe User
    To: <user@localdomain.com> Susan User
    Subject: Hello Susan

    How are you?
    .
    ```
12. RazorGate responds with:
    `250 message accepted for delivery`
13. Connecting server responds with:
    `QUIT`

This example conversation demonstrates at what points in an email transmission the different RazorGate features take affect. For more information regarding SMTP, see RFC 821.

Inbound Message Handling Layer

Figure 64 summarizes the inbound message handling layer.

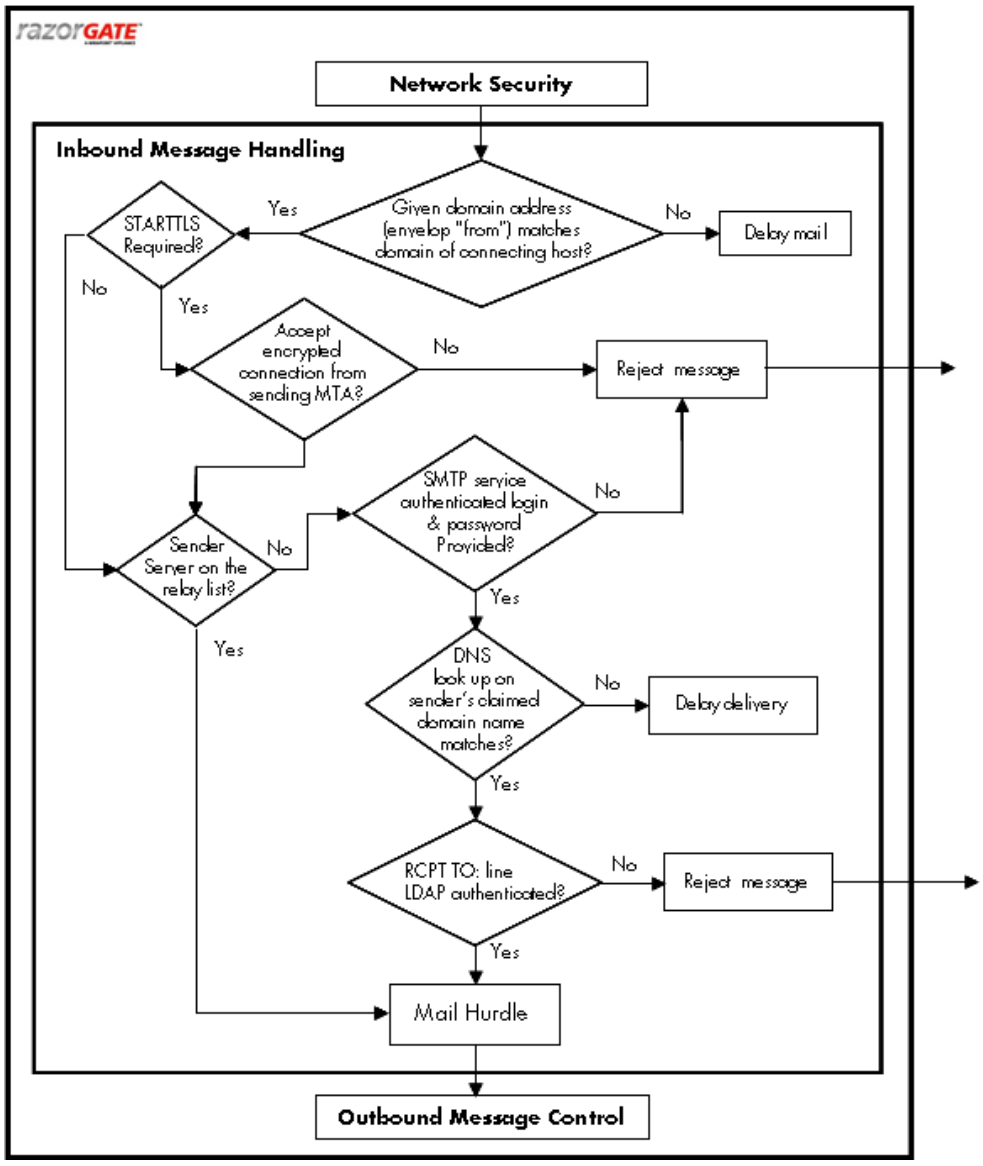


Figure 64 Inbound Traffic Handling Layer

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. If setting the SSL version, cipher suite, or SMTPS, is desired, please see the *Mirapoint Administrator's Protocol Reference* SSL chapter for new commands.

- **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 282 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 252 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 175 for details.

Message Content Handling Layer

Figure 65 summarizes the message content control layer.

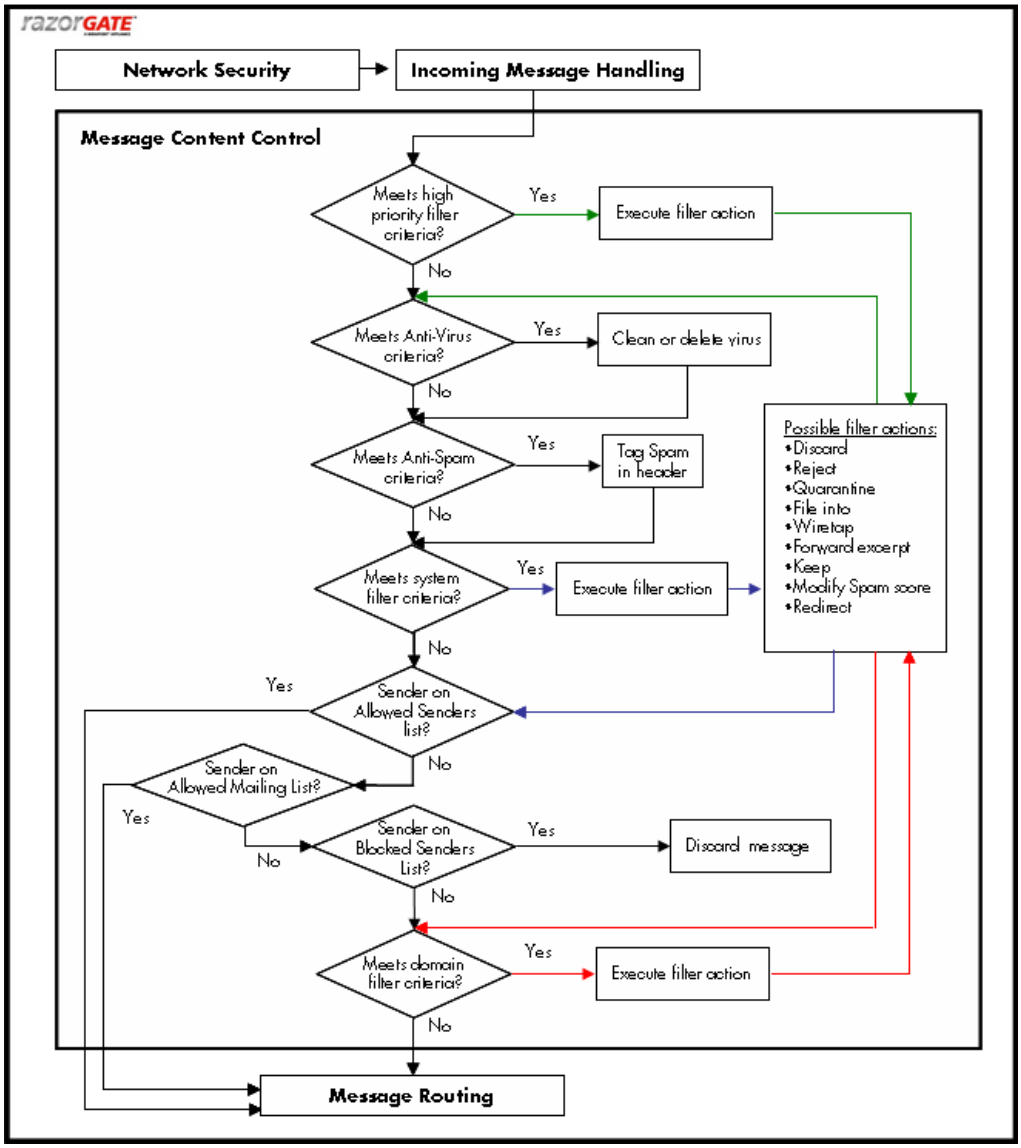


Figure 65 Message Content Control

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 238 for details.
- **Antivirus scanning**: Configure up to three antivirus engines to keep viruses out; see Using Antivirus Scanning on page 288 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 236 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 Layer

Figure 66 summarizes the outbound message control layer.

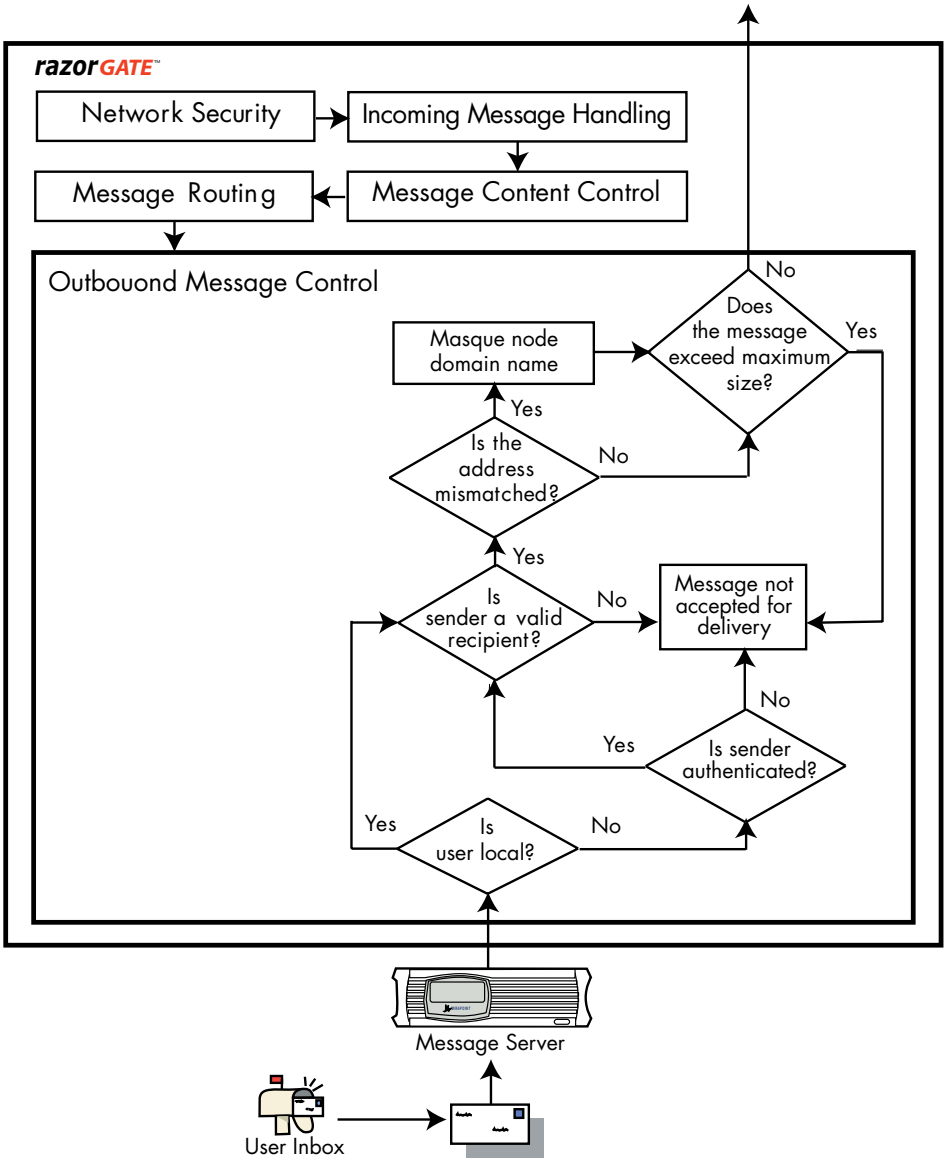


Figure 66 Outbound Message Control Layer

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 Smtpauth**: 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 Smtpauth; 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, called *triplets*:

- **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 67 summarizes MailHurdle processing during inbound message handling.

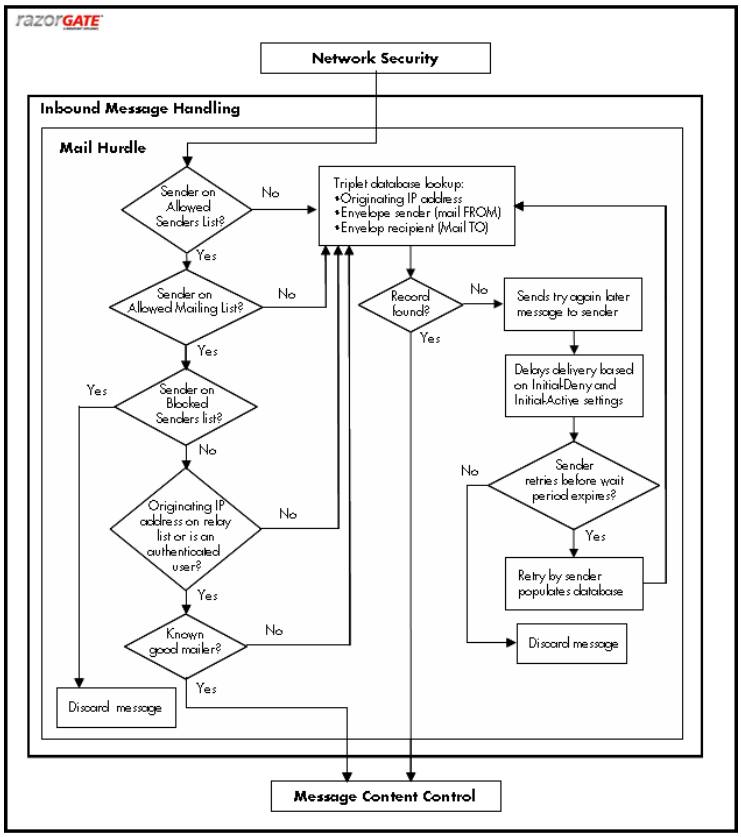


Figure 67 MailHurdle Processing for Inbound Messages

If you are deploying MailHurdle in an existing system, see Preparing for MailHurdle Deployment on page 119.

Modifying MailHurdle

Use the **Anti-Spam > MailHurdle > Configuration** page (shown in Figure 68) 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.

Figure 68 MailHurdle Configuration Page

To modify basic MailHurdle settings, follow these steps on the **MailHurdle > Configuration** page; see Figure 68 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 (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 retrys 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. 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).
4. 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 69) to specify which machines can query the MailHurdle server; each machine with the MailHurdle service should be an Allowed Host.

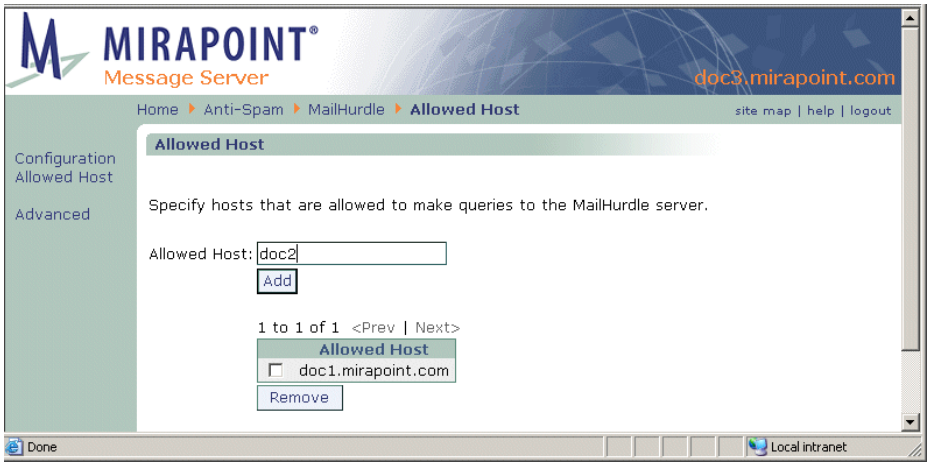


Figure 69 MailHurdle Allowed Hosts Page

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 MailHurdle Advanced Options

Use the **Anti-Spam > MailHurdle > Advanced** page (see Figure 70) to set filtering prioritization and other options, and also to search for triplets or manually flush the triplet cache.

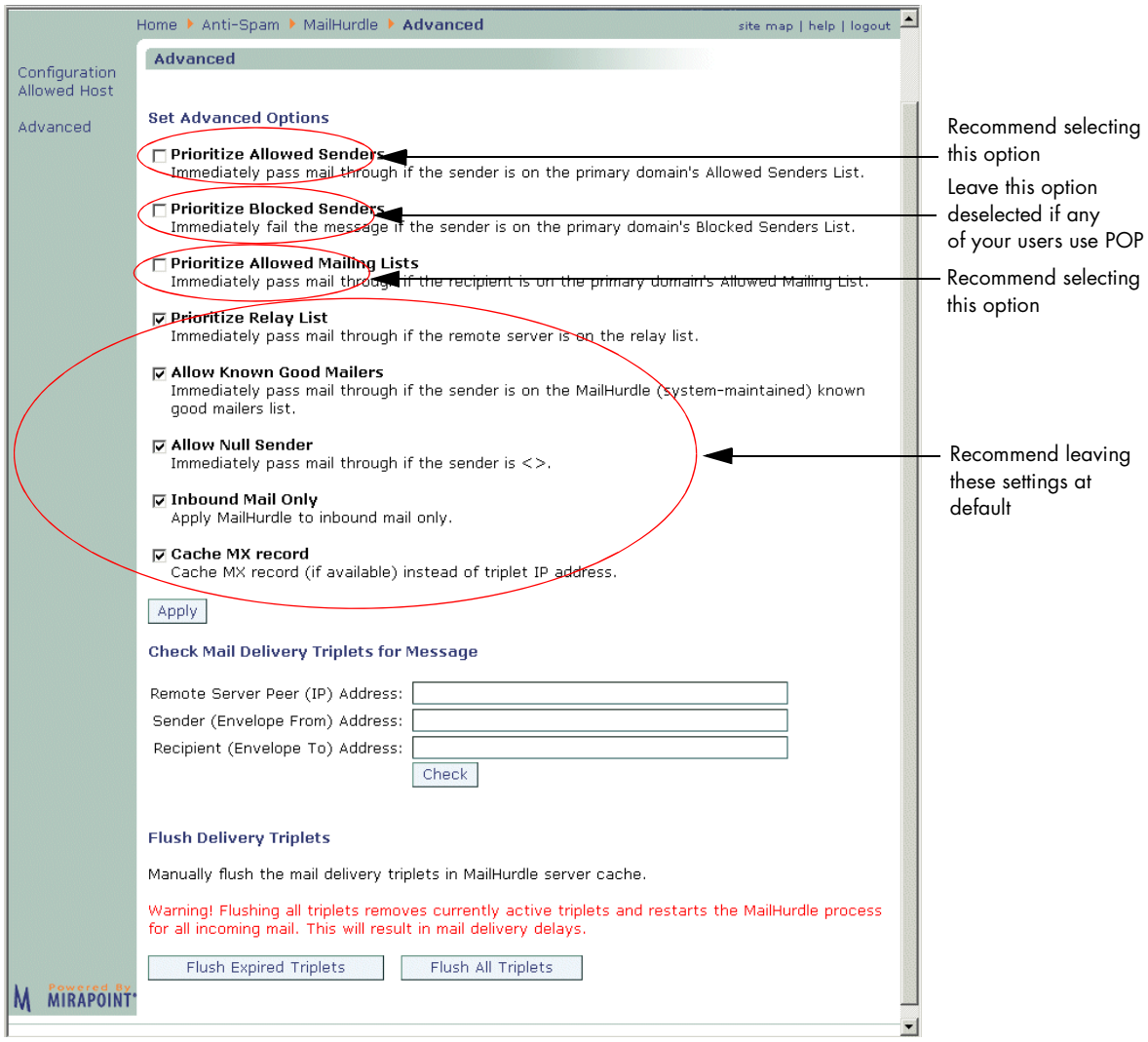


Figure 70 MailHurdle Advanced Page, Detail

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. Mirapoint recommends selecting this option.
- **Prioritize Blocked Senders** (deselected by default). Applies your set Blocked Senders list action immediately to mail from those senders without utilizing MailHurdle. Mirapoint recommends leaving this option deselected 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. Mirapoint recommends selecting this option.

Mirapoint recommends 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 Antispam Scanning on page 308.
- **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 (mail addressed to a domain listed on the system). 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).

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 71). This can be useful if you are trying to diagnose what happened to a message that a user was expecting, but did not receive.

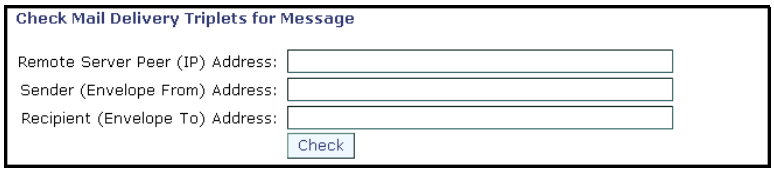


Figure 71 MailHurdle Check for Message Advanced Page Detail

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 162.

Flushing Mail Delivery Triplets

You can manually flush the triplet cache from the **MailHurdle > Advanced** page, shown in Figure 72.

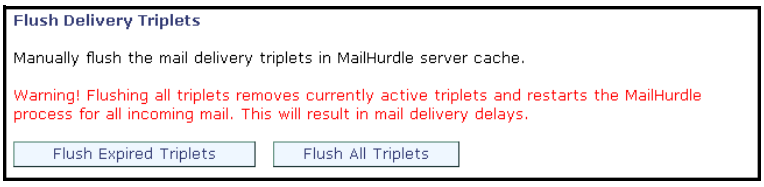


Figure 72 MailHurdle Flush Triplets Advanced Page Detail

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 290 and Modifying Predictive-based (RAPID) Anti-Virus on page 299.

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, Sohpos 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 examine 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 **Antivirus Set Quarantinedelay** command. For more information, see the *Mirapoint Administration Protocol Reference*.

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 203.

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 antivirus work see About Signature-Based Anti-Virus on page 289.

Mirapoint recommends 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 73 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 290 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 289 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.

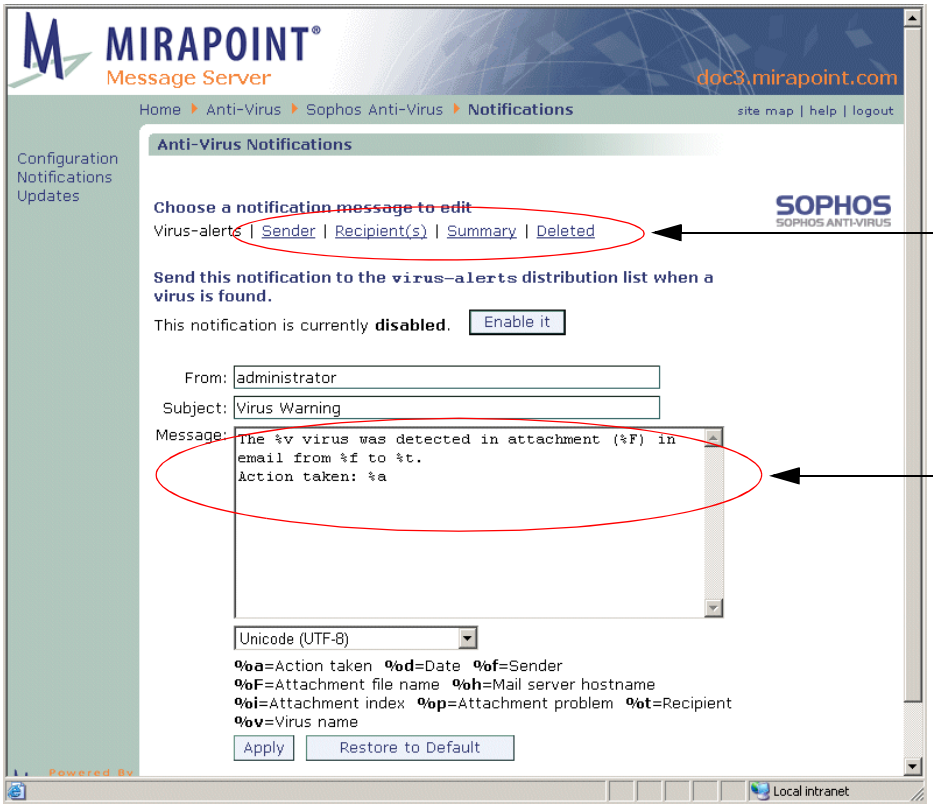


Figure 74 Anti-Virus Signature Engine Notifications Page

The following graphics depict the various notification messages that can be configured.

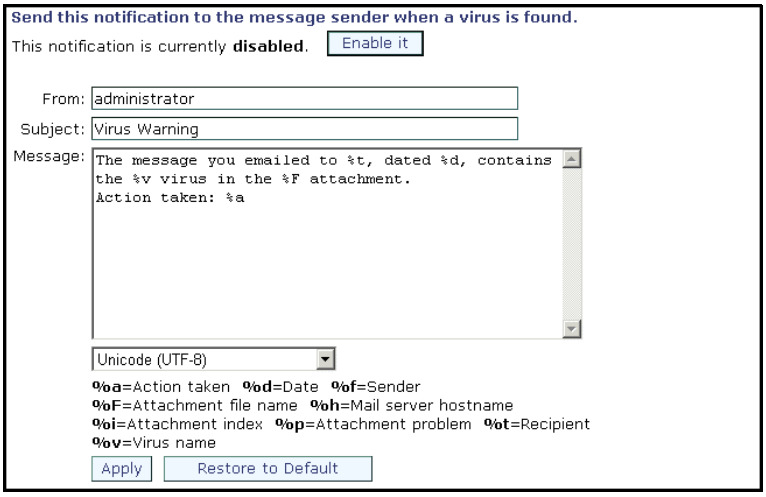


Figure 75 Anti-Virus SENDER Message, Notification Page Detail

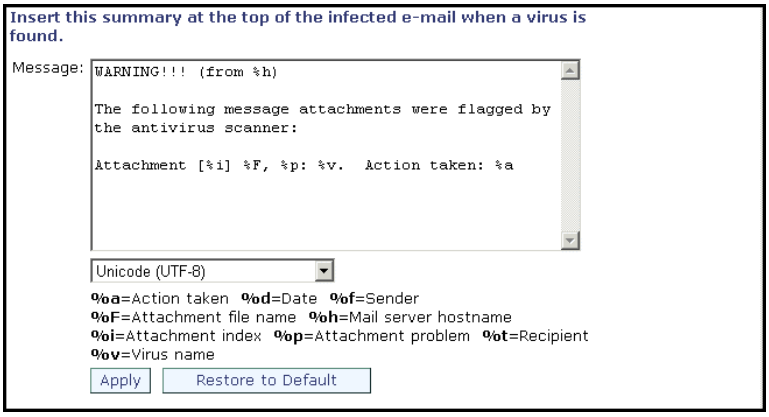


Figure 76 Anti-Virus SUMMARY Message, Notification Page Detail

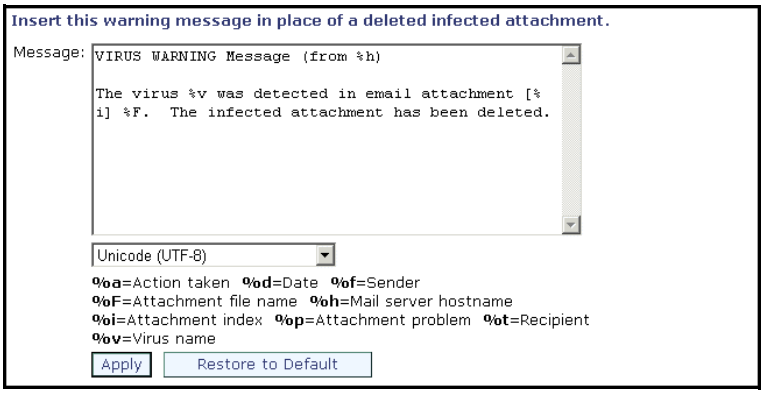


Figure 77 Anti-Virus DELETED Message, Notification Page Detail

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 75):

   - **Virus Alerts** (default): When a virus is detected, this notification is sent to the **virus-alerts** distribution list. See Figure 74 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 75 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 76 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 77 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.

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.

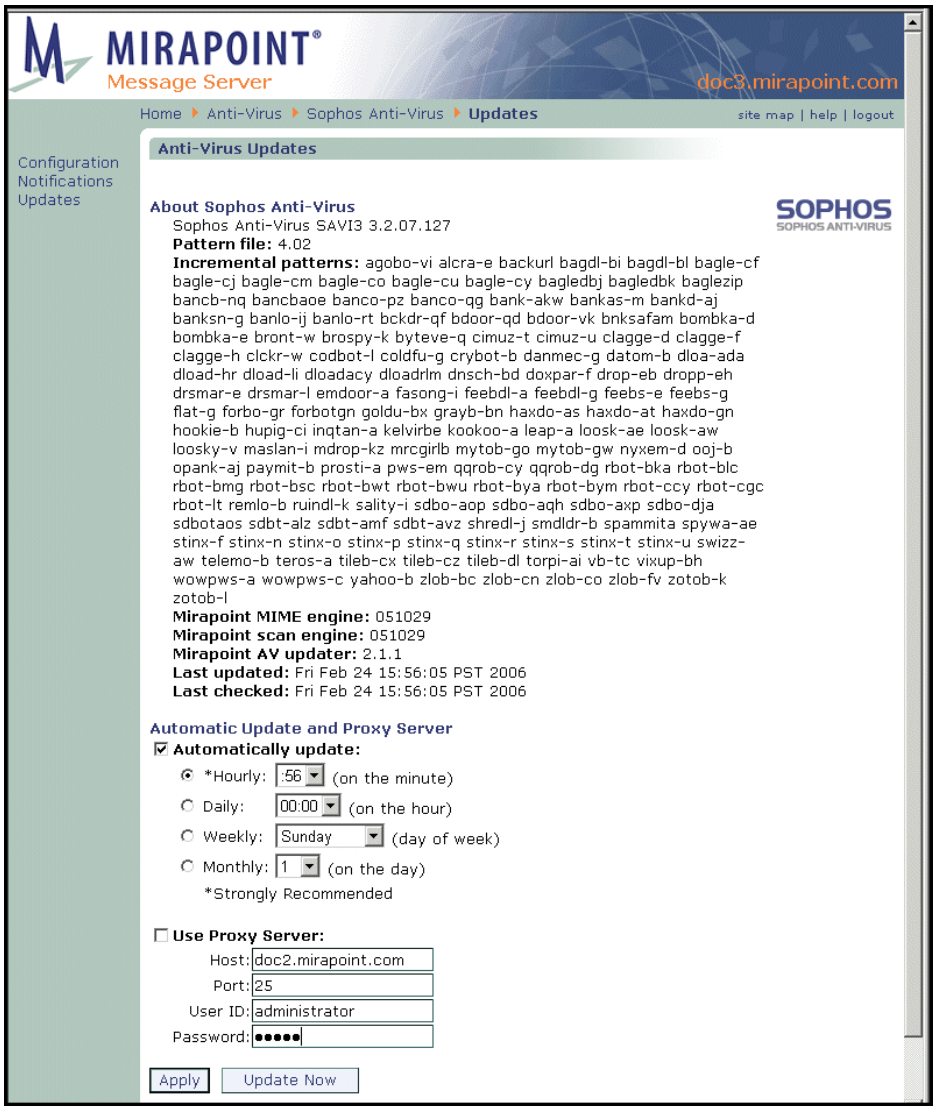


Figure 78 Anti-Virus Signature Engine Updates Page

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 menu, on that minute, every hour, the utility retrieves new virus information.
   - **Daily**: Choose an hour from the drop-down menu, on that hour, every day, the utility retrieves new virus information.
   - **Weekly**: Choose a day from the drop-down menu, on that day (at midnight), every week, the utility retrieves new virus information.
   - **Monthly**: Choose a day from the drop-down menu, 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 78 for an example. The following information, as well as the version number of that antivirus pattern file, displays. ***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. 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 289 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.

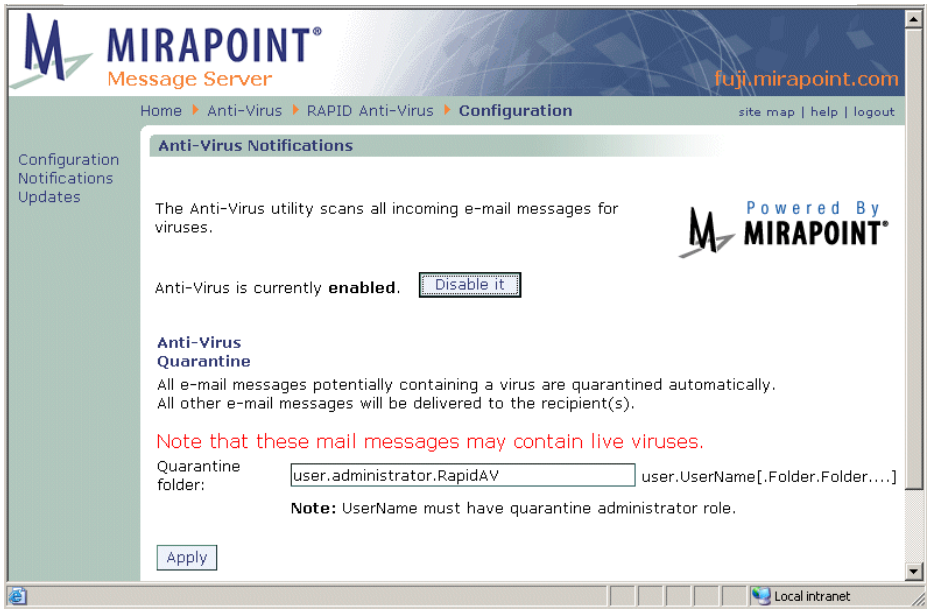


Figure 79 Anti-Virus Predictive Engine (RAPID) Configuration Page

There are some file extensions that always trigger the RAPID antivirus quarantine action; those extensions are:

- .scr
- .pif
- .com
- .exe
- .vbs
- .bat
- .cmd
- .dll
- .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 79 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. For more information, see the *Mirapoint Administration Protocol Reference*.

Setting Notifications for RAPID Anti-Virus

Mirapoint highly recommends that **RAPID Anti-Virus** notifications be configured to let users know that their mail is being quarantined due to a potential virus.

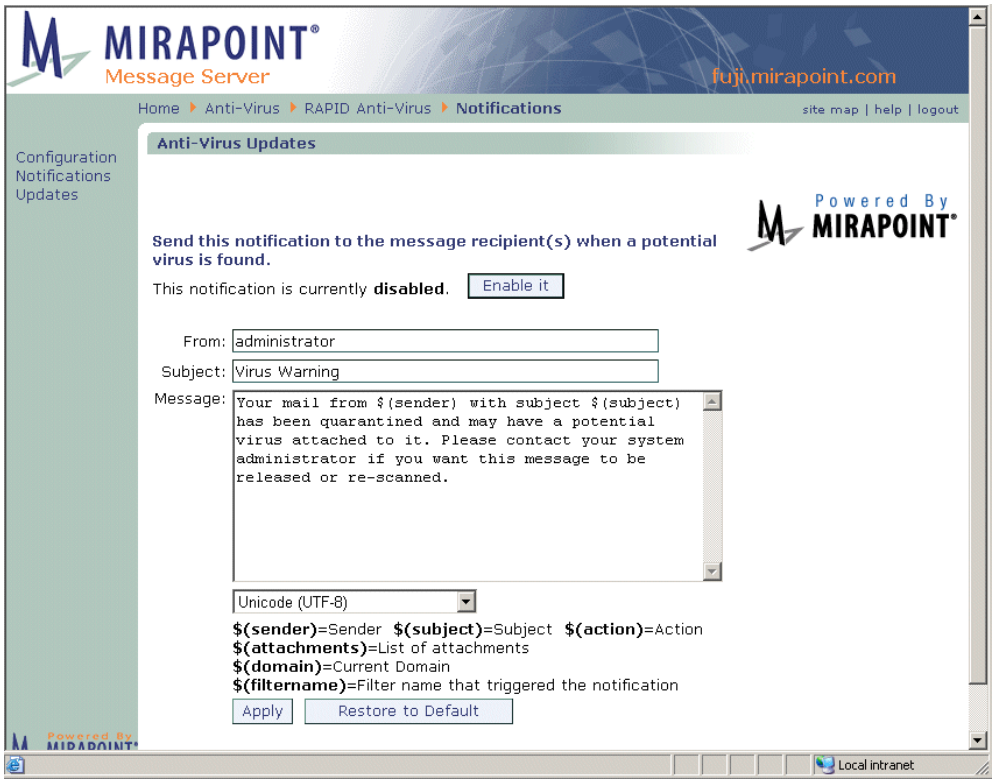


Figure 80 Anti-Virus Predictive Engine (RAPID) Notifications Page

To specify antivirus scanning notifications follow these steps on the **Anti-Virus > RAPID > Notifications** page; see Figure 80 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. 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 301 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 81 for an example. 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.

RAPID AV updates are not automatic, this is because RAPID AV updates may be seen as rarely as once a quarter, and if missed, are unlikely to affect accuracy, since detection is done remotely at the detection center. However, Mirapoint recommends setting automatic updates for RAPID AV as well as other AV engines you may be using.

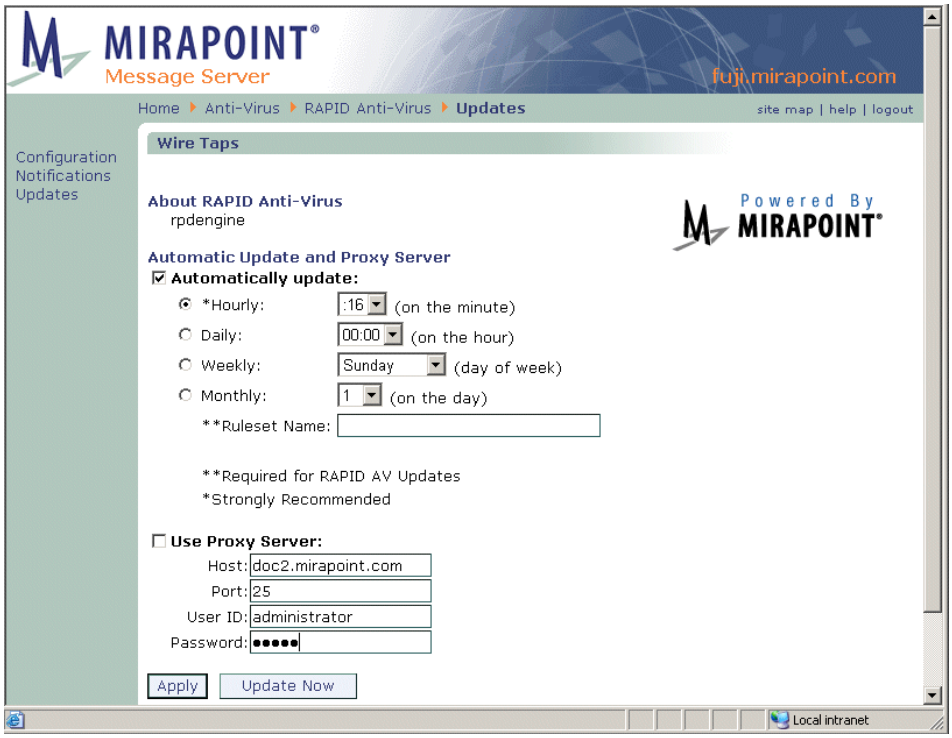


Figure 81 Anti-Virus Predictive Engine (RAPID) Updates Page

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 81.

1. Check the **Automatically update** checkbox and specify one:
   - **Hourly**: Choose a minute from the drop-down menu. On that minute, every hour, the utility retrieves new virus information.
   - **Daily**: Choose an hour from the drop-down menu. On that hour, every day, the utility retrieves new virus information.
   - **Weekly**: Choose a day from the drop-down menu. At midnight on that day, every week, the utility retrieves new virus information.
   - **Monthly**: Choose a day from the drop-down menu. At midnight on that day, every month, the utility retrieves new virus information.
2. Specify a **Ruleset Name** if no ruleset is selected.

   Result: The new ruleset displays in a list. Click the ruleset's **Delete** icon . to remove it.

   As they are developed, Mirapoint adds named Rulesets to the Mirapoint Support site at http://support.mirapoint.com.
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.

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 81. 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 antispam 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 Antispam Scanning—Enable/disable Anti-Spam scanning, specify how severely the utility should judge incoming mail for spam, and set other defaults.
- Scheduling Updates for Antispam 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 whose mail will 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 Real-time 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.
- Example System-Wide Antispam Filters—Use the **Content Filtering > Advanced** page to enhance antispam scanning.

Antispam 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 Antispam Scanning on page 306.

Principal Edition vs. Signature Edition

The antispam scanner uses one or two (depending on licensing) techniques to categorize mail as junk mail (spam): **Principal Edition** or **Signature Edition**.

Principal Edition antispam compares all incoming email messages to a set of rules. The more rules the message matches, the higher the junk mail UCE (unsolicited commercial email) score it is assigned. Any UCE score over the junk mail **Threshold** (50, by default) categorizes the mail as spam and triggers the **Junk Mail** filter. The rule group updates for Pricipal 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 junk mail **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 junk mail. This header is inserted when a message is scored above the junk mail **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 junk mail **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 162.

If you license both scanners, the higher score given by either technique is used for the message status. Using the CLI command **Uce Setoption Multienginebulkonly** you can set your Anti-Spam scanners to work together; only messages tagged as "Bulk" by Signature Edition are scanned by Principal Edition. For more details, see the *Mirapoint Administrator's Protocol Reference* book, Uce chapter.

If you add an additional antispam scanner, be sure to go the **Anti-Spam Updates** page for that scanner and click **Update Now** to get the most recent files for that scanner.

To learn more about the antispam threshold, see About the Antispam Scanning Rules and Threshold on page 240.

About the Junk Mail Filter

The **Junk Mail** filter, when ON, tells the Anti-Spam scanner what to do with mail categorized as junk mail (spam). The default action, **Move to the Junk Mail folder**, allows users to check their junk mail 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. Notify users that they 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.

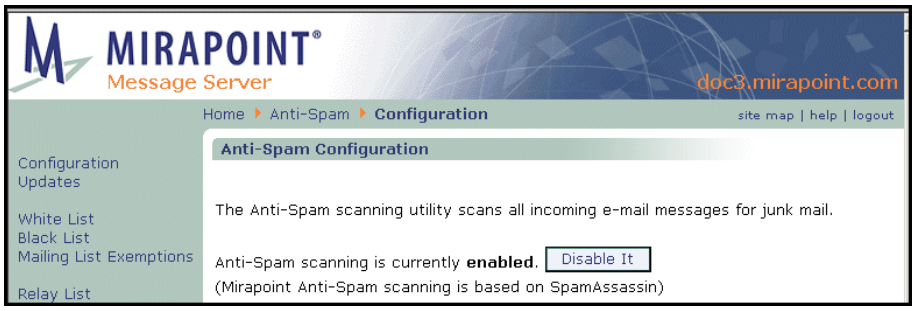


Figure 82 Anti-Spam Configuration Page Detail

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.

How the Anti-Spam Features Are Applied

Mirapoint's antispam features are applied in this order:

1. Unsolicited Commercial Email (UCE) blocking
2. Anti-relaying protections (relay list)
3. Anti-harvesting measures
4. Real-time Blackhole Lists (RBLs)
5. Junk Mail scanner
6. Domain white list
7. Domain black list
8. Domain-level content filters
9. Personal Allowed Senders and Blocked Senders (not available for RG 100s)
10. Junk Mail Filter (not available for RG 100s)

UCE blocking filters out mail from defined spam site domains and IP addresses. Further anti-relaying and anti-harvesting measures are applied before the message is handed off to the RBL filters.

RBL definitions are folded into the antispam scanner and may affect the message's junkmail score.

After a message is processed through the antispam scanner, if it is tagged as junkmail, it is given an **X-JunkMail** header.

Messages with the **X-JunkMail** header are adjusted by domain-level Allowed Sender and Blocked Sender lists before they are processed by domain-level message content filters. The final step is scanning through the personal-level Allowed Sender lists, Blocked Sender lists, and message filters.

Modifying Antispam Scanning

On the **Anti-Spam > Configuration** page (see Figure 83 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.

Figure 83 Anti-Spam Configuration Page Detail, Options

To modify antispam scanning, follow these steps on the **Anti-Spam > Configuration** page; see Figure 83 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 146. Click **Hide Junk Mail Statistics** to make the graph go away.

3. Set these antispam scanning options:

   - **Threshold Number**, text box option: Adjust the antispam 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 240 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** antispam scanner. For details on this header, see Reading Message Envelopes and Headers on page 162.
- **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 antispam 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*) (Principal 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 162.

Scheduling Updates for Antispam 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** antispam 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.

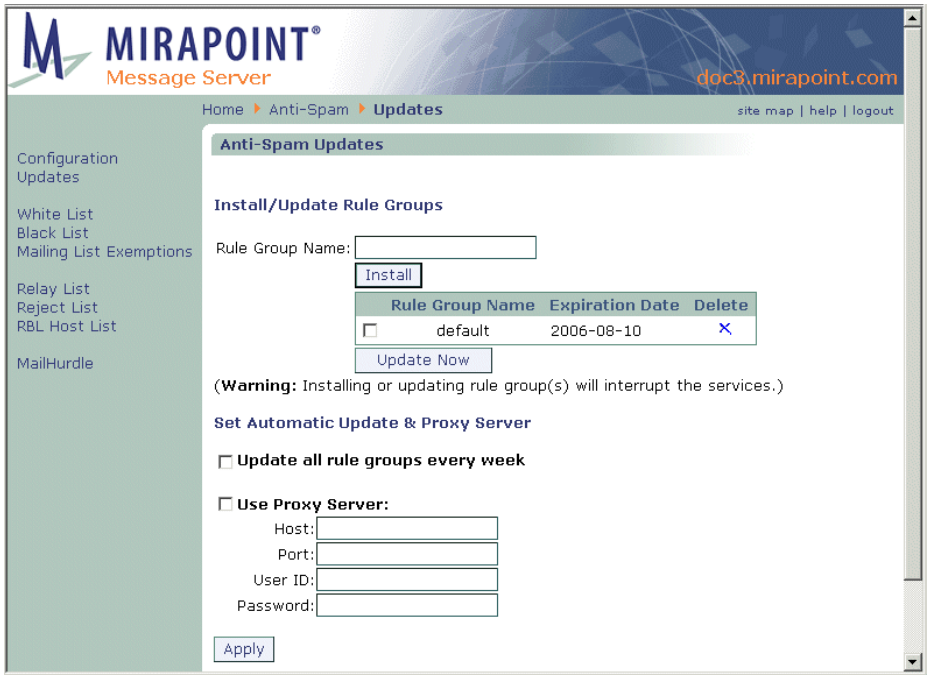


Figure 84 Anti-Spam Updates Page

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 84 for an example).

1. Enter the Rule Group Name and click **Install**.
   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.

   As they are developed, Mirapoint adds named Rule Groups to the Mirapoint Support site at http://support.mirapoint.com/.
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 junk mail 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 junk mail. 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**.

The **Allowed Senders** 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 185. 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 305. This does not apply to Junk Mail Manager, or non-WebMail, users.

The Allowed Senders filter does not do dot-to-underbar mapping so it might be necessary to create both a dot (.) 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 230 for details on using wildcards with filters.

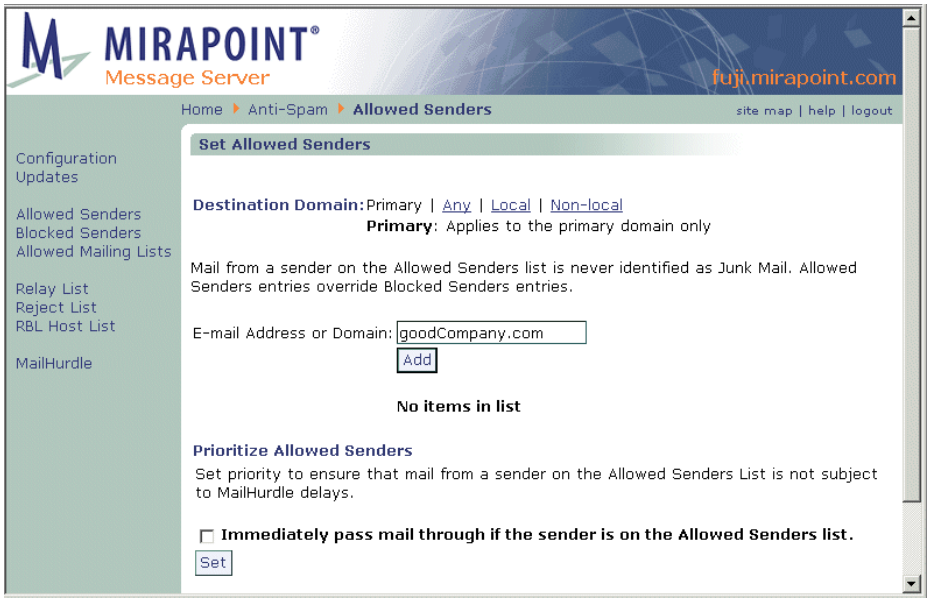


Figure 85 Anti-Spam Allowed Senders Page

To create an Allowed Senders filter follow these steps on the **Anti-Spam > Allowed Senders** page; see Figure 85 for an example.

1. In the **Destination Domain** area specify the scope for the filter. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 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**. For details on using wildcards, see Using Patterns on page 230. 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 may still 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. See How the Anti-Spam Features Are Applied on page 305 for details.

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 junk mail.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 185. 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 305. This does not apply to Junk Mail Manager, or non-WebMail, users.

The Blocked Senders filter does not do dot-to-underbar mapping so it might be necessary to create both a dot (.) 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 230 for details on using wildcards with filters.

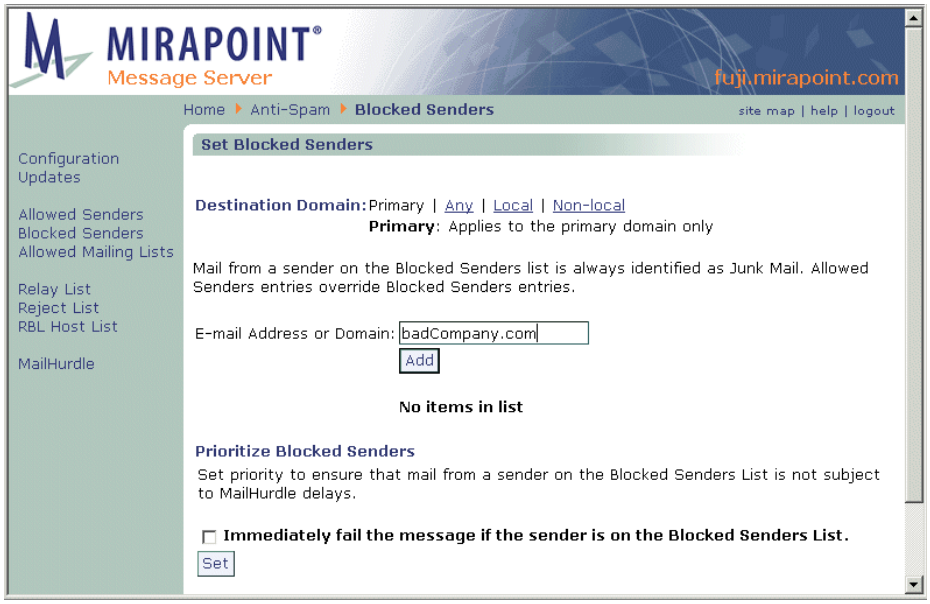


Figure 86 Anti-Spam Blocked Senders Page

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. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 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**. For details on using wildcards, see Using Patterns on page 230. 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.g

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 "whitelistto."

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 185. 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 305. This does not apply to Junk Mail Manager, or non-WebMail, users.

The Allowed Mailing Lists filter does not do dot-to-underbar mapping so it might be necessary to create both a dot (.) 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 230 for details on using wildcards with filters.

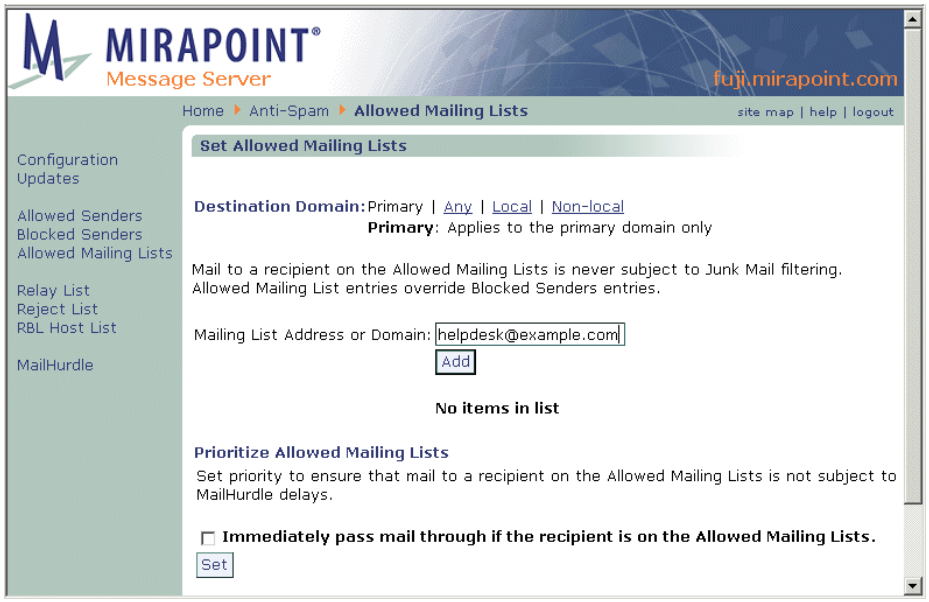


Figure 87 Anti-Spam Allowed Mailing Lists Page

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. 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 processes only mail addressed to the selected domain. See About the Destination Domain Options on page 238 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**. for details on using wildcards, see Using Patterns on page 230. 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.

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.

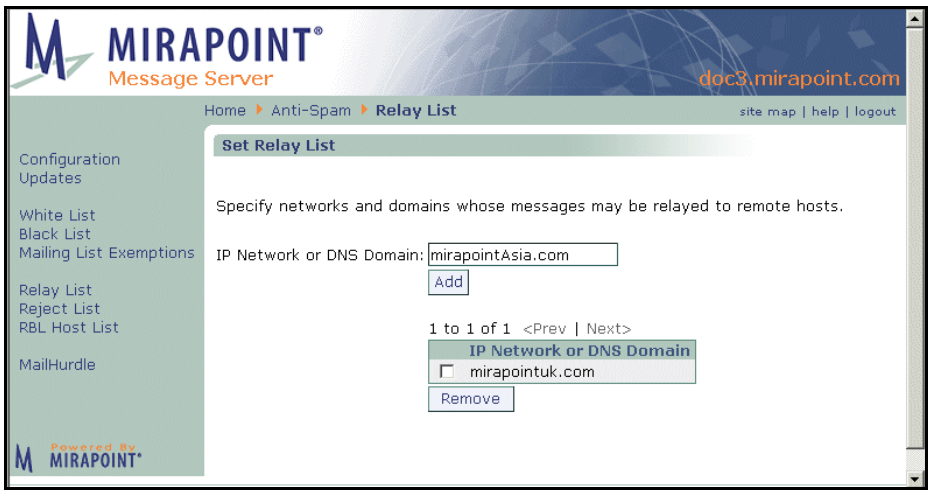


Figure 88 Anti-Spam Relay List Page

To configure a Relay List follow these steps on the **Anti-Spam > Relay List** page. See Figure 88 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.

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.)

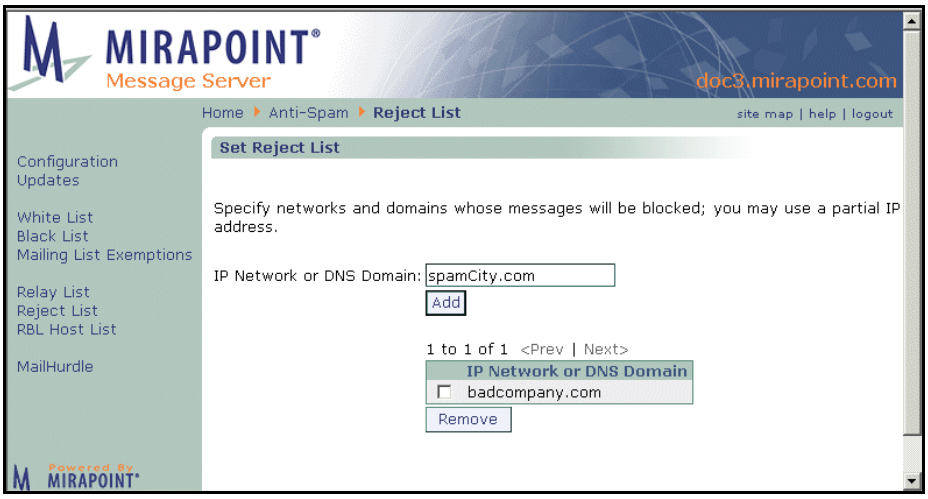


Figure 89 Anti-Spam Reject List Page

To configure a Reject List follow these steps on the **Anti-Spam > Reject List** page. See Figure 89 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 Real-time 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. 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 240), 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.

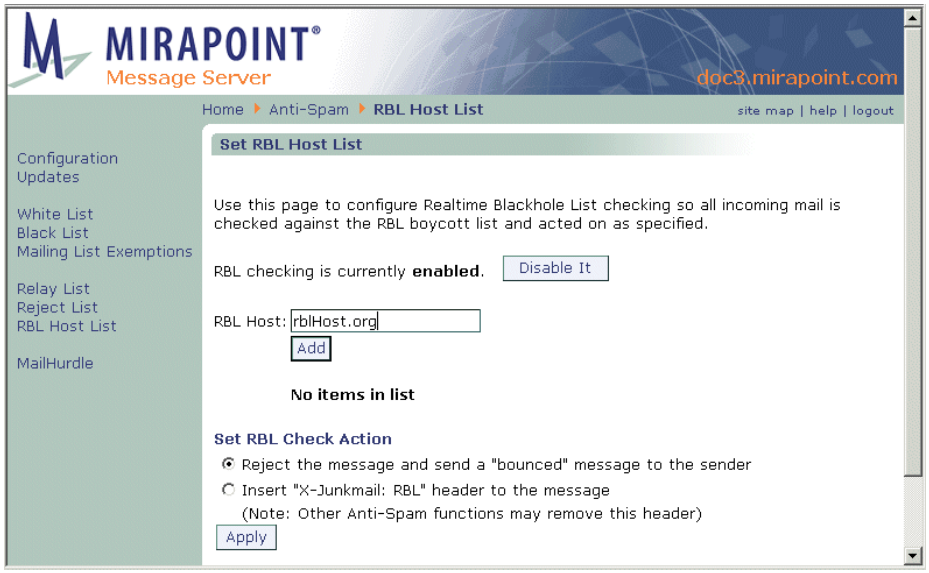


Figure 90 Anti-Spam RBL Host Page

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 90 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, search for "RBL" in the Mirapoint Knowledge Base at http://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.

Filters can be created that act on the **X-Junkmail** header. For details see Creating a Message Filter on page 243.

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.

Example System-Wide Antispam Filters

You can use the **Content Filtering > Advanced** page to create filters to enhance antispam scanning. This section provides some examples. For full details on creating these filters, see Creating a Message Filter on page 243.

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 RAPID-tagged spam messages:

Filter Name: DiscardUceScoreGreaterThan299
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. This is useful in conjunction with RAPID (Signature Edition) antispam scanning to automatically quarantine messages scored over 50 (Suspect) by RAPID.

By using a Quarantine Administrator address, these messages can be examined and released back to the mail stream.

Filter Name: QuarantineSuspectMail
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: DiscardDeletedViruses
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 288), 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: DiscardSobigVirusDeletedMessages
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: DiscardSobigVirusDeletedMessagesWC
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 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: DiscardJpegs
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

Filtering to Quarantine All Executable Files

This filter moves all exe files, common in spam, to a folder named "Qmail" for the "spamQA" user, but allows mail from internal distribution lists that begin with "dl". The purpose of this filter is to reduce spam using exe files. The "dl-" exception is added to safeguard internal mail from known sources using executables.

The "spamQA" user would require the Quarantine Administrator role in order to release these messages.

Filter Name: QuarantineExes
If all of these conditions are met
Attachment Type matches "exe"

AND (use **More>>** to add another condition)
Attachment Type matches-not "text/plain"

AND (use **More>>** to add another condition)
To/cc does not contain "dl-"
Send to Quarantine user.spamQA.Qmail
Do not apply any more filters to this message if action is taken

Filtering to Reject All RBL-Tagged Messages

This filter rejects all messages that have received the RBL header during antispam scanning (you must choose the **Insert "X-Junkmail: RBL" header to the message** option on the **Home > AntiSpam > Set RBL Host List** page first). This is useful in providing a log entry whenever a message receives the RBL tag.

Filter Name: RejectRblMessages
If all of these conditions are met
X-Junkmail contains RBL
Reject
Do not apply any more filters to this message if action is taken

Configuring Multi-Listeners

As of release 3.8.1, Mirapoint systems can listen for SMTP connections on multiple ports and interfaces at once. Previously, it was possible to change the **Listenport**, but only one SMTP port was allowed at a time.

Imagine that you want to set up a Message Server that accepts email from the Internet on the conventional SMTP port 25 at the server's public IP address, 10.1.1.25 for example. This is the default for message transfer. You also want to accept mail submissions on the agreed-upon port 587; see RFC 2476. Here is the command needed:

```
Smtp Addlistener *:587
```

Or imagine that a different Message Server at IP address 10.3.3.5 has a second Ethernet interface attached. On the primary interface port 25, you plan to run MailHurdle, Antivirus, Antispam, and filtering. But you also want this server to accept email quickly from trusted users on a local network. The second interface is at IP address 10.3.3.6 on the private network, and should accept email on the normal SMTP port 25. Here is the command needed:

```
Smtp Addlistener 10.3.3.6:25
```

To delete a listener, use the **Smtp Deletelistener** command, giving an IPaddr:port specification as shown by **Smtp Listlistener**.

See **Help About Smtp** using the CLI for more details.

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).

   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 203 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 Administrators

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. For more information, see the *Mirapoint Administration Protocol Reference*. Messages quarantined by the signature-based antivirus scanners contain live viruses and should never be released to the mail stream.

9 Using the Operations Console

Use the Mirapoint Operations Console (MOC) to create groups of machines, assign a master, and replicate the configuration of the master throughout the group.

MOC 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 MOC 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 35) to ensure that the MOC **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 MOC and the other members of that group re-synchronized at any time. Those options described in Administering Groups on page 330 can be synchronized.

You access the MOC through the **ocadmin** login page on the appliance hosting the MOC. For example, **http://miServer/ocadmin**.

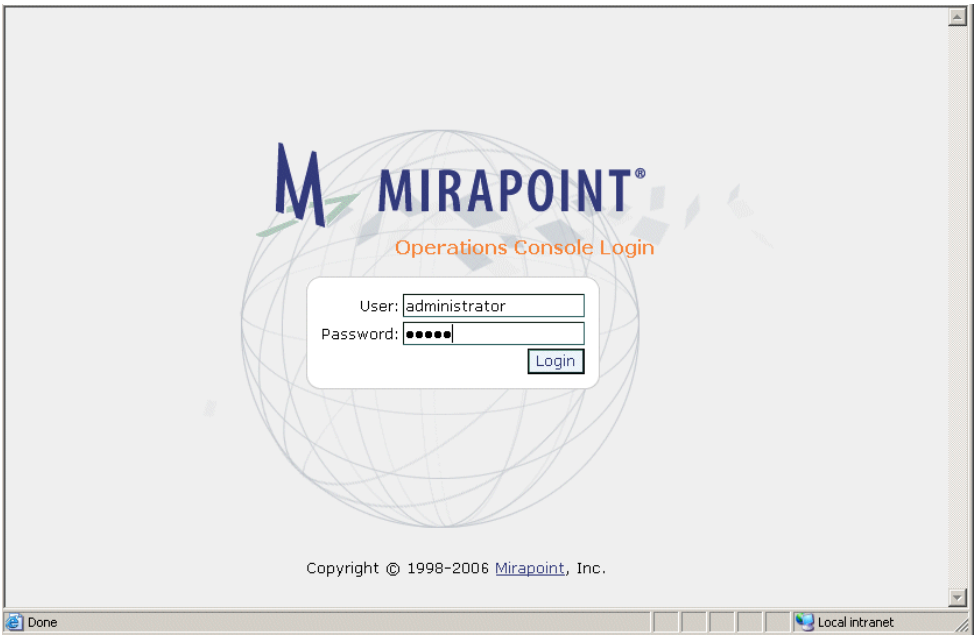


Figure 91 Mirapoint Operations Console Login Page

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 331 for details.

Click the **Administer** icon to open the **Administer-Home** page for a group's master.

The **Administer** icon does not display for groups without members. See Administering Groups on page 330 for details.

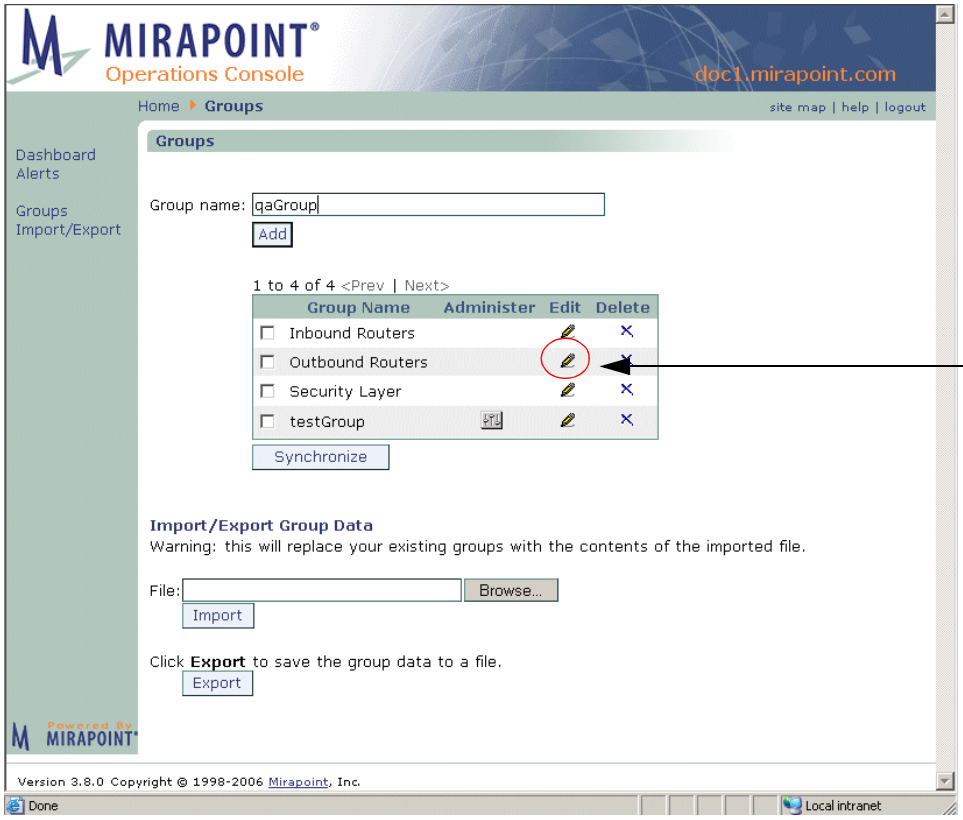


Figure 92 Operations Console Groups Page

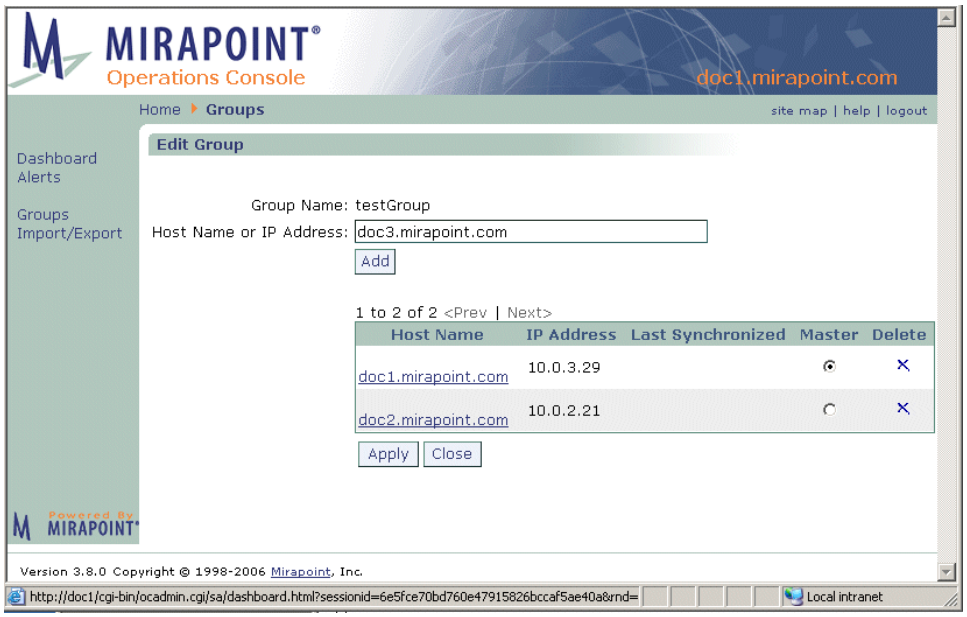


Figure 93 Operations Console Edit Groups Page

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 MOC. 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 92) 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 92 for an example).
3. On the **Edit Groups** page, shown in Figure 93, 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 MOC. 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 are done configuring the master, use the **Synchronize Groups** link to push your changes to the replicas. See Synchronizing Groups on page 331 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.

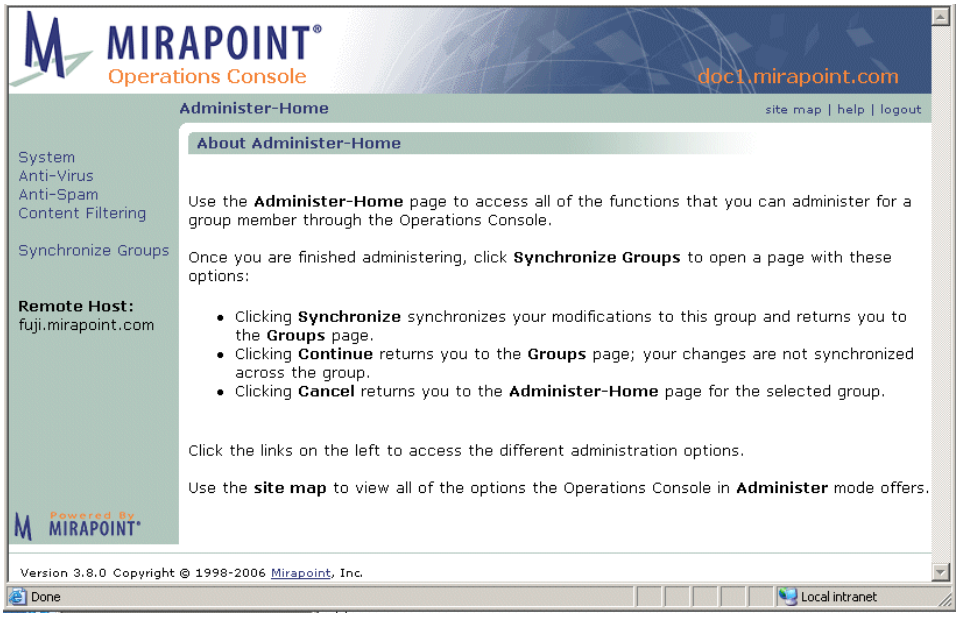


Figure 94 Operations Console Administer-Home View of Group Master

For details on using these administration options, see the following:

- Using Antivirus Scanning on page 288
- Using Antispam Scanning on page 303
- Managing Content Policies (Domain Filters) on page 236

Synchronizing Groups

Clicking the **Synchronize** button on the **Groups** page causes the MOC 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.

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 redisplays 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 92) 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 95 for an example.

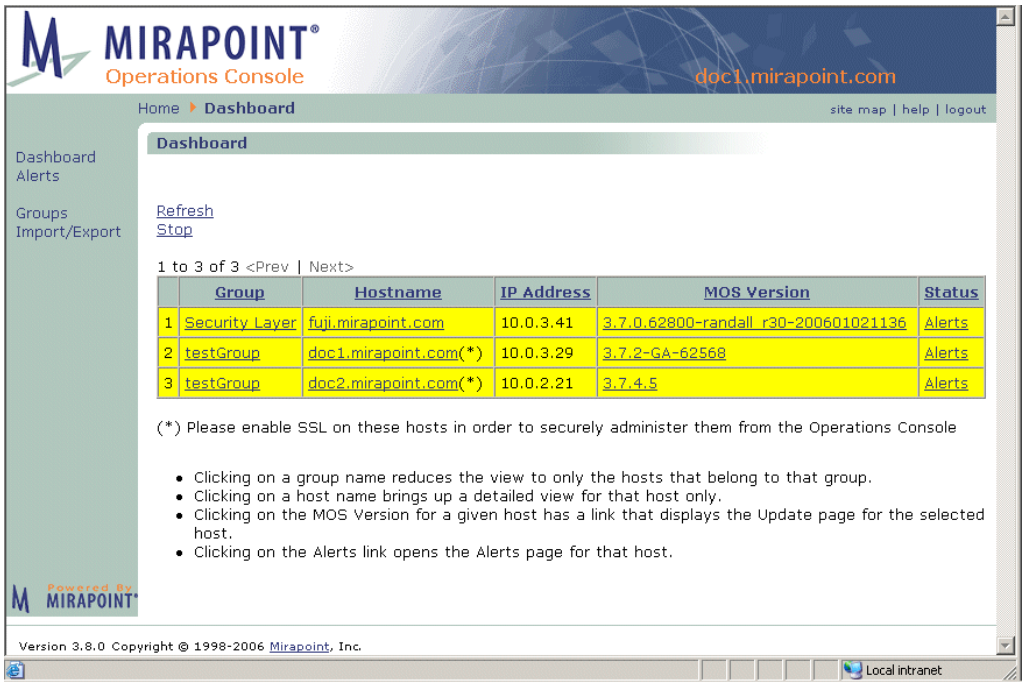


Figure 95 Operations Console Dashboard Page

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 23, Dashboard Status Colors, on page 333 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 23.

Table 23 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.

10

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 (DLs). 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 223.)

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 on the **Distribution Lists** page.

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 353.
- A local mail summary—Each message delivered to or received from a local user. For details, see Local (Mail Users) on page 353.
- A remote mail summary—Each message delivered to a remote recipient. For details, see Remote (Mail Users) on page 354.
- 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 360.
- Detailed mail logs—Chronological list of all SMTP transactions for the selected day. For details, see Detailed (Mail Logs) on page 356.
- 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 368.

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 362.
- Virus Statistics—Detailed information about viruses found. For details, see Detailed Virus Scanning Information Report on page 363.
- Content Filtering Summary—Detailed information about content filtering policies applied to messages on your system. For details, see Content Filtering Reports on page 364.
- SPAM Summary—Detailed information about messages identified as junk mail. For details, see Anti-Spam Reports on page 364.
- Failed Connections by User—The failed login attempts by user for the selected day. For details, see Failed by User (Logins) on page 361.

- 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 361.
- 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 365.
- 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 365.
- 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 366.

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 on the **Distribution Lists** page.

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 customercare@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 24 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
BACKUP	A list of backups performed on the system.	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

Table 24 Report Fields (Continued)

Field	Description	Example(s)
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 email of the administrator	Name: John Doe Phone: 408-720-3700 Address: 909 Hermosa Court, Sunnyvale, CA 94085 Email: jdoe@mirapoint.com
CONTROLLER	The model/type of SCSI disk contoller	2130S
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

Table 24 Report Fields (Continued)

Field	Description	Example(s)
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
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
HWCPU	CPU type and speed in magahertz	686 2400

Table 24 Report Fields (Continued)

Field	Description	Example(s)
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
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 Signature Edition Rapid Antispam 750 users 01/12/2007 Web-mail 300 users POP 750 users IMAP 301 users Directory Server Access 750 users XML unlimited users Sophos Antivirus 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

Table 24 Report Fields (Continued)

Field	Description	Example(s)
LOGINFOOTER (language selection links on the **Login** page)	Indicates if the login footer is on or off	On
LOGINS	The number of unique logins for a day or the average number of unique 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 syncinternal
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 3.3.10.52-EA
MONSETTINGS	A list of monitoring thresholds that have non-default values	system.adminc 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	port

Table 24 Report Fields (Continued)

Field	Description	Example(s)
NETIFSETTINGS	A list of NETIF settings that have non-default values	blackholeduration limittcpconnectcount limittcpconnectrate maxtcpconnectcount maxtcpconnectrate mediaport0 mediaport1
NETWORKMEDIA	The configuration and status of the Ethernet port 0	autoselect (100baseTX <full-duplex>) status: active
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	3.10
SERIAL	The system serial number	ESDW5420201
SERVICESENABLED	A list of the services enabled on the system or appliance	POP IMAP Calendar Webmail
SERVICESSTARTED	A list of the services started on the system or appliance	POP IMAP Webmail

Table 24 Report Fields (Continued)

Field	Description	Example(s)
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	3.10.1-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
VIRTDOM	The number of virtual domains on the system; deprecated as of 3.0. (not available on RazorGate appliances)	0
VIRTDOMMEM	The total number of members in all virtual domains. Virtual domains are deprecated as of 3.0. (not available on RazorGate appliances)	0

Table 24 Report Fields (Continued)

Field	Description	Example(s)
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 25 Time-Based Report Fields

Field	Description
ADMINREF	A list of which administrator commands have been executed and how many times they have been executed.
DIR.OPS	Number of directory operation (not available on RazorGate appliances)
DISKLOG	Percent full for the logging disk partition
DISKSTO	Percent full for the mail-store disk partition
DISKSYS	Percent full for the system disk partition
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
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

Table 25 Time-Based Report Fields (Continued)

Field	Description
FXPOPKTIN	The average number of network packets received per hour
FXPOPKTOU	The average number of network packets sent per hour
IMAPCONN	Number of IMAP connections per hour
LOAD1	The time-decaying average number of runable processes on the system or appliance over the previous one minute
LOAD15	The time-decaying average number of runable processes on the system or appliance over the previous 15 minutes
LOAD5	The time-decaying average number of runable processes on the system or appliance over the previous five minutes
LOCBYTRCV	The average number of bytes in all messages delivered locally per hour
LOCMSGRCV	The average number of messages received by the system
MTAVERIFY.ACTIVE	The Active setting for MailHurdle
MTAVERIFY.ANOTRETRIED	The number of messages that never retried MailHurdle's initial SMTP error code
MTAVERIFY.APASSED	The number of messages passed into the "Active" state by MailHurdle
MTAVERIFY.ATOTAL	The total number of messages processed by MailHurdle
MTAVERIFY.INITIALACTIVE	The Initial Active setting for MailHurdle
MTAVERIFY.INITIALDENY	The Initial Deny setting for MailHurdle
POPCONN	Number of POP connections per hour
SMTPBYTRCV	The average number bytes in all messages received from 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
SMTPMSGSNT	The average number of messages sent to remote systems per hour
SYSTEM.AMMSGATTACH	Number of messages with attachments since boot time
SYSTEM.AMMSGRECP	Number of message recipients since boot time
SYSTEM.AMMSGSPAM	Hourly number of Spam Mails (generated by phonestat.pl)
SYSTEM.AMMSGVIRUS	Number of email viruses found since boot time
SYSTEM.ASMTPCIN	Number of inbound SMTP connections since boot time
SYSTEM.ASMTPCOUT	Number of outbound SMTP connections since boot time

Table 25 Time-Based Report Fields (Continued)

Field	Description
SYSTEM.MAILQUEUE	Number of messages in the SMTP delivery queue at the top of each hour
SYSTEM.UCE1	Running count of messages scored 1-10 as junk mail
SYSTEM.UCE2	Running count of messages scored 11-20 as junk mail
SYSTEM.UCE3	Running count of messages scored 21-30 as junk mail
SYSTEM.UCE4	Running count of messages scored 31-40 as junk mail
SYSTEM.UCE5	Running count of messages scored 41-50 as junk mail
SYSTEM.UCE6	Running count of messages scored 51-60 as junk mail
SYSTEM.UCE7	Running count of messages scored 61-70 as junk mail
SYSTEM.UCE8	Running count of messages scored 71-90 as junk mail
SYSTEM.UCE9	Running count of messages scored 91-150 as junk mail
SYSTEM.UCE10	Running count of messages scored > 150 as junk mail
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 25 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.MSGDELMS	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)
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)

Table 25 Time-Based Report Fields (Continued)

Field	Description
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.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.

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 26 provides definitions for abbreviations used in the logs.

Table 26 Abbreviations Used in Logs

Abbreviation	Description
“”	Empty command arguments
ADMIN	Administration service
CLR	Cleartext or nonsecure
INVLD	Bad login
KB	Kilobyte
KERB4 or KERB5	Kerberos authentication
LCL	Local
NTP	Network Time Protocol
PLAIN	Plaintext
RMT	Remote
SSH	Secure Shell authentication
SSL	Secure Sockets Layer authentication

Table 26 Abbreviations Used in Logs (Continued)

Abbreviation	Description
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 SMTP.

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.

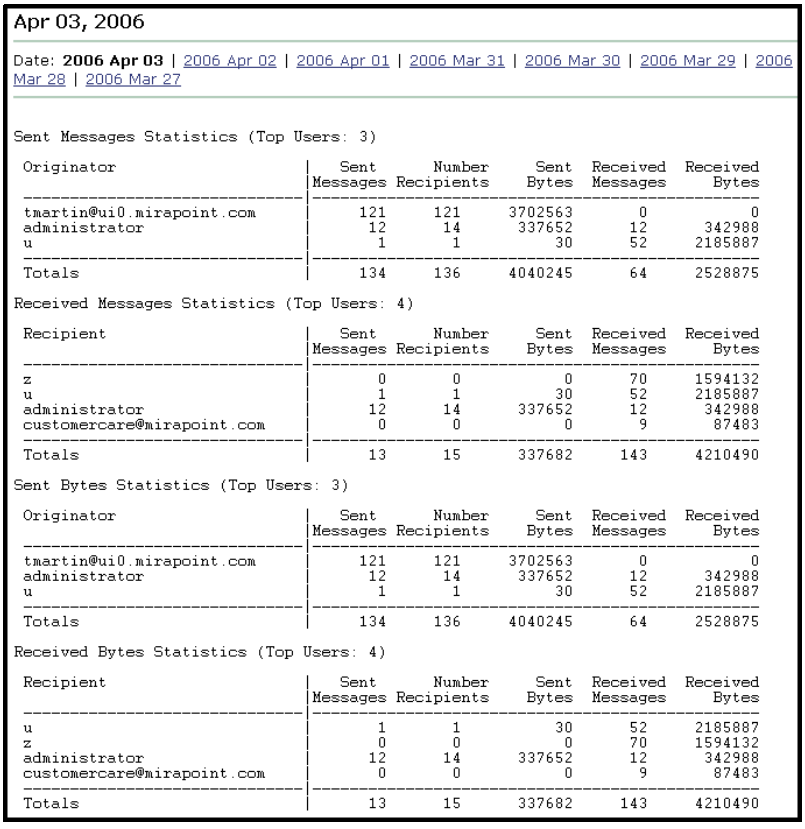
Use this report to find out who is sending the most and/or largest size messages. You can then take action through email or blocking/filtering those senders.

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 96 on page 352.

Table 27 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
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
customercare@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
customercare@mirapoint.com	0	0	0	9	87483
Totals	13	15	337682	143	4210490

Figure 96 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 35, Top Logins By User, on page 359.

Local (Mail Users)

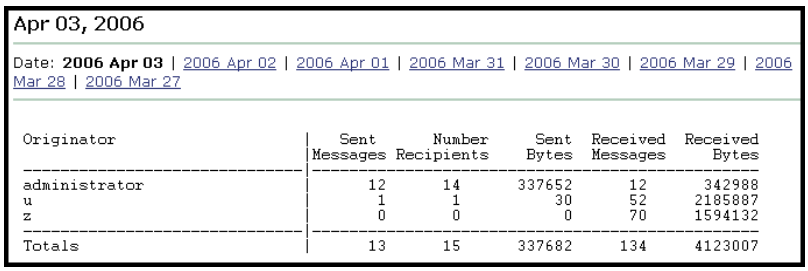
The **Local Mail Traffic** report shows data about the messages sent and received by each local email address on the system.

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 97 on page 353.

Table 28 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 97 Local Mail Traffic

Remote (Mail Users)

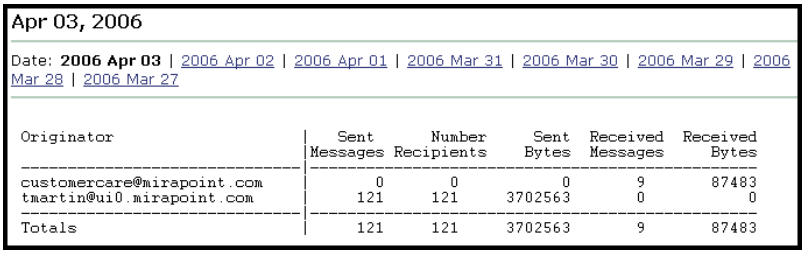
The **Remote Mail Traffic** report shows data about the messages received from remote email addresses.

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 98 on page 354.

Table 29 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
customercare@mirapoint.com	0	0	0	9	87483
tmartin@ui0.mirapoint.com	121	121	3702563	0	0
Totals	121	121	3702563	9	87483

Figure 98 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 or recipients

For these reports, see also, Code Explanations on page 357.

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 30 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 31 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 32 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 33 Detailed Mail Logs

Statistic	Description
originator	The sender of the message
queue-id	The unique ID that identifies the message within the mail queue
message-id@example-host-name	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 "*@host-name*" where the value of *hostname* depends on the configuration of the originating host machine of the message
evt-time	The time the event occurred

Table 33 Detailed Mail Logs (Continued)

Statistic	Description
event	One of the following: ❖ **received** *num-bytes num-recipients host-received-from* The message was received. ❖ **filtering** *code* (see Code Explanations) The message was filtered for *recipient* ❖ **queued** *recipient* The message was queued for *recipient* ❖ **recipient** *action* The recipient received the listed action; for example, "delayed" or "does not exist." ❖ **sent** *elapsed-time recipient-list* The message was sent. ❖ **Split** from *queue-id* The message was copied from *queue-id* and assigned a new queue ID to facilitate internal processing.
num-bytes	The number of bytes in the message
num-recipients	The number of recipients of the message
host-received-from	The host from which the message was received
recipient	The address of the recipient
elapsed-time	The total time that elapsed between receipt and final delivery
recipient-list	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 34 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

Table 34 Filtering Event Codes (Continued)

Code	Description
IDS	Domain Signatures, Inbound Only
IDF	Domain Filters, Inbound Only
N	Not Allowed (COS denied this service)
QN	Quarantine
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 356.

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. 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 35 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).
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 *days* (if more than an entire day), followed by *hours*:*minutes*:*seconds*.

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 36 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.

Table 36 Login Traffic Rates (Continued)

Field	Description
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.
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 37 Detailed Login Report

Statistic	Description
event	The login event; either LOGIN, LOGOUT, or BAD.
date	The date of the event in the format *year*/*month*/*day*.
time	The time of the event in the format *hours*:*minutes*:*seconds*.
GMT-offset	The offset in hours from Greenwich Mean Time (GMT)
service	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).
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).
IP-addr	The IP address of the connecting host.
user	The login name of the connecting user.
duration	(LOGOUT only) The duration of the connection in seconds.

Table 37 Detailed Login Report (Continued)

Statistic	Description
activity count	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 38 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 38, 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 39 Virus Scanning Summary Report

Field	Description
address	The address that sent or received the virus
virus-name	The name of the virus, as identified by the Sophos virus-scanning software
count	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 40 Detailed Virus Scanning Information Report

Field	Description
xport	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 290.

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 41 Anti-Spam Information Report

Field	Description
address	The address that sent or received the junk mail
sent-recv	Possible values are **sent** for messages sent, and **recv** for messages received
count	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 42 Content Filtering Statistics Report

Field	Description
domain	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 243 for details on using this filtering option.
rule-name	The unique name of the rule that defines this policy; this is usually a system-generated name, such as **Unnamed Rule 0** or (**implicit**)
action	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 243 for details on filtering.
count	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 310 or Setting the Allowed Mailing Lists List on page 314.

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 43 MailHurdle Host Summary

Field	Description
Host	The host running MailHurdle.
% Delayed	The percentage of messages from that sender IP, that were delayed by MailHurdle because no valid triplet existed.
Delays	The number of messages that did not retry within the allotted time period and were rejected.
Accepts	The number of messages that did retry within the allotted time period and were accepted for delivery.
Sender IP	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 44 MailHurdle To Address Summary

Field	Description
To	The email address to which the spam was sent.
% Rejected	The amount of mail that did not retry within the allotted time period and was rejected.
Msg Rej	The number of messages that did not retry within the allotted time period and were rejected.
Msg Acpt	The number of messages that did retry within the allotted time period and were accepted for delivery.
Sender IP	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 45 MailHurdle From Address Summary

Field	Description
From	The email address from which the spam came.
% Rejected	The amount of mail that did not retry within the allotted time period and was rejected.
Msg Rej	The number of messages that did not retry within the allotted time period and were rejected.
Msg Acpt	The number of messages that did retry within the allotted time period and were accepted for delivery.
Sender IP	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 46 System Information Report

Field	Description
year	The four-digit year of the event
month	The two-digit month of the event
day	The two-digit day of the event
hh	The two-digit hour of the event
mm	The two-digit minute of the event
ss	The two-digit second of the event
event	The event name
cause	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 47 Command Report

Field	Description
year	The four-digit year of the event
month	The two-digit month of the event
day	The two-digit day of the event
hh	The two-digit hour of the event
mm	The two-digit minute of the event
ss	The two-digit second of the event
id	The unique identifier for the administration service connection (session) in which the command was issued
userin-out	The user who issued the command (including domain name, for a delegated domain user), followed by > or <, which indicates whether *cmd-resp* is a command (>) or a command response (<)
cmd-resp	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 s pace 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 48 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 *used/quota*

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 48, 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%).

11 Business Continuity Tasks

This chapter describes Mirapoint business continuity tasks including backup and restore tasks and how to set up and use Remote Server Replication (RSR). Topics include:

- Backup and Restore Concepts—Concepts you should understand before proceeding with a Mirapoint backup task.
- NDMP Backup Solutions—What options are available and how to use them.
- Administration Protocol Backup Solution—What options are available and how to use them.
- Using Remote Server Replication—Configuration and use of RSR.

The methods described in this chapter are not applicable to SAN models (MOS 3.x and MOS 4.x) and NAS models (MOS 3.x only), which are backed up using the snapshot/backup capabilities of the SAN and NAS storage devices, respectively.

Backup and Restore Concepts

Data stored on a Mirapoint Message Server must be backed up regularly to ensure recovery in the event of a disaster or if it is accidentally deleted. This section provides the following information about backup and restore functions and summarizes the Mirapoint implementations:

- Backup Schemes
- What Is and What Is Not Backed Up
- About Tape Drives and Tape Libraries

This chapter includes several pointers to articles in the Mirapoint Knowledge Base on the Mirapoint Support website, http://support.mirapoint.com. You need a Mirapoint Support login ID and password to access this information. If you do not have a Mirapoint Support login ID, send an email to support-admin@mirapoint.com requesting one.

Backup Schemes

Your backup scheme answers *how* you are going to back up *what*:

- *How*—**Image-based** versus **message-based**:
  - Image-based backups take a "snapshot" of the entire system.
  - Message-based backups do not save all system information. In particular, message-based backups do not backup the directory, which is an integral part of the product. Also, message-based backups are considerably slower.
- *What*—**Full** versus **incremental** versus **selective**:
  - Full backups save all the data on the specified system.
  - Incremental backups save only the data that has changed since the last backup.
  - Selective backups save only specified folders; this is only available for message-based backups.

Mirapoint recommends image-based full backups with Network Data Management Protocol (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. Compared to message-based backup and restore, image-based backup and restore using NDMP is faster for both backup and restore. A message-based restore could take days to complete on very large systems.

Image-based restore works only if you are restoring to *exactly* the same MOS version, and patch level from which the backup was taken. For example, you may do an NDMP backup of an M4500 and restore it to an M5000 only if they have the same MOS version. 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 folders 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 49 summarizes what is saved by *image-based* versus *message-based* backups.

Table 49 What Gets Backed Up—Image-Based vs. Message-Based

Data	Image-Based	Message-Based
Folders (mailboxes)	Yes	Yes
User accounts	Yes	Yes
Distribution lists	Yes	Yes

Table 49 What Gets Backed Up—Image-Based vs. Message-Based (Continued)

Data	Image-Based	Message-Based
Calendar and address book	Yes	Yes
The SMTP delivery queue	Yes	No
Mail logs and system logs	Yes	No
\Recent and **\Seen** mail flags	Yes	No
Directory Information	Yes	No
Operations Console Information	Yes	No
Mirapoint licenses	No	No
SSH keys	No	No
Network Settings	No	No

Message-based incremental backups save only messages added to a folder since the last backup. Other folder state changes, such as deletions and changes to message flags, are not saved.

Selective restore from image backup is initiated with NDMP software, and can be traced with the **Ndmp Merge Status** command.

To find out current information on what system information is backed up, search for the "System Information That is Backed Up" article in the Mirapoint Knowledge Base at http://support.mirapoint.com.

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. Depending on the model, the SCSI interface for the tape drive is either single-ended or low voltage differential (LVD).

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 the backup can continue without interruption.

To find out which devices Mirapoint currently supports, search for the "Approved Local Tape and Library Devices" article in the Mirapoint Knowledge Base at http://support.mirapoint.com.

NDMP Backup Solutions

This section describes your NDMP backup options. Topics include:

- NDMP DMAs on page 372
- Using NDMP for Backup and Restore on page 374

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-based appliances. NDMP separates the data path and the control path, so network data can be backed up locally, yet readily managed from a central location. Mirapoint's current implementation is NDMP version 3.

An NDMP client requires two services to perform backups. The **mover/tape** service is used to control the autochanger connected to the tape device and the **data** service is used for the actual backup stream. Mirapoint appliances implement both services, and can be used to back up data locally (through a locally-attached auto-changer) or remotely (also known as a three-way backup).

Depending on the NDMP server, you can perform a backup or restore in one of two ways:

- **Local**—From a locally-attached SCSI drive. During local backup, the Mirapoint NDMP client initiates a request for backup to the NDMP server, which controls the drive and directs the data image onto tape. During restore, data streams from tape to RAID storage.
- **Three-way**—The NDMP server controls a SCSI drive attached to a remote server. During three-way backup, the Mirapoint NDMP client initiates a request for backup to the NDMP server, which streams the data image across the network onto a remote-attached tape drive. During restore, data streams from remote tape across the network to local RAID storage.

For more information on NDMP, see http://www.ndmp.org.

NDMP DMAs

The driving software for NDMP is called a Data Management Application (DMA). This is usually a graphical application that runs on a separate server; see Table 50, NDMP DMA. for details.

You can search for the associated Mirapoint Knowledge Base (KB) articles at http://support.mirapoint.com.

Table 50 NDMP DMA

DMA	Description	Mirapoint KB Article(s)
BakBone NetVault with NDMP Plugin Module	You can use BakBone NetVault NetVault version 7.4 or higher with the NDMP Plugin Module to perform Mirapoint backups and restores. For more information, go to: http://www.bakbone.com	"Configuring and Using BakBone NetVault for Mirapoint NDMP Backup"

Table 50 NDMP DMA (Continued)

DMA	Description	Mirapoint KB Article(s)
Legato NetWorker	You can use Legato NetWorker version 7 or higher with NDMP to perform image-based backups and restores to either local or three-way tape drives. For more information, go to: http://www.legato.com	❖ "Configuring Legato NetWorker for Mirapoint NDMP Backup" ❖ "Using Legato NetWorker to Perform a Manual Full Backup" ❖ "Performing a Mirapoint NDMP Restore Using Legato NetWorker" ❖ "Using Legato NetWorker to Perform a Save Set Restore" ❖ "Using Legato NetWorker to Perform an NDMP Selective Restore From Image"
Tivoli Storage Manager	You can use Tivoli Storage Manager (TSM) version 5.4 or higher to perform image-based backups and restores to local tape drives. For more information, go to: http://www.tivoli.com	❖ "Configuring Tivoli Storage Manager for Mirapoint NDMP Backup" ❖ "Using Tivoli Storage Manager to Perform a Backup" ❖ "Using Tivoli Storage Manager to Restore Files"
Veritas NetBackup	You can use Veritas NetBackup BusinesServer to perform image-based backups and restores to either local or three-way tape drives. Mirapoint currently requires Veritas NetBackup version 6 or higher and NetBackup for NDMP on the same server. For more information, go to: http://www.veritas.com	❖ "Configuring Veritas NetBackup Version 4.5 for NDMP" ❖ "Configuring Veritas NetBackup Version 5.1 for NDMP" ❖ "Performing an NDMP Message-Based Incremental Backup Using Veritas NetBackup" ❖ "Using Veritas NetBackup Version 4.5 to Perform a Manual Backup" ❖ "Using Veritas NetBackup Version 5.1 to Perform a Manual Backup" ❖ "Using Veritas NetBackup Version 4.5 or 5.1 to Perform an NDMP Selective Restore From Image" ❖ "Using Veritas NetBackup Version 4.5 to Perform an NDMP Restore" ❖ "Using a Veritas NetBackup Image Backup to Recover the System"

Using NDMP for Backup and Restore

To use an NDMP backup solution, you need to enable and start the Mirapoint NDMP service on the appliance you are 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. Enable and start the NDMP service. In the Administration Suite, go to **System > Services > NDMP** and enable and start the service.
   In the CLI, use the **Service Enable** and **Service Start** commands:

   ```
   Service Enable Ndmp
   Service Start Ndmp
   ```

2. Set the Data Management Application (DMA) and the NDMP version. In the Administration Suite, go to **System > Services > NDMP** and select a **Data Management Application** and **Version** from the drop-down menu; then click **Modify**.

   (Optional) In the CLI, use the **Ndmp Set** command.

   ```
   Ndmp Set Dma Product
   Ndmp Set Version 3
   ```

   Product can be **Default**, **BakBone**, **Legato**, **Tivoli**, or **Veritas** and *version* can be 2, 3, or 4.

Configuring Your DMA

To find information about how to configure your DMA to perform Mirapoint Backups, search for the "NDMP Backup and Restore: Where Do I Begin?" article 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 messaging services turned off; in general licenses are recovered as part of the image restore. 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; you can do this with the **License Fetch** command.
4. Perform the image recovery as described in the appropriate Mirapoint Knowledge Base article for your DMA:

- "Using a Veritas NetBackup Image Backup to Recover the System"
- "Performing A Mirapoint NDMP Restore Using Legato NetWorker"
- "About NDMP Image Restore and Target Mail Stores"

You can search for each article 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.

Administration Protocol Backup Solution

This section describes your Administration Protocol backup options. Topics include:

- Alerts and Completion Status on page 375
- Administration Protocol on page 376
- Using the Administration Protocol for Backup on page 376
- Using the Administration Protocol with a Local Storage Device on page 377
- Using the Administration Protocol with Remote Magnetic Tape (RMT) on page 379

Local backups and Remote Magnetic Tape (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.

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.

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.

Administrator has the ability to use all commands.

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 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 Magnetic Tape (RMT) protocol to a Sun Solaris system.

For RMT, you must first configure a Solaris system with tape drive. 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 about the backup and restore commands, see in the CLI, **Help Backup** and **Help Restore**.

For information on backup, restore, protocols, and tape devices, see Backup and Restore Concepts on page 369.

For information on what data is saved by message-based backup, see What Is and What Is Not Backed Up on page 370.

Using the Administration Protocol with a Local Storage Device

This section describes how to:

- Installing a Local Tape Drive for Backups on page 377
- Performing a Full Backup to a Local Device on page 377
- Performing a Selective Backup to a Local Device on page 378
- Performing a Full Restore from a Local Device on page 378
- Performing a Selective Restore from a Local Device on page 378

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 5-Series/MOS 3.x appliance is equipped with one
   - The tape drive or library
   - The Mirapoint appliance

When the appliance boots, it recognizes the newly connected tape drive.

Never power off 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 off 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 Remote Magnetic Tape (RMT)

You can use the Remote Magnetic Tape (RMT) protocol only to back up your appliance to a tape drive on a Sun Solaris system.

Mirapoint recommends using NDMP to perform image-based backups instead of using RMT. See Using NDMP for Backup and Restore on page 374

This section describes how to:

- Configuring a Solaris System for RMT on page 379
- Issuing Backup and Restore Commands for RMT on page 380
- Performing a Full Backup Using RMT on page 380
- Performing a Selective Backup Using RMT on page 380T
- Performing a Full Restore Using RMT on page 381
- Performing a Selective Restore Using RMT on page 381

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
   ```

3. For security, restrict access to **.rhosts**; enter:

   ```
   chown Backupuser .rhosts
   chmod 400 .rhosts
   ```

4. 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, search for the "Trouble with an Administration Protocol Backup Via RMT To A Unix System" article 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 back up, for example "user.joe" for the user mailbox for **joe**.

Using Remote Server Replication

Remote Server Replication (RSR) provides disaster recovery for Mirapoint Message Servers (MMS), letting you stage a secondary data center in a remote location to provide email service continuity if a disaster strikes your primary data center. RSR works on 5-series Message Servers, such as the M50, M500, and M5000 systems, using local storage and running system software release 3.7.4b or later.

RSR is a licensed feature.

This section describes how to use RSR; the following topics are included:

- Overview
- System Requirements
- Installation, Configuration, and Synchronization
- Scheduling Regular Synchronizations
- Monitoring and Troubleshooting
- Updating Systems
- Aborting a Synchronization in Progress
- Removing a Replica Configuration
- Performing a Failover
- Restoring a Master

RSR is used for continuity of mail services; it is not useful to recover accidental data loss or corruption or as a replacement for a backup strategy.

NTP, LDAP, and DNS servers must be replicated separate from the RSR process.

Overview

RSR lets you maintain a Replica of your message store (Master) at a different location. If your primary data center is lost or inaccessible for an extended period, the Replica can take over the function of your data center. The Replica is kept current through regularly scheduled synchronizations with the Master; these synchronizations require no production downtime.

The Replica is synchronized with user data from the Master, as well as any LDAP or DNS settings on the system. With a valid Replica, if disaster strikes the Master, the only downtime that occurs is the time until an administrator manually switches over to the Replica. User data on the Replica is current, except any new data on the Master since the last successful synchronization.

The procedures described here set up a single Master with a single Replica. To create a replica data center for multiple servers you must plan accordingly to account for multiple systems, but the actual replication procedures are performed individually for each system as documented here.

For the entire replica data center, you must plan for the staging of the equipment, configuring the network, and bandwidth requirements and limits. Presumably these elements would be similar to those of your primary data center and can be configured accordingly. For each replicated system, RSR copies the contents of a single Mirapoint server's message store and configuration via an IP network to another Replica Mirapoint server.

The Master and Replica must be:

- Identical system models (except for storage size).
- Running the same release of the Messaging Operating System (MOS), including the same patches.

The Administrator must:

- Configure the Master and Replica systems. All system configurations for mail store must be completed on both the Master and the Replica before starting replication.
- Initiate the initial copy of the Master to the Replica.
- Schedule regular updates (deltas) to keep the Replica current.
- Monitor to ensure that the Replica is ready to take over the Master if needed.
- If the Master fails, set the Replica to take over as the Master.
- The Replication system ensures that the Replica is robust in the face of reboots of either the Master or the Replica at any time. Reboots can require that data be copied again from the Master to the Replica. Because later syncs would then be larger, this can delay the availability of the Replica as a viable failover machine.

System Requirements

You must configure the Master and Replica systems at their respective locations. Typically, you can perform these tasks from a single location, over a TCP/IP network connected to both locations. For information on setting up and configuring a Message Server, see the *Mirapoint Message Server Administrator's Guide*.

When planning your RSR configuration, consider these requirements:

- Number of Systems—Each Master system at the primary site is copied to exactly one Replica system at the Replica site. You can have only one Replica system for a Master system. In a deployment with multiple Message Servers, each Master requires its own corresponding Replica system.
- Related Systems—The Router and Proxy servers must be replicated at the Replica site, using the CLI **Conf Export/Import** command. The Directory server must be replicated using LDAP replication. This document does not describe how to configure related systems; the steps vary depending on your network.
- Network Configuration—Connections between the Master and Replica systems are over a private network; the Master must be able to connect to the Replica on TCP port 873. The network link must be secure, reliable, and have sufficient capacity to let the RSR synchronization process complete in a reasonable time. If a WAN link is used, or the traffic traverses the public internet, to ensure that sensitive data is not transmitted in cleartext, provide transport encryption by use of a VPN or other technology. You can also perform the initial (typically largest) synchronization locally, with both systems on the same LAN, and then transport the Replica to the remote data center.
- Disk Storage—The Master system synchronizes more reliably if it has ten percent free space. The Replica system must have sufficient storage capacity to handle the data volumes to be replicated from the Master system. The storage space on the Replica must be equivalent to the Master's used store plus the size of accumulated changes since the last sync. In the most extreme case, this can approach double the amount of storage on the Master. However more frequent, regularly scheduled synchronizations result in smaller differences between the

Master and Replica, and therefore minimize the need for greater space on the Replica.

- DNS—The Master and the Replica must be configured with forward DNS resolving their hostnames and reverse DNS resolving their IP addresses.

Installation, Configuration, and Synchronization

These steps must be performed in the order provided; you must use the CLI. For example, you cannot perform all the Master steps together, then all the Replica steps together.

To perform the initial installation and synchronization between the Master and the Replica:

1. Install the RSR patch on both the Master and the Replica:

   `Update Install ftp://ftp.mirapoint.com/pub/updates/E3_Replicate`

2. Add the RSR license on both the Master and the Replica; replace *key* with the RSR license key:

   `License Apply` *`key`*

3. On the Replica system, prepare the Replica to receive data from the Master system:

   `Replicate From` *`master_hostname`*
   `OK Completed`

   where *master_hostname* is either the fully-qualified domain name or the IP address of the Master system.

   Changing the *master_hostname* invalidates the replication configuration, requiring a complete RSR re-configuration. For example, if the initial synchronization is performed on a LAN, use the hostname and not the IP address.

4. On the Master system, prepare the Master to transfer data to the Replica system:

   `Replicate To` *`replica_hostname`*
   `OK Completed`

   where *replica_hostname* is either the fully-qualified domain name or the IP address of the Replica system.

   Changing the *replica_hostname* invalidates the replication configuration, requiring a complete RSR re-configuration.

5. Check that the Master can contact the Replica, with the **Replicate Status** command (this example shows all possible values). See Table 51, Replicate Status Descriptions, next, for details.:

   `Replicate Status`
   `Host Role is: [Master|Replica|Undecided]`
   `Sync is: [Active|Inactive]`
   `Delta Application is: [Active|Inactive]`
   `Replica Current As Of:` *`ISO DATE-TIMESTAMP`*`;` *`HH:MM`* `Ago`
   `NOTE: Replica NOT Viable, No Syncs Completed`
   `Last Sync: [Applying|Running|Completed|Failed|Cancelled|None]`
   `Last Completed Sync Size:` *`integer`* `MB Elapsed Time:` *`HH:MM`*

```
Syncs: Attempted: integer, Completed: integer, Failed/Cancelled: integer
Replication Server: [Running|Down|Unreachable]
Master Store Size: integer MB, Used: integer MB, Inodes: integer, Used:
integer
Replica Store Size: integer MB, Used: integer MB, Inodes: integer,
Used:integer
OK Completed
```

If the replica cannot be contacted, check the network between the two servers and also that DNS is set up properly.

6. On the Master system, use the **Replicate Get** and **Replicate Set** commands to view and set the retry characteristics or bandwidth limits associated with the synchronization process, if needed. See Table 52, Replicate Get/Set Descriptions next, for details. For example, to obtain the current value of the **RetryDelay** parameter (10 seconds), and then set **RetryDelay** to 60 seconds, do this:

```
Replicate Get RetryDelay
10
OK Completed
Replicate Set RetryDelay 60
OK Completed
```

7. On the Master system, start the data transfer from the Master to the Replica:

```
Replicate Sync
* Sync Started
OK Completed
```

Successful completion or failure of the data transfer is logged in the system logs, and is available using the **Replicate Status** command.

Table 51 Replicate Status Descriptions

Statistic	Description
Host Role	Whether the host is the Master or Replica.
Sync	Whether a **Sync** transfer is currently active.
Delta Application	Whether a delta application (regularly scheduled update) is currently in progress.
Replica Current As Of	The time-stamp of the last successfully-completed **Sync** command and the number of hours since that time.
NOTE	Message that appears if no Syncs have ever completed on the Replica yet.
Last Sync	The status of the last **Sync** command.
Last Sync Size	The size and total elapsed time of the last **Sync** transfer. Size is specified in megabytes; elapsed time is specified in hours and minutes.
Syncs	Provides statistics on the number of **Sync** commands that have been attempted, completed, or failed/cancelled.
Replication Server	Reports whether the Replica system is listening for connections. Values displayed on the Master can be: **Running** or **Unreachable**; values displayed on the Replica can be: **Running** or **Down**.

Table 51 Replicate Status Descriptions (Continued)

Statistic	Description
Master Store Size	Provides storage statistics for the Master system, including total capacity (megabytes), storage used (megabytes), total number of inodes (files and directories), and the number of inodes in use.
Replica Store Size	Provides storage statistics for the Replica system, including total capacity (megabytes), storage used (megabytes), total number of inodes (files and directories), and the number of inodes in use.

Table 52 Replicate Get/Set Descriptions

Parameter	Description
RetryCount	The number of attempts made to copy a data set to the Replica system before aborting the Sync operation. Value can range from 0–100. A value of zero (0) means “retry forever”. The default is zero.
RetryDelay	The number of seconds to wait after a copy attempt failure before retrying the copy. Value can range from 10–600. The default is 10.
BandwidthLimi	Limit on the number of kilobytes per second of bandwidth used for the data transfer between the Master and Replica systems. Value can range from 0 to 1,000,000 KBps. A value of zero (0) means “no bandwidth limit”. The default is zero.

Scheduling Regular Synchronizations

To schedule periodic synchronization, use the **Schedule** command on the Master system. Because the **Sync** and **Backup** commands cannot run at the same time, schedule synchronizations so that they do not overlap with backups.

For example, to schedule a daily synchronization named **scheduledSync** at 2:00 a.m., enter this command on the Master system:

```
Schedule Add scheduledSync daily 2 "Replicate Sync"
OK Completed
```

To schedule synchronizations every eight hours, which is recommended, schedule three daily passes, one for each eight-hour interval:

```
Schedule Add scheduledSync2 daily 2 "Replicate Sync"
Schedule Add scheduledSync10 daily 10 "Replicate Sync"
Schedule Add scheduledSync18 daily 18 "Replicate Sync"
OK Completed
```

The data synchronization operation cannot run concurrently with an NDMP backup. You must ensure that these operations are not scheduled to overlap.

If an NDMP backup is in progress when a synchronization is attempted, the synchronization fails:

```
NO Snapshot In Use
```

If this problem persists, re-evaluate the NDMP backup and RSR synchronization schedules, and adjust them accordingly so the processes do not overlap.

Example: Configuring RSR on a Master and Replica

This example provides the commands for an administrator to execute on each system to configure them as a Master and Replica for server replication, run the initial synchronization, and schedule updates and verify the Replica's status every eight hours. As indicated earlier, both systems must already be fully configured with the same MOS, patches, services, and features.

1. On the Replica system, indicate the name of the Master system:

   Replicate From *master_host*

2. On the Master system, indicate the name of the Replica system:

   Replicate To *replica_host*

3. Check that the Master can contact the Replica:

   Replicate Status

4. On the Master system, run the initial synchronization:

   Replicate sync

5. On the Master system, schedule regular synchronization updates to occur every eight hours, starting at 1a.m.:

   ```
   Schedule Add scheduledSync1 daily 1 "Replicate Sync"
   Schedule Add scheduledSync2 daily 9 "Replicate Sync"
   Schedule Add scheduledSync3 daily 17 "Replicate Sync"
   ```

6. On the Replica system, schedule daily checks to run at 2a.m. to verify that the Replica is ready to take over for the Master system:

   Schedule Add scheduledCheckswitch daily 2 "Replicate Checkswitch"

   The output of scheduled commands is sent to the **scheduled-output** distribution list.

Daily Operations

Each day make sure that your RSR system is in condition to accept a failover.

1. Regularly check that the replication is no more than 24 hours out of date and the synchronizations are successful. Also, regularly confirm that the Replica mail store has sufficient space for the delta from the Master. To do this, use the **Replicate Status** command and monitor the logs. Table 51 on page 385 describes status results.
2. Regularly run the **Replicate Checkswitch** on the replica and check for errors.
3. If the **Replicate Status** command reports that the replication server is not running on the replica, check to see if the service is running on the Replica system with the following command:

   ```
   hostname.com> diag netstat *873*
   tcp 0 0 *873 *.* Listen
   OK Completed
   ```

If the **Listen** is not present, then the replication service needs to be restarted with the **Replicate Restart** command. The replication server only runs on the replica system and this step is not applicable to the master system.

Monitoring and Troubleshooting

Administrators should regularly monitor to ensure that the Replica system is ready to effectively take over if the Master fails. There are two methods for monitoring:

- Verify the replication process, checking that both systems share identical configurations and that the synchronizations are successful.
- Monitor the logs for any messages or alerts that indicate problems with the replication process.

There are some considerations when updating the software (MOS release, patches, etc.) on replication systems. Also, in some situations it might become necessary to abort a synchronization that is in progress or to entirely remove a replica configuration.

Verifying Replication

There are several factors to verify in order to confirm that the Replica is able to effectively take over for the Master if necessary:

- Verify that both systems are still running the same MOS release with the same patches.
- Verify via monitoring that the Replica is successfully synchronizing with the Master.
- Monitor email to see if any messages are sent to the system-alerts distribution list indicating synchronization-related failures.

On the Replica system, verify that the Replica is ready to assume the role of the Master if the Master fails:

```
Replicate Checkswitch
OK Completed
```

If another Replicate operation is in progress, the **Checkswitch** command fails:

```
Replicate Checkswitch
NO Operation in Progress
```

In this case, either wait for the Replicate operation to complete or cancel the operation.

Checkswitch reports any mismatches between MOS versions or patches:

```
Replicate Checkswitch
* MOS Version Mismatch: Store '3.7.5GA' Replica '3.7.4GA'
NO Replica Not Ready

Replicate Checkswitch
* Patchlist Mismatch
* Replica Missing: "E3_Hash_2"
* Replica Missing: "E3_FooBar_7"
* Replica Missing: "E3_Widgit_9"
```

```
* Replica Added: "debug-1"
* Replica Added: "E3_Widgit_8"
NO Replica Not Ready
```

In this case, update the Master or Replica system as necessary to ensure that the indicated software versions match exactly.

To schedule daily checks that the Replica is ready to assume the role of the Master, use the **Schedule** command. For example, to schedule a **Checkswitch** command to run daily at 1a.m.:

```
Schedule Add scheduledCheckswitch daily 1 "Replicate Checkswitch"
```

Monitoring Logs

Certain alert messages are sent to the system-alerts distribution list, but others appear only in the system log. Regularly monitor the logs to ensure no other messages indicating problems arise. You can check the log using the Administration Suite or, depending on how you configured reporting, in your daily and weekly reports. Simply scan the log for any of the problematic messages, or do a text search for the message header text.

For descriptions of each replication log message and troubleshooting information for the messages indicating problems, see Table 53, next.

Log Messages and Troubleshooting

This section describes the messages reported by the replication subsystem, and provides troubleshooting information for the messages that indicate problems.

When monitoring logs, these messages indicate problems to investigate:

- REPLICATE.SYNC.FAILED
- REPLICATE.SERVER.FAILED
- REPLICATE.CONFIG.ERROR
- REPLICATE.COMM.FAILURE
- REPLICATE.VERSMISMATCH.MOS
- REPLICATE.VERSMISMATCH.PATCH
- REPLICATE.VERSMISMATCH.REPLICATE

All of the above messages are sent to the **system-alerts** distribution list, except for VERSMISMATCH.MOS and VERSMISMATCH.PATCH; see Table 53, Replication Subsystem Error Messages next, for descriptions.

Any messages in this section that are the result of a scheduled command are sent to the **schedule-output** distribution list.

Table 53 Replication Subsystem Error Messages

Message & Description	Fields	Suggested Action
REPLICATE.SYNC.FAILED A synchronization event failed. An alert is sent to the **system-alerts** distribution list, and an SNMP trap is sent to any specified SNMP trap receiver.	❖ Master hostname ❖ Replica hostname ❖ Sync ID ❖ Numeric code indicating type of failure	Analyze the failure indicated by the numeric code in the message and correct the problem.
REPLICATE.SERVER.FAILED The Replication server failed to start on the Replica system. An alert is sent to the **system-alerts** distribution list and an SNMP trap is sent to any specified SNMP trap receiver.	❖ Master hostname ❖ Replica hostname ❖ Sync ID ❖ Numeric code indicating type of failure	Analyze the failure indicated by the numeric code in the message and correct the problem.
REPLICATE.CONFIG.ERROR The Replication system detects erroneous data in its configuration file. An alert is sent to the **system-alerts** distribution list and an SNMP trap is sent to any specified SNMP trap receiver.	❖ Parameter name ❖ Out-of-range parameter value ❖ Default value to be substituted	The system automatically ignores the invalid value and uses the indicated default value. If you do not want the indicated default used, modify the configuration file with another valid value.
REPLICATE.COMM.FAILURE The Master could not contact the Replica. An alert is sent to the **system-alerts** distribution list and an SNMP trap is sent to any specified SNMP trap receiver.	❖ Master hostname ❖ Replica hostname ❖ Numeric code indicating type of failure	Analyze the communication failure indicated by the numeric code in the message and correct the problem.
REPLICATE.VERSMISMATCH.MOS A system software release version mismatch between the Master and Replica was detected at the start of a **Sync** operation or when attempting to **Switchover** to the Replica.	❖ Master version number ❖ Replica version number	Ensure that both the Master and Replica systems have identical system software releases installed, then restart the operation.
REPLICATE.VERSMISMATCH.PATCH A patch-set mismatch between the Master and Replica is detected at the start of a **Sync** operation or when attempting to **Switchover** to the Replica.	❖ Patches only on the Master ❖ Patches only on the Replica	Ensure that both the Master and Replica systems have identical patch-sets installed, then restart the operation.
REPLICATE.VERSMISMATCH.REPLICATE A Replication software mismatch between the Master and Replica is detected at the start of a Sync operation. An alert is sent to the system-alerts distribution list and the operation stops.	❖ Master replicate software version number ❖ Replica replicate software version number	Ensure that both the Master and Replica systems have identical Remote Server Replication software versions installed, then restart the operation.

Updating Systems

The Master and Replica system must both run the exact same configuration when you run **Replicate To** on the Master during initial configuration. It is a good idea to always keep the system configurations identical so the Replica is running the same features if you switch, but RSR does not require it. RSR requires only that the RSR versions are compatible. To keep the configurations identical, at the time any replication operation is run, both systems must have the same exact MOS release and patch set.

There is no procedural requirement such as installing software on the Master system first and then on the Replica. Just ensure that any software updates are installed on both systems in between synchronizations; otherwise the next synchronization operation fails, returning a version mismatch error indicating the inconsistent software.

Aborting a Synchronization in Progress

To abort a synchronization that is in progress, on the Master or Replica system:

```
Replicate Cancel
* Sync Operation Terminated
OK Completed
```

If no action is indicated in response to the **Replicate Cancel** command:

```
Replicate Cancel
OK Completed
```

Then no synchronization was running.

If you abort a synchronization on the Master, the process stops and no delta is sent to the Replica.

If you abort a synchronization on the Replica system, it stops the replication server on the Replica so no more data can be transferred from the Master. Depending on the timeout set on the Master, it might continue trying to transfer unless you abort it on the Master. To start the replication system again on the Replica, run **Replicate Restart**.

If you abort a synchronization on the Replica while it is applying a delta from the Master, the **Replicate Cancel** command can fail.

Removing a Replica Configuration

To terminate the entire replication process and remove all replication information for both systems, on both the Master or Replica system:

1. On both the Master and Replica systems, erase all replication information:

   ```
   Replicate Clear
   OK Completed
   ```

2. On the Master system, remove any scheduled commands, such as **Replicate Sync** or **Replicate Checkswitch**:

   ```
   Schedule Delete Replicate Sync
   Schedule Delete Replicate Checkswitch
   OK Completed
   ```

The **Clear** command cancels any replication processes underway, except for data from the Master being copied into the message store on the Replica, and removes all the replication data on that system. Once complete on both systems, there is no remaining indication that RSR was used on either system.

If you run the **Clear** command on only the Master, the Replica remains viable, albeit increasingly out of date. If you run the **Clear** command on only the Replica, the Master might continue to attempt delta transfers to the Replica.

Performing a Failover

If the Master system fails, the Replica system can assume the role of the Master. On the Replica system:

1. Confirm that the Replica system is ready to take over as the Master:

   ```
   Replicate Checkswitch
   OK Completed
   ```

2. Check the status of the Replica to confirm expectations for the currency of the Replica's data (statistic descriptions provided in Table 51 on page 385):

   ```
   Replicate Status
   Host Role is: [Master|Replica|Undecided]
   Sync is: [Active|Inactive]
   Delta Application is: [Active|Inactive]
   Replica Current As Of: ISO DATE-TIMESTAMP; HH:MM Ago
   NOTE: Replica NOT Viable, No Syncs Completed
   Last Sync: [Applying|Running|Completed|Failed|Cancelled|None]
   Last Completed Sync Size: integer MB Elapsed Time: HH:MM
   Syncs: Attempted: integer, Completed: integer, Failed/Cancelled: integer
   Replication Server: [Running|Down|Unreachable]
   Master Store Size: integer MB, Used: integer MB, Inodes: integer, Used:
   integer
   Replica Store Size: integer MB, Used: integer MB, Inodes: integer,
   Used:integer
   OK Completed
   ```

3. Enter the **Switchover** command:

   ```
   Replicate Switchover
   * Stopping Services
   * Installing Replica Store
   * Scheduling Reboot
   OK Completed
   ```

   The switchover typically completes in under one minute.

4. Reconfigure your network infrastructure as needed, including LDAP and DNS settings, so the Replica system is recognized by the network as taking the place of the Master. This task varies depending on your network configuration.

   For example, you likely need to change the DNS records so the IP address of the failed Master now points to the Replica.

The Replica system is now effectively the Master, providing normal mail services. To create a Replica for this system, now that it is the Master, follow the normal instructions for configuring a Replica.

Before you perform a **License Fetch** on the new Master, you must contact Mirapoint Technical Support and inform them that you switched over to your Replica system. Provide the former and current host-ids so Mirapoint can update your licenses to reflect the change.

Restoring a Master

After switching over from a Master system to a Replica, if you want to later return the original Master to being the Master again, use the E3_migrate_7 patch. For instructions, see the E3_migrate_7 Patch Notes.

Index

Symbols

"X" headers, about 163

A

abbreviations used in logs 350
about
  content policies (domain filters) 236
  Destination Domain option 238
  domains 179
  LDAP GUI 51
  LDAP GUI and LDAP GUI-JMM 85
  LDAP user records 23
  MIME and filtering attachments 239
  Remote Server Replication
  the Blacklist header 314
  the **Junk Mail** filter 305
  the message queue 157
  the Recipient-Whitelist header 316
  the Whitelist header 312
  trusted network specifiers 35
  UCE Score Threshold 240
  users and administrators 203
access control
  changing 216
  folders 212
  permissions defined 212
accessing
  Administration Suite 24
  Administration Suite Wizard 26
  command line interface 26
  delegated domains 186
  restricted for administrators 34
  setting default 74
accounts
  autoprovisioning, all-in-one 58
  autoprovisioning, multi-tier MMS 94
  definition 203
Active Directory
  getting the bindDN, all-in-one 76
  getting the bindDN, multi-tier MMS 112
  setting up, all-in-one 55
  setting up, multi-tier MMS 91
Add/Edit Folders page 214
adding
  an antispam license 47
  arrays 171
  blocked domains 318
  classes of service 228
  delegated domain administrators to the postmaster DL 184
  delegated domains 182
  delegated domains, tasks 181
  distribution lists 221
  distribution lists to distribution lists 221
  groups, Operations Console 330
  members to distribution lists 221
  quarantine administrators 325
  remote members to distribution lists 221
  SNMP traps 177
  sub-folders 217
  users 206
address book
  configuring URLs, all-in-one 60
  Url Add
    multi-tier MMS 98
  Url Add all-in-one 60
  URLs, all-in-one 60
  URLs, multi-tier MMS 98
  verifying the URL, all-in-one 73
  verifying the URL, multi-tier MMS 111
addresses
  blocking 257
  character limitations 204
  example wiretaps 253
  restricting for administration 34
addressing mail
  to folders 218
  to sub-folders 218
Admin Audit Trail report 175
administering groups, Operations Console

330
Administration Suite
accessing 24
accessing the Setup Wizard 26
administrator daily reports 336
setting the default timeout 41
text display 25
using the Setup Wizard 25
administration, setting security 35
administrators
about 203
accessing a user's folder 186
creating for delegated domains 183
default distribution lists 138
password recommendation 28
quarantine 325
quarantine administrator 203
restricting access 34
alarms, silencing 172
alerts
antivirus notifications, RAPID 300
antivirus notifications, Sophos and F-Secure 293
management 333
system health 174
viewing for groups 332
all-in-one deployment
antispam 47
antivirus 42
configuring MailHurdle 46
configuring user directory service 51
example 37
internal LDAP directory 51
required information 38
required licenses 39
setting up Active Directory 55
troubleshooting 76
verifying 70
Allowed Mailing Lists
about the Junkmail header 316
creating 315
domain level, creating 315
preventing MailHurdle delays 316
removing entries 316
searching for entries 316
setting 314
Allowed Senders
creating 311
domain level, creating 310
entries, finding 311
for antispam scanning 310
antispam
allowed senders 310
blocked senders 312
example filters 320
mailing list exemptions 314
RBL Host lists 319
reject lists 318
relay lists 317
Anti-Spam Information report 364
antispam scanning
about 303
about the **Threshold** 240
adding a license 47
configuring for all-in-one 47
configuring for multi-tier 122
configuring for multi-tier MMS 83
configuring MailHurdle 282
configuring second scan 59, 123
destination domains, about 238
DSN (delivery status notification) filters 246
filtering out "virus deleted" messages 321
getting an immediate update 310
installing or removing rule groups 309
Junk Mail filter, about 305
modifying 306
Principal Edition vs **Signature Edition** 304
scanning outbound mail 308
setting the proxy server 310
specifying automatic updates 310
threshold differences 240
using security quarantine 325
Anti-Virus Reports 362
antivirus scanning
available engines 288
common extension names 240
configuring for all-in-one 42
how quarantine works 290
predictive-based 289
recommendation 39
recommendations 42
signature-based 289
signature-based, configuring for multi-tier 121
types of viruses 289
antivirus scanning, RAPID
checking current information 303
configuring 299
configuring for multi-tier 121
getting an immediate update 303
getting updates 301

setting notifications 300
setting the proxy server 302
specifying automatic updates 302
antivirus scanning, Sophos or F-Secure
checking current information 298
configuring 291
getting an immediate update 298
getting updates 296
setting notifications 293
setting the proxy server 298
specifying automatic updates 297
Array properties 171
arrays
adding/configuring 171
deleting 172
installing 171
assigning
classes of service 229
quarantine administrator 325
attachments
about MIME and filtering 239
blocked, specifying 262
common virus extensions 240
redirected, specifying 264
authentication
and filters 249
SMTP and MailHurdle 285
autochanger, *see* tape library
autoprovisioning
setting up, all-in-one 58
setting up, multi-tier MMS 94
auto-reply
enabling for domains 183
Average Number of Recipients Summary report 355
Average Size Summary report 355

B

backup schemes
image-based 370
message-based 370
backups
about tape drives and libraries 371
full vs. incremental vs. selective 370
image based 370
supported DMAs
what data gets backed up 370
BakBone NetVault, supported versions 372
banner delay, configuring 59, 95, 122
bindDN for Active Directory, all-in-one 76
bindDN for Active Directory, multi-tier MMS 112
blacklist header, about 314
blade servers, monitoring functions 137
blocked
addresses 257
attachments 262
messages 260
Blocked Senders
creating 313
finding entries 313
header, about 314
searching for entries 313
boolean operators 166

C

calendar
configuring URLs, multi-tier MMS 100
enabling/starting, all-in-one 64
enabling/starting, multi-tier MMS 101
group calendar, all-in-one 62
group calendar, multi-tier MMS 99
setting timeout 102
setting timeout, all-in-one 64
URLs, all-in-one 63
calendars, subscribed, setting 200
changing
default user limit in a delegated domain 192
folder access control 216
folder access permissions 216
folder quotas 216
passwords for users 208
SMTP listenport 323
user data 208
characters
disallowed for email addresses 205
prohibited in folder names 212
checking
current antivirus information, RAPID 303
current antivirus information, Sophos 298
for software updates 32
the message queue 165
checking for licenses 41
class of service
adding and populating 228
assigning 229
configuring message expiration 234
configuring message undelete 233
definition 225
deleting 231
editing 230

enabling 90
enabling, all-in-one
features 226
finding 230
inheritance and dependencies 226
selecting services 227
clearing, the message queue 159
CLI commands
Ndmp Merge Status 371
CLI. *See* command line interface
CNAME records, for multi-tier 23
codes used in reports 357
colors, dashboard 333
command line interface
accessing 26
Command Report 367
configuration
pre-configuration checklist 21
SNMP 176
configuring
antispam scanning 306
arrays 171
banner delay 59, 95, 122
Junk Mail Manager, multi-tier deployment 124
NIC failover 324
second scan for antispam 59, 123
security screening, multi-tier deployment 119
configuring address book
URLs for all-in-one 60
URLs for multi-tier MMS 98
configuring antispam
for all-in-one 47
for multi-tier 122
for multi-tier MMS 83
configuring antivirus
for all-in-one 42
for multi-tier, RAPID 121
for multi-tier, signature-based 121
configuring calendar
URLs for all-in-one 63
URLs for multi-tier MMS 100
configuring IMAP
for all-in-one 66
for multi-tier MMS 103
configuring MailHurdle
for all-in-one 46
for multi-tier deployment 119
configuring SMTP
for all-in-one 67
for multi-tier MMS 104
configuring user directory service
for all-in-one 51
for multi-tier MMS 87
configuring WebMail
for all-in-one 65
for multi-tier MMS 102
connections, SNMP setup 176
content filtering
blocked addresses 257
blocked attachments 262
blocked messages 260
creating corporate word list 267
creating objectionable word list 269
creating wire taps 252
filter list entries 255
filter list words & phrases note 255
how quarantine works 241
order, general 239
redirected attachments 264
using the filter list 254
Content Filtering Statistics report 364
content policies
about 236
creating 237
example filters 250
cookies, requiring 66, 102
corporate word list, creating 267
COS, *see* class of service
CPU Activity graph
definitions 156
description 156
example use 156
CPU usage, troubleshooting 141
creating
administrators for delegated domains 183
Allowed Mailing Lists 315
Allowed Senders entries 311
antispam black lists 312
antispam mailing list exemptions 314
Blocked Senders entries 313
content policies 237
corporate word list 267
delegated domain signatures 189
distribution lists in delegated domains 188
domain black lists 312
domain mailing list exemptions 315
domain quota messages 190
domain white lists 310
folders in delegated domains 187
groups, Operations Console 330

message filters 243, 244
objectionable word list 269
over-quota message delegated domains 190
RBL Host lists for antispam 319
Reject lists for antispam scanning 318
Relay lists for antispam 317
shared folders 217
storage policies 232
white lists for antispam 310
wire taps 252
customizing
over-quota message for delegated domains 190
quota messages for domains 190

D

daily reports, attachments summary 336
dashboard
colors 333
how to use 332
data management application (DMA) 374
defaults
boolean operator 165
calendar timeout 64
changing user limit, delegated domains 192
distribution lists for administrators 138
filtering order 239
maximum number of group members 330
order of filtering 239
performance graphs view 139
quarantine folder, RAPID AV 44
setting HTTP access 74
telnet port 26
user folder location 203
virus alerts, Sophos and F-Secure 295
defaults, WebCal
main configuration 195
resources configuration 197
search configuration 196
setting in delegated domains 192
delegated domains
accessing 186
accessing a user's folder 186
adding the administrator to the postmaster DL 184
adding, procedure 182
adding, task overview 181
Allowed Senders for 310
Blocked Senders 312
changing the default user limit 192
creating Allowed Mailing Lists 315
creating distribution lists 188
creating folders 187
creating signatures 189
creating the administrator 183
custom over-quota message 190
deleting 202
disk quota 182
editing 186
enabling auto-reply 183
enabling distribution lists 183
enabling forwarding 183
finding 184
LDAP enabled 181
limit 181
quarantine filters 242
quota messages for 190
recommended use 39, 117
routing messages 180
selecting 184
selecting as current 185
sensitivity 181
setting user limit 182
setting user limits 187
spanning multiple message servers 192
delegated domains, WebCal
main configuration 195
resources configuration 197
search configuration 196
setting defaults 192
subscribed calendars 200
deleting
arrays 172
classes of service 231
delegated domains 202
distribution lists 223
folders 218
groups, Operations Console 330
spares 170
storage policies 236
traps 177
users 209
deployments
all-in-one 37
multi-tier 115
multi-tier MMS 79
Destination Domain, filtering option 238
Detailed Login Report 360
Detailed Mail Log report 356
Detailed Virus Scanning Information report

363
directory service
address book URL, all-in-one 60
address book URL, multi-tier MMS 98
testing, all-in-one 73
testing, multi-tier MMS 111
disallowed characters for email addresses 205
Disk properties 169
Disk Usage Information graph
definitions 152
description 152
Disk view, properties 169
distribution lists
adding distribution lists to 221
adding remote members to 221
adding/removing 221
adding/removing members 221
as aliases for users 220
creating in delegated domains 188
defaults 138
deleting 223
deleting, troubleshooting 224
editing 223
enabling for domains 183
entry properties 219
finding 223
naming 220
reserved names 220
DIT, definition 52, 87
DLs, *see* distribution lists
DMA, definition
DNS
multi-tier deployment 22
multi-tier MMS deployment 81
replication process 382
requirements 21
domain disk quota
setting 182
domain names, definition 179
domains
about 179
about content policies 236
creating black lists 312
creating mailing list exemptions 315
creating quota messages 190
creating white lists 310
primary, definition 179
domains, delegated
accessing 186
accessing a user's folder 186
adding the administrator to the postmaster DL 184
adding, procedure 182
adding, task overview 181
changing the user limit 192
creating distribution lists 188
creating folders 187
creating signatures 189
creating the administrator 183
custom over-quota message 190
deleting 202
disk quota 182
editing 186
enabling auto-reply 183
enabling distribution lists 183
enabling forwarding 183
finding 184
LDAP enabled 181
properties 180
routing messages 180
selecting as current 185
setting user limit 182
setting user limits 187
setting WebCal defaults 192
spanning multiple message servers 192
WebCal main configuration 195
WebCal resources configuration 197
WebCal search configuration 196
WebCal subscribed calendars 200
what you can control 180
domains, delegated limit 181
dotted-quad, definition 35
DSN (delivery status notification) filters 246

E

editing
antivirus notifications, RAPID 300
antivirus notifications, Sophos and F-Secure 293
blocked addresses list 257
blocked attachments list 262
blocked messages list 260
classes of service 230
corporate word list 267
delegated domains 186
distribution lists 223
folders 214
groups, Operations Console 330
messages filters 244
objectionable word list 269
redirected attachments list 264
storage policies 235

traps 177
user data 208
wire taps list 252
enabling
calendar, all-in-one 64
calendar, multi-tier MMS 101
class of service 90
class of service, all-in-one
domain distribution lists 183
domain mail auto-reply 183
domain mail forwarding 183
IMAP, all-in-one 67
IMAP, multi-tier MMS 104
LDAP directory service, all-in-one 53
LDAP directory service, multi-tier MMS 88
LDAP GUI 51
SMTP, all-in-one 68
SMTP, multi-tier MMS 105
WebMail 66
envelopes, messages, reading 162
example filters
antispam 320
content policies 250
exiting the groups administer pages 331
expired licenses, note 22
exporting
corporate word lists 267
group data 332
objectionable word lists 269
exporting groups 332
External Server Monitoring graph
definitions 151
example use 150

F

Failed Logins by Remote IP Address report 361
Failed Logins by User report 361
failover, for RSR 392
filter examples, antispam
discard based on UCE score 320
exe files 322
jpeg files 322
messages with deleted viruses 321
quarantine based on UCE score 320
RBL-tagged messages 323
virus deleted messages 321
filter examples, content policies
mail to competitors 250
over-sized messages 251
social security number 250
specific words 250
too many recipients 251
wire taps 251
filter list
entries 255
guidelines for using 253
integrating new words 256
using 254
words & phrases note 255
filtering
about content policies 236
about MIME and attachments 239
about the antivirus quarantine 290
about the Content Filtering quarantine 241
about the Quarantine Administrator 203
common virus attachment names 240
creating filters 244
Forward to vs. **Send to Quarantine folder** filter actions 257
order executed 239
order, general 239
priority levels 239
reordering filters 249
using patterns 230
using the **Keep** (**process normally**) option 257
filters
Allowed Mailing Lists 314
Allowed Senders 310
blocked addresses 257
blocked attachments 262
blocked messages 260
Blocked Senders 312
corporate word list 267
creating 244
destination domain 238
filter list entries 255
filter list words & phrases note 255
for DSN (delivery status notifications) 246
Junk Mail, about 305
objectionable word list 269
redirected attachments 264
reordering 249
using for empty **To**/**CC** lines 247
using the filter list 254
using wordlists 253
wire taps 252

filters, domains
black lists 312
mailing list exemptions 315
white lists 310
finding
Allowed Senders entries 311
Blocked Senders entries 313
classes of service 230
delegated domains 184
directory service contacts, all-in-one 73
directory service contacts, multi-tier MMS 111
distribution lists 223
folders 213
messages in the queue 165
users 208
First Use screen 26
flushing MailHurdle triplet cache 288
flushing the queue for a domain 167
Folder Size & Quota Information report 368
folders
access control 216
access control lists 212
access permissions meanings 212
accessing in delegated domains 186
adding sub-folders 217
address mail to sub-folders 218
addressing mail to 218
changing access permissions 216
changing quotas 216
creating in delegated domains 187
default for RAPID AV 44
definition 211
deleting 218
finding 213
Folder Size & Quota Information report 368
hierarchy separator 211
Largest 50 Folders report 368
naming conventions 211
removing quotas 208
renaming 216
root 211
setting quotas 207
setting the domain disk quota 182
shared, creating 217
special characters you cannot use 212
Top 50 Folders Nearest Quota report 368
using patterns to search 230
working with 214
folders reports 367
font conventions 15
Forward to vs. **Send to Quarantine folder** filter actions 257
forwarding
enabling for domains 183
F-Secure antivirus
checking current information 298
configuring 291
getting an immediate update 298
getting updates 296
setting notifications 293
setting the proxy server 298
specifying automatic updates 297
full backup, definition 370
full name, definition 204
fully qualified domain name (FQDN), definition 179
function, definition 116

G

gauges for performance graphs 140
group calendar
configuring URLs, all-in-one 63
Mail Routing license requirement 133
setting up, all-in-one 62
setting up, multi-tier MMS 99
url add
syntax, all-in-one 62
syntax, multi-tier MMS 99
URLs, multi-tier MMS 100
groups, Operations Console
adding, editing, deleting 330
administering 330
creating 330
Dashboard page 332
exiting the administer pages 331
importing/exporting data 332
synchronizing 331
GUI, *see* Administration Suite

H

hardware, monitoring disk, array, and store views 169
headers, messages
about "X" headers 163
reading 162

hosts, SNMP configuration 177
HTTP Root, setting 74

I

IDE, definition 168
image based backups 370
IMAP
  configuring, all-in-one 66
  configuring, multi-tier MMS 103
  enabling, all-in-one 67
  enabling, multi-tier MMS 104
  quota warning limit, all-in-one 67
  quota warning limit, multi-tier MMS 103
importing
  corporate word lists 267
  group data 332
  objectionable word lists 269
importing groups 332
incremental backup, definition 370
installing
  antispam rule groups 309
  hot spare disks 170
  MailHurdle known good mailers 309
  new arrays 171
  Remote Server Replication 384
internal LDAP directory
  configuring for all-in-one 51
  configuring for multi-tier MMS 87
international login names 205
IP addresses
  setting "trusted" 34

J

JMM, *see* Junk Mail Manager
jukebox, *see* tape library
Junk Mail Manager
  configuring for multi-tier deployment 124
  LDAP GUI 85
  provisioning users, multi-tier deployment 125
junk mail scanning, *see* antispam scanning
Junk Mail Statistics graph
  "Total Messages" note 147
  definitions 147
  description 146

L

Largest 50 Folders report 368
LDAP
  license required 41
  replication process 382
  user records 23
LDAP attributes
  group calendar, all-in-one 62
  group calendar, multi-tier MMS 99
LDAP directory service
  enabling, all-in-one 53
  enabling, multi-tier MMS 88
  for delegated domains 181
  Mail Routing license and Group Calendar 133
LDAP Directory Statistics, graph
  definitions 148
LDAP Enabled, pages 51
LDAP GUI
  and LDAP GUI-JMM 85
  enabling, all-in-one 51
Legato NetWorker, supported versions 373
licenses
  all-in-one deployment 39
  checking 41
  expired 22
  MailHurdle not displaying 41
  required for multi-tier MMS 81
Lightweight Directory Access Protocol, *see* LDAP
limiting TCP connections 60
Local Mail Traffic report 353
logging in
  Administration Suite 24
  command line interface 26
  to Mirapoint Support 16
login account, definition 203
login names
  international 205
  permitted characters 204
  reserved 205
Login Summary repor 353
Login Traffic Rates report 359
LoginID LDAP attribute, definition 62
logins
  tracking with the Admin Audit Trail 175
  tracking with the User Audit Trail 175
logins reports
  Detailed Login Report 360
  Failed Logins by Remote IP Address 361
  Failed Logins by User 361
  Login Summary 353
  Login Traffic Rates 359
  options 358
  Top Logins By User 359

logs
Remote Server Replication 389
logs, abbreviations 350

M

mail reports
Average Number of Recipients Summary 355
Average Size Summary 355
Detailed Mail Log 356
Local Mail Traffic 353
Mail Traffic Summary 354
Message Events by Hour 355
options 351
Remote Mail Traffic 354
searching 358
Top Mail Users 351
Mail Routing license 41
Mail Traffic graph
definitions 143
description 142
what to look for 143
Mail Traffic Summary report 354
mail, addressing to folders 218
Mailhost LDAP attribute, definition 62
MailHurdle
advanced options 286
Allow Known Good Mailers 120
Allowed Host page 285
Allowed Mailing Lists, where placed 316
and SMTP authentication 285
antispam, about 282
flushing the triplet cache 288
license not displaying 41
modifying 283
reports 365
searching for triplets 287
MailHurdle report 365
MailHurdle, configuring
for all-in-one 46
for multi-tier deployment 119
Mailroutingaddress LDAP attribute, definition 62
managing
quarantines 241
storage policies 231
mask-bits, definition 35
Message Events by Hour report 355
message expiration
setting up 234
message filters
about MIME and filtering attachments 239
about the quarantine action 241
creating 244
filter list entries 255
filter list words & phrases note 255
how quarantine works 241
Junk Mail, about 305
reordering 249
using patterns 230
using the filter list 254
using the **Keep** (**process normally**) option 257
message queue
about 157
clearing 159
flushing for a domain 167
refreshing 159
sorting messages 160
viewing messages 161
viewing the summary 159
Message Server
Administration Suite access 24
all-in-one deployment 37
multi-listeners configuration 323
multi-tier MMS deployment 79
setting up the internal LDAP, all-in-one 51
setting up the internal LDAP, multi-tier MMS 87
user autoprovisioning 58
message undelete, setting up 233
messages
addressing to sub-folders 218
clearing the queue 159
codes used in reports 357
flushing the queue for a domain 167
in queue, what you can view 165
order of filtering 239
refreshing the queue 159
releasing from quarantine 242
routing to delegated domain 180
searching the queue 165
sorting the queue 160
top content concerns 237
viewing in the queue 161
viewing the queue summary 159
messages, setting
expiration 234
undelete 233

MIME, about 239
Mirapoint
  Support Site URL 16
Mirapoint recommends
  administrator passwords 28
  antivirus engines 39
  using an NTP server 30
Misc graph
  definition 149
  description 149
miUUID LDAP attribute, definition 62
MOC, *see* Operations Console
modifying
  antispam scanning 306
  antivirus scanning, RAPID 299
  antivirus scanning, Sophos or F-Secure 291
  MailHurdle 283
monitoring
  adding/configuring arrays 171
  deleting arrays 172
  deleting spares 170
  for RGs on blade servers 137
  Remote Server Replication 388
  scanning the RAID system 172
  silencing alarms 172
  system alerts 174
  system health data tables 173
  using the views: **Disk**, **Array** , and **Store** 169
  viewing **Alerts** data 333
  viewing array data 170
  viewing disk data 169
  viewing storage data 167
  viewing store data 172
  viewing system health data 173
  weekly reports 337
MOS, definition 32
MTA, definition 157
Mtaverify rule group 120
MTL, definition 16
multi-listeners, configuring 323
multi-tier deployment
  configuring antispam 122
  configuring Junk Mail Manager 124
  configuring MailHurdle 119
  configuring RAPID antivirus 121
  configuring security screening 119
  configuring signature-based antivirus 121
  DNS recommendations 22
  example 115
  provisioning users for JMM 125
  requirements 116
multi-tier MMS deployment
  configuring antispam 83
  configuring internal LDAP directory 87
  configuring user directory service 87
  example 79
  required information 80
  required licenses 81
  requirements 79
  setting up Active Directory 91
  tasks 81
  troubleshooting 112
  user autoprovisioning 94
  verifying 107

N

naming
  about domains 179
  distribution lists 220
  folders 211
  folders, renaming 216
  international login names 205
  reserved distribution list names 220
Ndmp Merge Status command 371
NDMP, *see* Network Data Management Protocol
Netif Setlogical command 324
Network Data Management Protocol
  about 372
  image based backups 370
  setting up 374
  supported DMAs 372
network specifiers, about 35
network time protocol, *see* NTP
Network Traffic graph
  definitions 154
  description 154
NIC failover alert message 325
NIC failover, configuring 324
non-ASCII characters in login names 204
nonconformant mailers 120
notifications, antivirus scanning
  RAPID 300
  Sophos and F-Secure 293
NTP
  replication process 382
  server recommendation 30

O

objectionable word list, creating 269
Operations Console
  adding, editing, and deleting groups 330
  administering groups 330
  alerts, management 333
  creating groups 330
  default groups 330
  groups, management 328
  groups, maximum allowed 330
  synchronizing groups 331
order of filtering, default 239
outbound mail, antispam scanning 308
over-quota messages
  creating for domains 190

P

passwords
  administrator recommendation 28
  changing for users 208
  definition 204
patterns, using in searches 230
performance graphs
  about the different views 139
  gauges 140
  Junk Mail Statistics 146
  LDAP Directory Statistics 147
  Mail Traffic 142
  pie charts 139
  POP/IMAP Activity 144
  WebMail Activity 145
pie charts categories 139
POP/IMAP Activity graph
  definitions 144
  description 144
ports
  telnet default 26
postmaster DL, adding delegated domain administrators to 184
pre-configuration checklist 21
predictive-based antivirus scanning 289
primary domain, definition 179
Principal Edition antispam scanning 304
priority levels, filtering 239
provisioning
  user accounts 209
  users for JMM, multi-tier deployment 125
proxy
  antispam scanning 310
  setting for virus scanning, RAPID 302
  setting for virus scanning, Sophos 298

Q

quarantine
  about the Quarantine Administrator 203
  antivirus scanning, about 290
  assigning the administrator 325
  content filtering, about 241
  default folder, RAPID AV 44
  monitoring the quarantine folder 242
  releasing messages from 242
  two types 241
  usage tips 242
  using 325
queue
  about 157
  clearing 159
  flushing for a domain 167
  refreshing 159
  sorting messages 160
  viewing messages 161
  viewing the summary 159
quotas
  changing, folders 216
  creating over-quota messages 190
  custom message for delegated domains 190
  removing on folders 208
  setting delegated domain user limits 187
  setting domain user limits 182
  setting for delegated domains 182
  setting on user folders 207
  warning limit for IMAP, all-in-one 67
  warning limit for IMAP, multi-tier MMS 103

R

RAID, definition 168
RAPID antivirus
  checking current information 303
  configuring 299
  getting an immediate update 303
  getting updates 301
  setting automatic updates 302
  setting notifications 300
RAPID AV
  default quarantine folder 44
RazorGate
  Administration Suite access 24
RBL Host lists
  for antispam scanning 319

redirected attachments, specifying 264
refreshing the message queue 159
Reject lists, for antispam 318
Relay lists, for antispam scanning 317
Remote Mail Traffic report 354
Remote Server Replication
about
Get/Set descriptions 386
installing 384
logs 389
monitoring 388
performing a failover 392
removing a configuration 391
restoring a master 393
status descriptions 385
stopping a synchronization 391
subsystem error messages 390
synchronizations 386
system requirements 383
updating systems 391
verifying replica readiness 388
removing
a replica configuration 391
Allowed Mailing Lists entries 316
Allowed Senders entries 312
Blocked Senders entries 314
distribution lists 223
members from distribution lists 221
users 209
renaming folders 216
reordering filters 249
reports
abbreviations used 350
codes used 357
daily, attachments summary 336
email traffic 351
large, saving 356
protocol commands 367
security-related events 362
system, **System Information** 366
User Audit Trail 175
reports, folders
Folder Size & Quota Information 368
Largest 50 Folders 368
sections 367
Top 50 Folders Nearest Quota 368
reports, logins
Detailed Login Report 360
Failed Logins by Remote IP Address 361
Failed Logins by User 361
Login Summary 353
Login Traffic Rates 359
sections 358
Top Logins By User 359
reports, mail
Average Number of Recipients Summary 355
Average Size Summary 355
Detailed Mail Log 356
Local Mail Traffic 353
Mail Traffic Summary 354
Message Events by Hour 355
Remote Mail Traffic 354
searching 358
Top Mail Users 351
reports, security
Anti-Spam Information 364
Anti-Virus reports 362
Content Filtering Statistics 364
Detailed Virus Scanning Information 363
MailHurdle 365
sections 362
Virus Scanning Summary 362
required licenses
all-in-one deployment 39
multi-tier MMS deployment 81
reserved login names 205
resources, configuring for WebCal 197
restricting administrator access 34
roles
about the Quarantine administrator 203
about users and administrators 203
Administrator 206
root, definition 211
routing
all-in-one deployment 50
multi-tier MMS deployment 85
round-robin DNS records 23
to delegated domains 180
RSR, *see* Remote Server Replication

S

saving large reports 356
Scan button 172
scheduling
synchronizations for RSR 386
searching
default boolean operator 165
for MailHurdle triplets 287
searching for
Allowed Mailing List entries 316
Allowed Senders entries 311

Blocked Senders entries 313
delegated domains 184
distribution lists 223
folders 213
mail reports 358
messages in the queue 165
setting WebCal defaults 196
second scan for antispam, configuring 59, 123
secure shell, *see* SSH
Secure Socket Layer, *see* SSL
securing WebMail session IDs
all-in-one 66
multi-tier MMS 102
security reports
Anti-Spam Information 364
Anti-Virus Reports 362
Content Filtering Statistics 364
Detailed Virus Scanning Information 363
MailHurdle 365
options 362
Virus Scanning Summary 362
security screening, multi-tier 119
security, setting for administration 35
selecting delegated domains 185
selective backup, definition 370
selective restore from image 370
Send to Quarantine folder filter action 241
service reporting, setting 31
session IDs
securing for WebMail, all-in-one 66
securing for WebMail, multi-tier MMS 102
setting
administration security 35
Administration Suite timeout 41
calendar timeout 102
calendar timeout, all-in-one 64
default HTTP access 74
delegated domain user limits 187
domain user limits 182
notifications, RAPID antivirus 300
quota warning limit for IMAP, all-in-one 67
quota warning limit for IMAP, multi-tier MMS 103
service reporting 31
SSL version 277
the domain disk quota 182
timeout for WebMail, all-in-one 66
timeout for WebMail, multi-tier MMS 103
trusted IP addresses 34
WebCal defaults for delegated domains 192
WebCal main configuration for delegated domains 195
WebCal resources configuration for delegated domains 197
WebCal search configuration for delegated domains 196
WebCal subscribed calendars for delegated domains 200
setting up
group calendar, all-in-one 62
group calendar, multi-tier MMS 99
message expiration 234
message undelete 233
NDMP service and clients 374
user autoprovisioning 94
user autoprovisioning, Message Server 58
Setup Wizard, accessing 26
Setup Wizard, using 25
shared folders, creating 217
Signature Edition antispam scanning 304
signature-based antivirus scanning 289
signatures, creating for delegated domains 189
Silence Alarm button 172
SMTP
stopping traffic 167
SMTP configuration
all-in-one deployment 67
and MailHurdle 285
changing the listenport 323
enabling, all-in-one 68
enabling, multi-tier MMS 105
multi-tier MMS deployment 104
specifying reject lists 318
specifying relay lists 317
Smtp Set Bannerdelay *see* banner delay
SNMP configuration
hosts
adding
SNMP hosts 177
traps 177
Sophos antivirus
checking current information 298
configuring 291
getting an immediate update 298
getting updates 296
setting notifications 293
setting the proxy server 298

specifying automatic updates 297
sorting, messages in the queue 160
spam, *see* antispam scanning
spares
deleting 170
special characters prohibited in folder names 212
specifying
blocked addresses 257
blocked attachments 262
blocked messages 260
redirected attachments 264
SSH
administration security 35
SSL
administration security 35
setting version 277
stopping
an RSR synchronization 391
SMTP traffic 167
storage
adding/configuring arrays 171
deleting arrays 172
IDE, data available 168
viewing array data 170
viewing data 167
viewing disk data 169
viewing store data 172
storage polices
managing 231
storage policies
creating 232
deleting 236
editing 235
Store properties 172
Store view, properties 172
sub-folders
adding 217
addressing mail to 218
support
getting a login ID 16
getting a Mirapoint Support login ID 16
supported DMAs
synchronizing groups, Operations Console 331
system
deleting users 209
editing users 208
health alerts 174
health data tables 173
viewing health data 173
System Information report 366
system reports, **System Information** 366
system requirements, Remote Server Replication 383
system, services configuration
SNMP 176

T

tape drives, about 371
tape libraries, about 371
TCP connections
limiting 60
telnet, default port 26
tier, definition 116
timeout
setting for Administration Suite 41
setting for calendar 102
setting for calendar, all-in-one 64
setting for WebMail, all-in-one 66
setting for WebMail, multi-tier MMS 103
Tivoli Storage Manager, supported versions 373
Top 50 Folders Nearest Quota report 368
top email concerns 237
Top Logins By User report 359
Top Mail Users report 351
top-level domain, definition 179
traps configuration 177
triplets
definition 282
flushing 288
searching for 287
troubleshooting
adding an antispam license 47
adding folders 211
Administration Suite text display 25
alias addresses 207
all-in-one 76
all-in-one deployment required information 38
Allowed/Blocked Senders filters 310
antispam scanning, end-user options 305
class of service selection 227
CPU usage 141
distribution lists, deleting 224
domain disk quota 182
domain sensitivity 181
email address character limitations 204
expired LDAP-related licenses 22
filter list entries 255
filter list guidelines 253

First Use screen 26
getting a Mirapoint Support login ID 16
Group Calendar and Mail Routing license 133
integrating new words to a wordlist filter 256
LDAP provisioning and the setup wizard, all-in-one 51
LDAP provisioning and the setup wizard, multi-tier MMS 86
MailHurdle and SMTP authentication 285
mailing list exemptions, where placed 316
multi-tier MMS 112
multi-tier MMS deployment required information 80
pre-configuration checklist 21
RSR 388
selecting a delegated domain 185
setting service reporting 31
setting SSL version, cipher suite, or SMTPS 277
synchronized clocks 30
telnet default port 26
wire taps, empty 253
word lists 256
trusted IP addresses
setting 34
trusted network specifiers, about 35
types of viruses 289
typographic conventions 15

U

UCE
about junk mail scoring 240
definition 318
updates
antispam scanning 308
antivirus scanning, RAPID 301
antivirus scanning, Sophos and F-Secure 296
checking for 32
updating
antispam rule groups and MailHurdle known good mailers 309
antispam scanning, immediate 310
antispam/junk mail, automatically 310
antivirus scanning, immediate, RAPID 303
antivirus scanning, immediate, Sophos 298
antivirus, automatically, RAPID 302
antivirus, automatically, Sophos 297
RSR systems 391
Url Add
syntax for addressbook 60, 98
url add
syntax for group calendar, all-in-one 62
syntax for group calendar, multi-tier MMS 99
url delete 63
url delete command 100
URLs
for address book, all-in-one 60
for address book, multi-tier MMS 98
for group calendar, all-in-one 63
for group calendar, multi-tier MMS 100
User Audit Trail report 175
user directory service
all-in-one deployment 51
multi-tier MMS deployment 87
users
about 203
about the Quarantine Administrator 203
accessing folders in delegated domains 186
adding 206
changing folder access permissions 216
changing the default limit for delegated domains 192
default folder location 203
deleting 209
editing 208
finding 208
folder access permissions, meanings 212
number limits on RazorGates 205
provisioning accounts 209
reserved login names 205
setting limits in delegated domains 187
working with folders 214
using
Administration Suite Wizard 25
patterns 230
security quarantine 325
wordlist filters 253
UTF encoded login names 205

V

verifying
address book URL, all-in-one 73
address book URL, multi-tier MMS 111
multi-tier MMS deployment 107

replica readiness 388
Veritas NetBackup, supported versions 373
viewing
array data 170
disk data 169
group data and alerts 332
mail traffic 142
message envelopes and headers 162
messages, what you can view 165
sorted messages, in the queue 161
storage data 167
store data 172
system activity 138
system health data 173
the queue summary 159
virus deleted messages, filtering out 321
Virus Scanning Summary report 362
viruses, types of 289

W

WebCal
main configuration for delegated domains 195
resources configuration for delegated domains 197
search configuration for delegated domains 196
setting defaults for in delegated domains 192
subscribed calendars for delegated domains 200
WebMail
configuring, all-in-one 65
configuring, multi-tier MMS 102
enabling 66
requiring cookies 66, 102
securing session IDs
multi-tier MMS 102
securing session IDs, all-in-one 66
setting the timeout, all-in-one 66
setting the timeout, multi-tier MMS 103
WebMail Activity graph
definitions 145
description 145
statistics breakdown 145
weekly reports, description 337
white list, about the Junkmail header 312
wire taps
creating 252
empty, troubleshooting 253
Wizard, accessing 26
Wizard, using 25
wordlists, *see* filter list