MIRAPOINT®

RazorGate Administrator's Guide

Release 4.3-GA
September 2011
Part Number 010-00861d

This manual supports Messaging Operating System (MOS) release 4.3.2-FCS and later MOS releases until replaced by a newer edition.

Contents

Preface ... 8
About the Mirapoint Documentation ... 8
Getting Technical Support ... 8
Typographic Conventions ... 9
Iconic Conventions ... 10

Chapter 1: Getting Started ... 11
Planning Your Deployment ... 11
Running the Setup Wizard ... 11
Completing Additional Administration Tasks ... 12
Using the Setup Wizard ... 13
Before You Begin ... 13
Changing Your Password ... 15
Setting the QuarantineAdmin User Account ... 15
Setting Network Identifiers and DNS Servers ... 15
Applying Licenses ... 16
Setting the System Time ... 16
Choosing a Routing Function ... 16
Setting DirectPath Destination Host ... 17
Setting Disk Write Cache ... 17
Setting Junk Mail Manager ... 18
Setting the Relay List ... 18
Setting Mail Domains ... 18
Choosing a Routing Method ... 19
Setting up LDAP User Queries ... 19
Setting up LDAP Mail Group Queries ... 20
Setting up Domain Mail Host Mapping ... 20
Setting up Junk Mail Manager Domain to Host Mapping ... 20
Setting up Antivirus and Antispam Scanning ... 21
Setting up Services ... 21
Setting up Proxies ... 21
Setting up Service Reporting ... 22
Viewing the Configuration Summary ... 22

Chapter 2: Managing System Settings ... 23
Configuring Network Settings ... 23
About Domains ... 24
Understanding Domain Sensitivity ... 24
Configuring Network Interface Settings ... 24
Setting the System Time ... 28

Managing Services ... 30
About Enabling/Disabling and Starting/Stopping Services ... 30
Managing the Administration Service ... 30
Managing the Calendar Service ... 33
Managing the Directory Service ... 34
Managing the HTTP Service ... 35
Managing the IMAP, NDMP, and POP Services ... 37
Managing the SMTP, SNMP, and WebMail ... 42
Managing User Accounts ... 54
About Users and Administrators ... 54
User Account Requirements ... 55
Adding Users ... 57
Finding Users ... 59
Editing Users ... 60
Deleting Users ... 60
Viewing Presence/Last Login Times ... 61
Bulk Provisioning Users ... 61
Managing Distribution Lists ... 62
About Distribution Lists ... 63
Creating and Deleting Distribution Lists ... 64
Adding Members to and Removing Members from a Distribution List ... 65
Finding Existing Users and Distribution Lists ... 67
Creating a Mail Signature ... 68
Choosing a Routing Method ... 69
Selecting a Routing Method ... 69
Configuring LDAP User Queries ... 77
Configuring LDAP Mail Group Queries ... 78
Configuring Domain to Mail Host Mapping ... 80
Changing Your Password ... 80
Using Utilities ... 81
Managing Licenses ... 81
Service Reporting and Updating the Appliance ... 83
Importing and Exporting Configuration Data ... 87
Halting and Rebooting the Appliance ... 88

Chapter 3: Managing Security Settings ... 90
Using Security Features ... 90
Network Security Layer ... 90
SMTP Layer Security ... 91
Inbound Message Handling Layer ... 92
Message Content Handling Layer ... 93
Outbound Message Handling Layer ... 94
Configuring Multi-Listeners ... 95
Configuring NIC Failover ... 95
Using Domain Keys Identified Mail Security ... 96
Managing Certificates ... 97
Viewing Installed Certificate Information ... 97

Downloading and Installing Certificates 98
Editing and Downloading a Certificate Signing Request 99
Viewing and Installing an Intermediate CA Certificate 100
Selecting the Certificate Interface 101
Recovering a Certificate 101
Managing SSL Connections 101
Specifying SSL Connections 102
Managing Trusted Admins 103
About Trusted Network Specifiers 103
Specifying a Trusted Admin List 104
Managing Antivirus Scanning 105
About Signature-based Antivirus 105
About Predictive-based Antivirus 106
How Antivirus Features Are Applied 106
About Cleanable vs. Non-cleanable Viruses 107
How Antivirus Quarantine Works 107
Managing Sophos Antivirus 108
Managing F-Secure Antivirus 114
Managing RAPID Antivirus 120
Managing Quarantine Messages 124
Managing Antispam Scanning 125
About Antispam Scanning 126
Updating Antispam 134
Managing Allowed Senders 136
Managing Blocked Senders 138
Managing Allowed Mailing Lists 141
Managing the Relay List 144
Managing the Reject List 145
Managing RBL Host Lists 146
Managing MailHurdle 148
Configuring MailHurdle 149
Setting Allowed Hosts 151
Setting Advanced MailHurdle Options 151
Managing Junk Mail Manager 155
What is a Junk Mail Domain? 156
Configuring Junk Mail Manager 157
Managing Junk Mail Domains 161
Enabling LDAP Provisioning for Junk Mail Manager 169
Bulk Creating Junk Mail User Accounts 169
Sending a Junk Mail Summary Message 171

Chapter 4: Managing Content Filters 172
Creating Content Policies 172
Top Email Content Concerns 172
Creating Advanced Content Filters 173
Content Filtering Options 173
Reordering a List of Filters 187

Using the Filter List ... 188
Using Patterns and Wildcard Characters ... 191
How Content Filtering Quarantine Works ... 192
Managing Wire Taps ... 193
Example Wire Tap Address Entries ... 194
Managing Blocked Addresses Filters ... 195
Example Blocked Address List Entries ... 197
Managing Blocked Messages Filters ... 197
Example Blocked Messages List Entry ... 199
Managing Blocked Attachments Filters ... 199
Example Blocked Attachments List Entries ... 201
Managing Redirected Attachments Filters ... 202
Managing Corporate Word List Filters ... 204
Managing Objectionable Word List Filters ... 206

Chapter 5: Monitoring the Appliance ... 209
Internal Distribution Lists for Monitoring ... 209
Monitoring System and Data Storage Status ... 211
Viewing Storage Information and Managing Arrays ... 211
Using Health Monitoring ... 216
Managing Alerts ... 219
Monitoring External Systems via SNMP ... 233
Obtaining SNMP OIDs ... 233
Viewing the Message Queue ... 234
About the Queue ... 234
Sorting the Message Queue ... 236
Viewing the Queue Summary ... 242
Searching the Message Queue ... 244
Using Appliance Logs, Reports, and Graphs ... 246
Viewing Performance Graphs ... 277

Chapter 6: Managing Class of Service ... 297
About Class of Service ... 297
Finding a Class of Service ... 298
Creating a Class of Service ... 298
Configuring a Class of Service ... 299
Deleting a Class of Service ... 302

Appendix A: Managing Branding and Localization ... 303
Process Overview ... 304
Determining a Brand Method ... 304
Publishing a Brand ... 305
Changing Brands ... 306
Managing the Dictionary ... 306
Dictionary File Types ... 306

Dictionary Naming Convention ... 307
Downloading a Dictionary ... 307
Publishing Custom or Additional Dictionaries ... 308
Selecting a Brand ... 310
Downloading a Brand ... 311
Deleting a Brand ... 312
Deleting a Named Brand ... 312
Restoring the Factory Default System Brand ... 313
Assigning a Brand ... 314
Customizing the Over-Quota Message ... 316
Branding and Localization Tasks and Tips ... 318
Preserving Your Brand - Appliance Upgrades and Patches ... 318
Application Entry Points ... 318
Localizing Address Book - WebMail vs. Calendar ... 319
Localization Guidelines ... 319
Installing a User Interface Localization ... 320
Localizing Junk Mail Manager Messages ... 320
Displaying Available Localizations on Login Pages ... 320

Index ... 321

Preface

Welcome to the *Mirapoint RazorGate Administrator's Guide*. This manual is designed to allow system administrators to administer Mirapoint messaging solutions. For information regarding deployment scenarios and the configuration tasks related to those scenarios, see the *Mirapoint Site Planning Guide* and *Mirapoint MOS Configuration Guide*.

In this manual, the term *router* refers to an email router, rather than a network packet router. Email routers are also known as *relays*.

This manual assumes that you are familiar with industry-standard networking concepts and terminology and have a general understanding of how Internet email messaging works.

This manual provides information on the following administrative tasks:

- Chapter 1: Getting Started on page 11
- Chapter 2: Managing System Settings on page 23
- Chapter 3: Managing Security Settings on page 90
- Chapter 4: Managing Content Filters on page 172
- Chapter 5: Monitoring the Appliance on page 209
- Chapter 6: Managing Class of Service on page 297
- Appendix A: Managing Branding and Localization on page 303

About the Mirapoint Documentation

Documentation for all Mirapoint products is available through the Information Library on the Mirapoint Support website:

https://support.mirapoint.com/

The Information Library provides the hardware and software documentation for all supported Mirapoint releases and appliances, and the Support Knowledge Base. The Support site is accessible to all customers with a valid Support Contract. If your company has a valid contract but you need a Support login ID, email support@mirapoint.com.

For a glossary of terms associated with Mirapoint products, see http://www.mirapoint.com/glossary/.

Getting Technical Support

If you experience problems with your appliance, contact the company from which you purchased your Mirapoint appliance.

If you purchased your appliance directly from Mirapoint, contact Mirapoint Technical Support by email, telephone, or via the Mirapoint Support website:

Email: support@mirapoint.com
(China) support@mirapoint.com.cn

Telephone:

- (USA) 1-877-MIRAPOINT (1-877-647-2764)
- (UK) +44 (or 0) 1628-535699
- (China) 400 707 1086
- (Australia) 1 800 633 784
- (Elsewhere) +1 408-720-3800

Website: https://support.mirapoint.com/

When contacting Technical Support, be prepared with the following information about your appliance:

Table 1 Appliance Information for Technical Support

Information	MOS CLI command (Message Server, RazorGate)	AOS UI Location (RazorSafe)
Software release	`Version`	In the **Status** tab, select **System Info**.
Host ID	`License Hostid`	In the **Status** tab, select **System Info**.
Serial number	`Model Get Serial`	In the **Status** tab, select **System Info**.
Hardware model	`Model Get Chassis`	In the **Status** tab, select **System Info**.

Typographic Conventions

The following table describes what the different fonts and typefaces indicate in the documentation.

Table 2 Typographic Conventions

Typeface	Use	Examples
Bold	User interface elements	From the **File** menu, select **Save As...**
Italic	Definitions, emphasis, or titles	A *folder* is a container that stores email messages. Specify *at least two* DNS servers. See the *Mirapoint Message Server Administrator's Guide*.
`Courier`	Screen display text, command names, text to type*	`Enter your IP Address:` Use the `License Hostid` command. At the prompt, type `Version`.
`Courier Italic`	Variables for which you substitute when you type	*`your_IP_address`*
*Command-line interface (CLI) commands are case-*insensitive, except where noted. For readability, commands in this manual are shown in mixed case (for example, `License Hostid`).		

Iconic Conventions

The following table describes what the different icons in the documentation indicate.

Table 3 Iconic Conventions

Icon	Use
	Best practices information (Mirapoint recommendations)
	Note information that *should* be read
	Critical information
	License information
	Potential of causing bodily harm (hardware only)

Chapter 1: Getting Started

This chapter describes configuration-related first steps for properly administrating your appliance. These steps should be completed immediately *after* completing all of the necessary steps for setting up your hardware and using First Use Login administration pages. For more information about the First Use Login, see the *Mirapoint Hardware Getting Started Guide* for your appliance model and the First Use Login online help.

After initially setting up your hardware, make sure that you complete your software setup by:

- Planning Your Deployment below
- Running the Setup Wizard below
- Completing Additional Administration Tasks on next page

Planning Your Deployment

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 *Mirapoint Site Planning Guide* introduces Mirapoint's messaging architecture, describes several common deployment scenarios, and gives a detailed overview of Mirapoint's security and message server features. The *Mirapoint MOS Configuration Guide* describes the various configuration procedures that need to be performed for all Mirapoint appliances, Message Servers as well as RazorGates, for each deployment scenario.

Mirapoint recommends reading the *Mirapoint Site Planning Guide* prior to the *Mirapoint MOS Configuration Guide*.

Running the Setup Wizard

During your hardware setup, you should have completed the First Use Login procedure and the Setup Wizard. If you have not gone through the Setup Wizard, Mirapoint recommends doing so before performing any additional configurations:

- Before You Begin on the facing page
- Changing Your Password on page 15
- Setting the QuarantineAdmin User Account on page 15
- Setting Network Identifiers and DNS Servers on page 15
- Applying Licenses on page 16
- Setting the System Time on page 16
- Choosing a Routing Function on page 16
- Setting DirectPath Destination Host on page 17
- Setting Disk Write Cache on page 17
- Setting Junk Mail Manager on page 18
- Setting the Relay List on page 18
- Setting Mail Domains on page 18
- Choosing a Routing Method on page 19
- Setting up LDAP User Queries on page 19
- Setting up LDAP Mail Group Queries on page 20
- Setting up Domain Mail Host Mapping on page 20
- Setting up Junk Mail Manager Domain to Host Mapping on page 20
- Setting up Antivirus and Antispam Scanning on page 21
- Setting up Services on page 21
- Setting up Proxies on page 21
- Setting up Service Reporting on page 22
- Viewing the Configuration Summary on page 22

If you are enabling and configuring Junk Mail Manager (JMM) on your RazorGate appliance, make sure that you have enabled LDAP Provisioning for Junk Mail Manager on your Message Server. For more information, see the Message Server Online Help and the *Mirapoint MOS Configuration Guide*.

Completing Additional Administration Tasks

There are a number of additional features you can configure according to your site's requirements. Mirapoint recommends completing the following tasks:

- Schedule Software Updates—In addition to antivirus and antispam updates, you can schedule MOS update checks through the **Update Check** page (**Home > System > Utilities > Updates > Update Check**). For more information, see Using Update Check on page 86.
- Configure Class of Service (COS) Message Undelete and Message Expiration features—These COS features must be configured using the command-line interface (CLI). For more information, see the *Mirapoint Message Server Administrator's Guide* and *Mirapoint Administration Protocol Reference*.
- Set up the **daily-reports**, **weekly-reports**, and **system-alert** distribution lists (DLs)—These DLs are created during installation and Mirapoint uses these lists to send logs and reports to specified users on a scheduled basis. The **Administrator** user is added by default. You can add and remove members to these lists as needed. For more information about daily or weekly reports and system alerts, see Receiving Daily and Weekly Reports on page 247.
- Apply Your Brand—You can customize the appearance of Mirapoint's Junk Mail Manager user interface (`http://hostname/spam`) and other Mirapoint application user interfaces by changing the HTML style sheets and providing custom images. This gives you the ability to reflect your company's corporate identity. For more information about branding Mirapoint applications, see the *Mirapoint Branding Guide*.
- Set up System Backups—Mirapoint supports a number of different solutions for backing up and restoring user data. For more information, see the *Mirapoint Backup and Restore Guide*.
- Set up ConnectR for Outlook Users or MCM for Mac Users—If you have users who maintain their calendars in Microsoft Outlook or on a Mac, they can use ConnectR or MCM respectively to synchronize with WebCal. For more information about installing and using ConnectR or MCM, see the *Mirapoint ConnectR User's Guide* (http://www.connectrinfo.com) or the *Mirapoint Connector for Mac (MCM) User's Guide* (http://www.mcminfo.com).

Using the Setup Wizard

Use the **Setup Wizard** (**Home > System > Setup Wizard**) to network-configure and setup your appliance as an inbound, outbound, combined inbound/outbound, or DirectPath router, with or without LDAP. Use the **Previous**, **Next**, and **Close** links at top to navigate through the wizard. The configurations you make using the wizard can be changed at any time using its associated Administration Suite page(s).

The progression of the setup tasks in the wizard presumes a first time set up. The wizard pages provide these options, which display depending on appliance type and licensing.

Before You Begin

The **Setup Wizard** is designed to be an easy place to make all initial configuration settings. Most settings can also be made on the appropriate page under **Home > System**. Within the wizard, many data fields are filled in for you and there are likely pages that you can skip depending on what you want to configure.

Before you begin using the **Setup Wizard**, you should have the following information handy:

- Administration Username and Password - The login password that you want to use. Your system is pre-configured with the login name `administrator` and password `admin`. Make sure that you change these pre-configured credentials.
- IP Address - The Internet Protocol (IP) address that you want for this appliance, in dotted-quad notation as defined by the Internet Protocol in STD 5, RFC 791. Your system is pre-configured with 192.168.250.250 as the default IP address.
- Netmask - Network mask for computers on the same subnet as this appliance, in dotted-quad notation.
- Default Router - The IP address of the default router (gateway) for the subnet, in dotted-quad notation (such as 192.168.0.1). There is no pre-configured IP address for the default router.
- DNS Server - The IP address of a Domain Name System (DNS) server, in dotted-quad notation (such as 192.168.0.1). There is no pre-configured IP address for the DNS server.
- Host Name - The host name you assigned to the appliance (such as mail1), not including the domain name. There is no pre-configured host name.
- Domain Name - The organization name for your network and appliance (such as example.com) that you will configure in your DNS server. There is no pre-configured DNS domain name.

Hostnames and domain names are case-insensitive.

PC or UNIX workstation requirements:

- Administrator access to your PC/workstation.
- IP Address of your PC/workstation, in dotted-quad notation.

For an appliance, the important pages within the **Setup Wizard** are as follows:

- The first page of importance is the **License** page so you can make sure that all the licenses you need are installed.
- The next important page is the **Set Relay List** page, where you tell the appliance what machines should have mail relayed to them.
- If you are going to use JMM, use the Set Junk Mail Manager page, to enable it. Enabling JMM automatically sets up many required configurations and can take a few moments. For more information, see Configuring Junk Mail Manager on page 157.
- Use the **Choose Routing Method** page to tell the appliance whether to use the Local Routing Table, LDAP with Mirapoint schema, LDAP with Active Directory, or LDAP with non-Mirapoint schema. You will need to know, at least, your LDAP server and the Bind DN (distinguished name) credentials (if you use them). The following LDAP pages, **LDAP User Queries** and **LDAP Mail Group Queries** allow you to specify defaults by clicking the **Use Default Base DN**, but you will need to enter your Bind DN credential if it is needed to write to your LDAP server.
- The remaining pages allow you to enable and start key services like antivirus and antispam on the **Security** page, to specify proxies, set service reporting, and check your configuration summary.

Changing Your Password

The typical first task in setting up the appliance is to change the temporary administrator password to a more secure password. For more information, see Changing Your Password on page 80.

Setting the QuarantineAdmin User Account

The QuarantineAdmin user account is the default quarantine account, and you must create it using the **Set QuarantineAdmin User Account** page within the **Setup Wizard**, or on the **Add User** page (**Home > Users**). If you create the user on the **Set QuarantineAdmin User Account** page, the account is automatically granted the Quarantine Administrator role. If you create the account on the **Add User** page, be sure and grant the account the Quarantine Administrator role. You can grant any user the Quarantine Administrator role.

For more information, see About the Quarantine Administrator User, and How Content Filtering Quarantine Works. For information on accessing the Quarantine Administrator's WebMail, see Managing Quarantine Messages on page 124.

To set the QuarantineAdmin user account within the Setup Wizard:

1. Go to **Home > System > Setup Wizard**.
2. Click **Next** until you reach the **Setup Wizard: Set QuarantineAdmin User Account** page.

   The preset **User Name** is `QuarantineAdmin`.
3. (Optional) In the **Full Name** text field, type the name to be displayed in messages alongside the username.
4. In the **Password** text field, type a password for the QuarantineAdmin account.
5. In the **Confirm Password** text field, type the password again.
6. In the **Folder Quota** text field, type a quota (in kilobytes, KB) for the QuarantineAdmin account's system folder. You can completely remove a quota from a folder by typing `-1`.
7. Click **Next** until you reach the **Setup Wizard: Finish** page.
8. Click **Close**.

Setting Network Identifiers and DNS Servers

Use the **Setup Wizard: Set Network Identifiers** page to make changes or additions to the initial network parameters. You can add backup DNS servers and test connectivity to a DNS server.

To set network identifiers within the Setup Wizard:

1. Go to **Home > System > Setup Wizard**.
2. Click **Next** until you reach the **Setup Wizard: Set Network Identifiers** page.
3. In the **IP Address** text field, type the Internet Protocol (IP) address that you want for this appliance, in dotted-quad notation (such as 192.168.0.1).
4. In the **Netmask** text field, type the bitmask which shows how an Internet address is to be divided into network, subnet, and host parts.

5. In the **Host Name** text field, type the unique name by which a computer is known on a network. Do not include the domain name.
6. In the **Domain Name** text field, type the Internet name of the organization, such sales.com or sales.example.com. The domain name, when prefixed with the hostname, comprises a fully-qualified domain name (FQDN), such as `mail.example.com` or `smtp.sales.example.com`.
7. In the **Default Router** text field, type the IP address of the default router (gateway) for the subnet, in dotted-quad notation (such as 192.168.0.1).
8. Click **Set**.
9. Under **Set Domain Name Servers**, in the **DNS Server** text field, type the IP address that responds to Domain Name Service (DNS) queries.
10. Click **Add**. You can add additional DNS servers as needed.

    A table displays with the domain name. You can select a DNS Server checkbox and click **Remove** to remove a domain name from the table.

    Make sure you test both the domain name and IP address for each appliance and LDAP server you will integrate. For more information, see Configuring Network Interface Settings on page 24.
11. Click **Next** until you reach the **Setup Wizard: Finish** page.
12. Click **Close**.

Applying Licenses

Use the **Setup Wizard: License** page to retrieve and apply available licenses. This page displays all of the licenses currently applied to the appliance and can fetch additional licenses over the Internet. Your appliance must have Internet connectivity for this step. If not, you must have a printed license agreement so you can type the license keys manually. For more information, see Managing Licenses on page 81.

Setting the System Time

Use the **Setup Wizard: Set System Time** page to set the system clock, timezone, and NTP servers. This page allows you to configure the date and time of the system, or has the system automatically retrieve time from a specified NTP server on the network. For more information, see Setting the System Time on page 28. Using an NTP server requires the correct open ports (i.e., port 123), if you are using a firewall. For more information, see the *Mirapoint MOS Configuration Guide*.

Choosing a Routing Function

The **Setup Wizard: Choose Routing Function** page requires that you choose whether you are setting up a dedicated inbound router, dedicated outbound router, or a combined Inbound/outbound router. There are different options for each routing function.

On the **Setup Wizard: Choose Routing Function** page, select one of the following routing options:

- **Inbound message router** (IMR) - A host that sits between the Internet and your network, delivering email from the outside to message servers at your site. The inbound router must know where user folders are located, and may perform antivirus and antispam services. Inbound routers can be configured to perform regular DNS routing, or to work with a Directory Server using LDAP routing. They can be configured as a border router inside or outside the firewall.
- **Outbound message router** (OMR) - A host that routes messages composed at your site to addresses outside your organization. Also known as a relay host. The outbound router should have access to all-Internet DNS lookup, and may perform filtering or wiretap services. The outbound message router can be set on message servers to avoid direct connection with destination hosts. Outbound routers can be located inside or outside the firewall. Mail domains and relay lists on all systems should match those on the OMR.
- **Inbound/Outbound combination** - A host that will function as both an inbound and outbound router. Dedicated inbound and outbound message routers are useful for increased security, throughput, and load balancing. For instance, outbound routers can be placed outside a firewall for better DNS access, while inbound routers are placed inside a firewall for secure LDAP user lookup. Router hardware can be optimized for network bandwidth instead of storage. Inbound and/or outbound routers can be added to accommodate increased load. Optional antivirus and antispam software can be run on inbound routers, or dedicated security appliances, to avoid overloading the outbound router. The principal advantage of a combined router is low initial cost. Setup is no easier overall, but is all done on one system.
- **DirectPath message router** - A host that uses SMTP DirectPath mode that guarantees delivery without a queue; you must have a DirectPath license for this page to display. SMTP DirectPath filters messages at end-of-receipt to avoid message queuing overhead. It is recommended to improve reliability on systems without disk caching (for example, an RG 100 with disk write caching disabled) but it is less flexible than normal Fastpath. This routing function requires a DirectPath Destination Host (outbound and local router). The queue is still used for secondary messages generated by the filtering, antivirus, and antispam functions. With filtering at end-of-receipt, filtered addresses are before alias expansion: Distribution list (DL) names instead of DL recipient lists. If this is your selection, the next page in the wizard will be **Set DirectPath Destination Host**.

To set up Junk Mail Manager (JMM), you must choose either a dedicated **Inbound message router** or an **Inbound/Outbound combination**.

Setting DirectPath Destination Host

The **Setup Wizard: Set DirectPath Destination Host** page allows you to enable DirectPath, specify your outbound router, local router, and turn off the disk write cache. Caching is not needed for fast performance with the SMTP Fastpath option.

Setting Disk Write Cache

The **Setup Wizard: Set Disk Write Cache** page allows you to turn off the IDE disk write cache. This page does not display if you have a SCSI disk. By default the disk write cache is on, this setting provides the fastest performance and is industry-standard if you are using DirectPath as your routing function. If you are not using DirectPath for routing, turning off disk caching will cause performance to suffer.

If you change your disk write cache setting, you will be prompted to reboot. You can also modify this setting on the **Storage** page (**Monitoring > Storage**).

Setting Junk Mail Manager

The **Setup Wizard: Set Junk Mail Manager** page displays if you choose the dedicated **Inbound message router** or **Inbound/Outbound combination** option on the **Setup Wizard: Choose Routing Function** page. You cannot enable Junk Mail Manager (JMM) for dedicated outbound message routers.

JMM is a licensed junk mail management service that allows you to add junk mail user accounts to your router. The number of accounts you can add depends on your licensing.

If you are enabling JMM for the first time, use the Setup Wizard to enable the feature. Do *not* enable JMM on the **Junk Mail Manager Configuration** page (**Home > Junk Mail Manager > Configuration**) initially. If you do, there are complications that are noted in Troubleshooting Junk Mail Manager in Existing Setups on page 159.

After JMM is enabled, you can use the various JMM administration pages (**Home > Junk Mail Manager**) to set configuration defaults for the router, add Junk Mail Domains (one for each mail domain in your system), and add junk mail user accounts. For more information, see Managing Junk Mail Manager on page 155.

Setting the Relay List

The **Setup Wizard: 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.

To set the relay list within the Setup Wizard:

1. Go to **Home > System > Setup Wizard**.
2. Click **Next** until you reach the **Setup Wizard: Set Relay List** page.
3. In the text field, type an IP address or domain name.
4. Click **Add**.

A table displays with the domain name. You can select the checkbox for a domain name and click **Remove** to delete a name from the table. You can also modify this setting on the **Set Relay List** page (**Home > Antispam > Relay List**).

Setting Mail Domains

The **Setup Wizard: Set Mail Domains** page allows you to select the domains that are considered local for mail routing. Mirapoint refers to these domains as *mail domains* because they receive mail. Any DNS MX record you have created for a domain should be added to the list of local domains.

To set mail domains within the Setup Wizard:

1. Go to **Home > System > Setup Wizard**.

2. Click **Next** until you reach the **Setup Wizard: Set Mail Domains** page.
3. In the text field, type the DNS domain name, the part after the at sign (@), that should receive incoming mail.
4. Click **Add**.

A table displays with the domain name. You can select the checkbox and click **Remove** to delete a domain name from the table. You can also modify this setting on the **Mail Domains** page (**Home > System > Services > SMTP > Mail Domains**).

Choosing a Routing Method

If you have Mail Routing licensed, the **Setup Wizard: Choose Routing Method** page displays, otherwise, the **Setup Wizard: Route via Local Message Router** page displays.

To select a routing method:

1. Go to **Home > System > Setup Wizard**.
2. Click **Next** until you reach the **Setup Wizard: Choose Routing Method** page.
3. From the drop-down menu, select one of the following routing methods:
   - **Route via Local Message Router** - This method only displays if you do *not* have Mail Routing licensed or JMM enabled. This method directs the machine to refer all routing to the message router you specify.
   - **Route via Local Routing Table** - Deployments with only a few Message Servers and routers, and lacking access to an LDAP directory server, are the best candidates for the local routing table method.
   - **Route via LDAP Server with Mirapoint Schema** - This method requires you to use an LDAP database using the Mirapoint Schema. LDAP routing is the most flexible option, and offers the considerable advantage of a centralized database, but requires a directory server to be configured on your appliance.
   - **Route via Microsoft Active Directory** - This method requires you to use Microsoft Active Directory.
   - **Route via Other LDAP Server with Non-Mirapoint Schema** - This method is for configurations using an LDAP database, not Active Directory, and without the Mirapoint Schema.

After you have made your selection the page changes to display additional options. The options that display depend on your licensing, hardware, and configuration. For information on setting up LDAP and each routing method, see the *Mirapoint MOS Configuration Guide* and Choosing a Routing Method on page 69. You can also modify this setting using the **Choose Routing Method** page (**Home > System > Routing**).

Setting up LDAP User Queries

The **Setup Wizard: LDAP User Queries** page displays if you have chosen an LDAP-based routing method on the **Setup Wizard: Choose Routing Method** page. If you selected **Route via Local Routing Table** as your routing method, the **Security** page displays.

Click **Use Default Base DN** for a direct setup of your existing schema. If you had a previous, different LDAP routing configuration, those queries display until you click **Use Default Base DN**. For more information, see Configuring LDAP User Queries on page 77.

Setting up LDAP Mail Group Queries

The **Setup Wizard: LDAP Mail Group Queries** page appears after the **Setup Wizard: LDAP User Queries** page for LDAP-based routing.

Click **Use Default Base DN** for a direct setup of your existing schema. If you had a previous, different LDAP routing configuration, those queries display until you click **Use Default Base DN**. For more information, see Configuring LDAP Mail Group Queries on page 78.

Setting up Domain Mail Host Mapping

The **Setup Wizard: Domain Mail Host Mapping** page displays only if the **Route via Microsoft Active Directory** routing method is selected and you have Junk Mail Manager (JMM) disabled.

To set up domain mail host mapping:

1. Go to **Home > System > Setup Wizard**.
2. Click **Next** until you reach the **Setup Wizard: Domain Mail Host Mapping** page.
3. For every mail domain for which this appliance might route mail, specify the following options:
   - In the **Domain Name** text field, type the name of the mail domain.
   - In the **Mail Host** text field, type the name of the mail server or host for that domain.
4. Click **Next** until you reach the **Setup Wizard: Finish** page.
5. Click **Close**.

Setting up Junk Mail Manager Domain to Host Mapping

The **Setup Wizard: Junk Mail Manager Domain to Host Mapping** page displays only when Junk Mail Manager (JMM) is enabled and you have chosen one of the LDAP routing methods. Use this page to set up your Junk Mail Domains, mail domains whose junk mail you want JMM to quarantine. You can set up local or remote Junk Mail Domains, however, the remote domains must be created on the remote JMM host. The domains you add here, display on the **Junk Mail Manager Configuration** page (**Home > Junk Mail Manager > Configuration**).

If you selected the **Route via Local Routing Table** method, you must set up your Junk Mail Domains on the **Administer Local Junk Mail Domains** page (**Home > Junk Mail Manager > Junk Mail Domains**).

To configure Junk Mail Manager Domain to Host Mapping:

1. Go to **Home > System > Setup Wizard**.
2. Click **Next** until you reach the **Setup Wizard: Domain Mail Host Mapping** page.

3. In the **Junk Mail Manager Domain** text field, type the name of the mail domain for which a JMM is to handle junk mail. The name must match the mail domain name on your mail host.
4. In the **Junk Mail Host** text field, type the name of the JMM enabled router or host for that domain. If this is your only JMM appliance, you can use `localhost`.
5. (Optional) In the **Mail Host** text field, type the name of the mail server for that domain. The **Mail Host** option only displays if the **Route via Microsoft Active Directory** or the **Route via Other LDAP Server with Non-Mirapoint Schema** methods were selected. The Mirapoint schema, if configured properly, contains the LDAP mailhost attribute. For more information, see Junk Mail Manager LDAP Records on page 159.
6. Click **Add**.
7. Repeat steps 3 through 6 for every mail domain that a JMM host must handle junk mail for.
4. Click **Next** until you reach the **Setup Wizard: Finish** page.
5. Click **Close**.

Once you exit the Setup Wizard, you can modify these settings on the **Junk Mail Manager Configuration** page (**Home > Junk Mail Manager > Configuration**). For more information, see Configuring Junk Mail Manager on page 157.

Setting up Antivirus and Antispam Scanning

Use the **Setup Wizard: Security** page to enable or disable the antivirus and antispam scanning functions. If these services are not already enabled, you can enable them using the options on this page.

Antivirus and antispam scanning each require a license.

By enabling these services, all messages that are received by SMTP will be scanned for viruses and spam. You can modify these settings on the Configuration pages at **Home > Antivirus > *Scanner Name* (e.g., Sophos, F-Secure, RAPID) > Configuration** and **Home > Antispam > Configuration**, respectively.

Setting up Services

Use the **Setup Wizard: Services** page to enable and start the SMTP and SNMP services. Once enabled, you can modify these settings on the SMTP administration pages (**Home > System > Services > SMTP**) and SNMP administration pages (**Home > System > Services > SNMP**), respectively.

The SMTP service must be enabled for Junk Mail Manager (JMM) setups. However, if you are going to set additional SMTP options, such as LDAP routing, change those settings on the SMTP **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**) before starting the service.

Setting up Proxies

You must have Mail Routing licensed and Junk Mail Manager (JMM) must *not* be licensed, in order to see the **Setup Wizard: Proxies** page, otherwise, the **Setup Wizard: Service Reporting** page displays.

The **Setup Wizard: Proxies** page enables the appliance to proxy (i.e., pass through) user connections to the IMAP message service, POP email download, and HTTP services like WebMail and WebCal. If these services are not already enabled, you can enable them using the options on this page. Proxying is useful when users have IMAP, POP, or WebMail mailboxes on a separate Message Server.

You can also modify these settings on the **HTTP** (**Home > System > Services > HTTP**), **IMAP** (**Home > System > Services > IMAP**), and **POP** pages (**Home > System > Services > POP**), respectively.

Setting up Service Reporting

Use the **Setup Wizard: Service Reporting** page to configure service reporting to Mirapoint, specify a contact for Mirapoint (include names, email and/or postal addresses, and phone numbers as appropriate), and specify who in your organization should receive alert notifications.

The **Setup Wizard: Service Reporting** page enables the Mirapoint Customer Care or service reporting feature. Service reporting allows an appliance to report back anomalies and trend information to Mirapoint Technical Support, so that when problems do occur, Mirapoint can ship replacement parts in advance, and alert you of potential problems and known fixes.

By enabling the service reporting feature, you add critical information to Mirapoint's database of appliances in the field. This is how Mirapoint formulates current reliability figures and uptime data. Service reporting sends out only high-level summary information and system alerts. No actual email data is sent back to Mirapoint, so your confidential information is protected.

You can also modify this setting on the **Service Reporting** page (**Home > System > Utilities > Service Reporting**).

Viewing the Configuration Summary

Use the **Setup Wizard: Configuration Summary** page to view your entire configuration status on the last page of the Setup Wizard.

If necessary, click **Previous** near the upper right hand corner of the screen and return to earlier pages so you can adjust settings. When the settings are configured appropriately, click **Close** near the upper-right hand corner of the page. This will return you to the **About System** page in the Administration Suite.

Chapter 2: Managing System Settings

This chapter describes how to manage an appliance's system settings, including how to configure the network interface, set the system time, configure routing, and import/export configuration data. Information on how to use the Setup Wizard, various system utilities, and system services is also provided.

The system setting-related administration pages (**Home > System**) display depending on your appliance's licensing and configuration.

The following topics are included:

- Configuring Network Settings below
- Managing Services on page 30
- Choosing a Routing Method on page 69
- Managing User Accounts on page 54
- Managing Distribution Lists on page 62
- Creating a Mail Signature on page 68
- Changing Your Password on page 80
- Using Utilities on page 81
- Importing and Exporting Configuration Data on page 87
- Halting and Rebooting the Appliance on page 88

Although the Setup Wizard is initially run after the First Use Login setup, you can still access the Setup Wizard from the **Home > System** area at any time afterward. For more information about the Setup Wizard, see Using the Setup Wizard on page 13.

- Users - Provision and manage an appliance's user accounts, including assigning roles, setting account defaults, and assigning a class of service (COS).
- Distribution Lists - Provision and manage an appliance's distribution lists (DLs).
- Signature - Set an ASCII signature for all email traffic emanating from a specific domain.

Configuring Network Settings

Use the network-related administration pages (**Home > System > Network**) to make basic network configuration changes to the appliance as well as set the system clock.

The **About Network** page provides the following links:

- Interface - Set the appliance's IP address, netmask, hostname, domain name, and DNS servers.
- Time - Set the appliance's timezone and NTP servers.

Additional information about domains and network configuration is provided in the following sections:

- About Domains below
- Understanding Domain Sensitivity below

About Domains

A *domain* is an organization or entity on a host whose name (the domain name) is part of its Internet address. A fully-qualified domain name (FQDN) is the hostname plus the domain name. The last component of the domain name is the top-level domain. On the Internet, domains are represented by domain names such as `example.com` or `sfsu.edu`. Domains are mapped to IP addresses by DNS (Domain Name System) servers so that web browsers can find websites and Message Servers can deliver messages. A DNS domain is one that has been configured in a DNS database.

A Message Server must have a primary domain. Depending on your licensing, you can configure other domain types. The types of domains you can configure are as follows:

- Primary domain - The default system domain. This domain is specified on the **Set Interface** page (**Home > System > Network > Interface**).
- Relay domain - A DNS domain from/to which an appliance accepts messages for relay to other computers. This domain is specified on the **Set Relay List** page (**Home > Antispam > Relay List**).
- Mail domains - Additional DNS domains for which an appliance accepts messages. A mail domain acts as an alias for the primary domain. This domain type is specified on the **Mail Domains** page (**Home > System > Services > SMTP > Mail Domains**).
- Delegated domains - Fully administrable DNS domains that function like the primary domain. This domain type is specified on the **Administer Domains** page (**Home > Domains > Administration**).
- Blocked domains - DNS domains for which an appliance rejects messages. This domain type is useful for blocking known spam-generating sites. This domain type is specified on the **Reject List** page (**Home > Antispam > Reject List**).

You can change the domain naming structure on a appliance for both mail domains and delegated domains. Each are hostname aliases for sets of appliance users. A delegated domain is like a separate domain container, with its own named subset of users.

For each domain, DNS must have a mail exchange (MX) record referring to the appliance. For information about how to configure MX records, see your DNS server's product documentation .

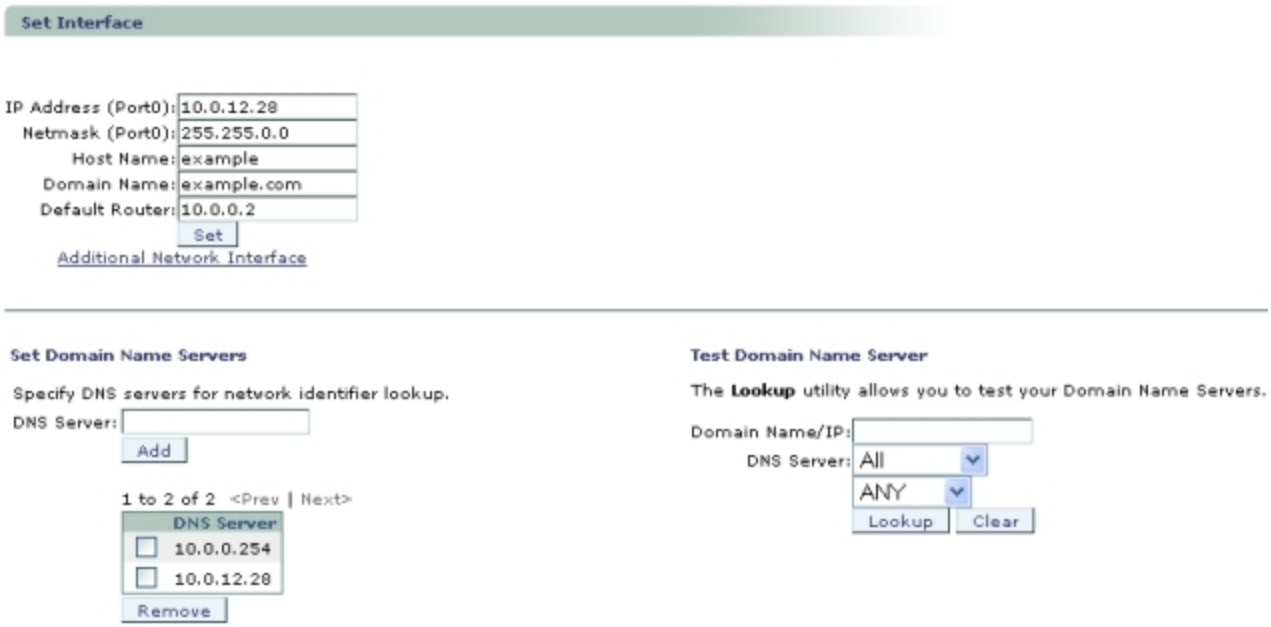
Understanding Domain Sensitivity

Some administration pages behave differently if a delegated domain is selected. In particular, tasks that affect user accounts, folders, and distribution lists (DLs) 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.

Configuring Network Interface Settings

Use the **Set Interface** page (**Home > System > Network > Interface**) to set the appliance's IP address, netmask, hostname, domain name, and Domain Name Servers (DNS).

Figure 4 Set Interface Page



Additional information about configuring network interface settings is provided in the following sections:

- Setting Your System Interface and Domain Name below
- Setting Additional Network Interfaces on next page
- Adding or Removing Domain Name Servers on page 27
- Testing Domain Name Servers on page 27

Setting Your System Interface and Domain Name

Changing your appliance's hostname disrupts email services unless you update your DNS server's name database and MX records to refer to the new name. Users are also required to change their email client configurations to refer to the new name.

To set the appliance interface and domain name:

1. Go to **Home > System > Network > Interface**.

   The **Set Interface** page appears.

2. Type in the appropriate information in the following text fields:

- **IP Address (port 0)** - The 32-bit host address defined by the Internet Protocol in STD 5, RFC 791; usually represented in dotted decimal notation. To configure the IP Address for another port, see Setting Additional Network Interfaces below.
- **Netmask (port 0)** - A 32-bit bitmask which shows how an Internet address is to be divided into network, subnet and host parts; usually in dotted quad notation. Plus signs (+) are not allowed in the netmask value. To configure the netmask for another port, see Setting Additional Network Interfaces below.
- **Host Name** - The unique name by which a computer is known on a network.
- **Domain Name** - The domain portion of the FQDN (fully-qualified domain name).
- **Default Router** - The IP address of the default router (gateway) for the subnet, in dotted-quad notation (such as 192.168.0.1).

3. Click **Set**.

The appliance uses the specified hostname and domain name, and a message displays. A confirmation page might display if the changes you want to apply will disrupt services.

Setting Additional Network Interfaces

If your appliance has more than one port, the **Additional Network Interface** link displays on the **Set Interface** page, allowing you to make changes to the IP address or netmask for each port.

To edit additional network interface information:

1. Go to **Home > System > Network > Interface**.

   The **Set Interface** page appears.

2. Click **Additional Network Interface**.

   The **Additional Network Interfaces** page appears. The following information is displayed for each port:

   - **Port** - The TCP port number.
   - **IP Address** - The 32-bit host address defined by the Internet Protocol in STD 5, RFC 791, usually represented in dotted decimal notation.
   - **Mask** - A 32-bit bitmask which shows how an Internet address is to be divided into network, subnet and host parts; usually in dotted quad notation.
   - **MAC Address** - The hardware address of a device connected to a shared network medium.

3. Click the **Edit** icon () for a configured interface in order to make changes to the **IP Address** or **Netmask**.
4. Click **Set**.

Adding or Removing Domain Name Servers

A DNS server is a host that responds to Domain Name Service (DNS) queries. The system maintains a list of DNS servers to which it issues DNS queries. When making a DNS query, the system queries the DNS servers in the DNS Servers list in the order entered until it receives a response, or until all the servers have been queried. To change the list order, you must remove servers from the list and add them again in the order you want.

To add/remove DNS servers:

1. Go to **Home > System > Network > Interface**.

   The **Set Interface** page appears.

2. Under the **Set Domain Name Servers** area, in the **DNS Server** text field, type in the IP address of the DNS server.
3. Click **Add**.

   The DNS server is added to the **DNS Server** table. You can remove a server by selecting the checkbox next to the name of the server and clicking **Remove**.

Any SMTP transactions that are pending when you click **Add** or **Remove** are aborted and retried later. For this reason, it is best to add DNS servers only when email traffic is light.

Testing Domain Name Servers

You can test your DNS servers using the lookup function. You can also query your DNS servers for a specific record (i.e., A, PTR, CNAME, MX, etc.).

To test a DNS server:

1. Go to **Home > System > Network > Interface**.

   The **Set Interface** page appears.

2. Under the **Test Domain Name Server** area, in the **Domain Name/IP** text field, type in a domain name or IP address.

   Or,

   From the **DNS Server** drop-down menu, select an domain name or IP address.

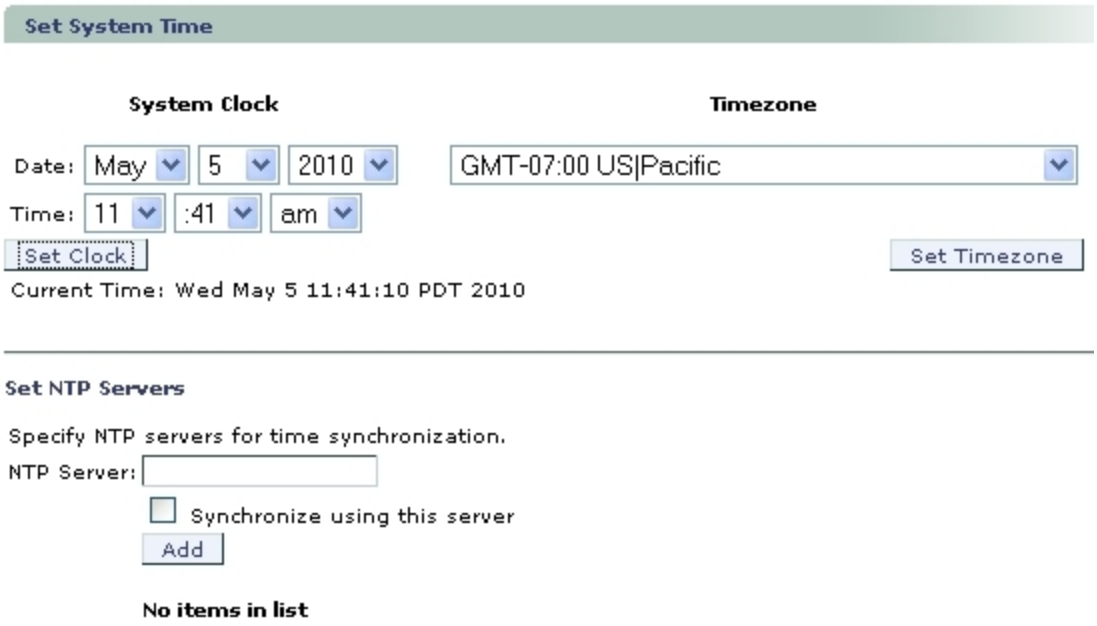
3. (Optional) If a particular record (e.g., A, PTR, MX, etc.) is desired, select a record from the drop-down menu. The default is **ANY**.
4. Click **Lookup**.

The lookup results display below the **Lookup** button. If there is an error, a **Test DNS Server** status message displays at the top of the page.

Setting the System Time

Use the **Set System Time** page (**Home > System > Network > Time**) to set your timezone, and add or remove Network Time Protocol (NTP) Servers.

Figure 5 Set System Time Page



Additional information about setting the system time is provided in the following sections:

- Configuring the System Time Settings below
- Adding and Removing an NTP Server on the facing page
- Synchronizing the System Clock with an NTP Server on the facing page

Configuring the System Time Settings

Use the **Set System Time** page to view the current date, time and timezone of the appliance and modify them.

To set the system clock and timezone:

1. Go to **Home > System > Network > Time**.

   The **Set System Time** page appears.

2. Under the **Set System Clock** area, use the drop-down menus to specify a date and time. By default, the current set time is shown.
3. Click **Set Clock**.
4. From the **Timezone** drop-down menu, select your timezone.

The timezone defaults to GMT, not your local timezone.

5. Click **Set Timezone**.

Adding and Removing an NTP Server

Your appliance uses the Network Time Protocol (NTP) to keep its clock synchronized with one or more NTP servers.

To add an NTP server:

1. Go to **Home > System > Network > Time**.

   The **Set System Time** page appears.

2. Under the **Set NTP Servers** area, in the **NTP Server** text field, type the fully-qualified host name (including DNS domain) of the NTP server you want to add.
3. Click **Add**.

To remove an NTP server:

1. Go to **Home > System > Network > Time**.

   The **Set System Time** page appears.

2. Under the **Set NTP Servers** area, select the name of the server you want to remove in the list.
3. Click **Remove**.

Synchronizing the System Clock with an NTP Server

You only need to explicitly synchronize the appliance's system clock with an NTP server when you first set up the appliance. Once the system clock is set within one hour of the time indicated by an NTP server, it automatically keeps its clock synchronized with the NTP servers you have specified.

To synchronize the system clock with an NTP server:

1. Go to **Home > System > Network > Time**.

   The **Set System Time** page appears.

2. Under the **Set NTP Servers** area, select the name of the server that you want to synchronize the system clock with.
3. Click **Synchronize**.

Managing Services

Use the services-related pages (**Home > System > Services**) that allow you to enable/disable and configure various licensed appliance services.

The **About Services** page provides the following links:

- Administration - Configure Trusted IP Addresses, set connection security, and set the connection timeout default.
- Calendar - Enable, disable, start, or stop the Calendar (i.e., WebCal) service.
- Directory - Enable, disable, start, or stop the LDAP service.
- HTTP - Configure defaults, LDAP redirect, proxy settings, enable, disable, start, or stop the service.
- IMAP - Configure defaults and proxies; enable, disable, start, or stop the mail service.
- NDMP - Configure, enable, disable, start, or stop the backup service.
- POP - Configure defaults and proxies; enable, disable, start, or stop the mail service.
- SMTP - Configure defaults and mail domains; enable, disable, start, or stop the service.
- SNMP - Configure defaults, hosts, and traps; enable, disable, start, or stop the service.
- WebMail - Configure timeout; enable, disable, start, or stop the service and additional WebMail features.

About Enabling/Disabling and Starting/Stopping Services

Services must be **enabled** and **running** (i.e., started) to be available. A service that is **enabled** starts automatically when the appliance boots. If a service is **disabled**, then it is not available for use, will not start automatically when the appliance boots, and must be enabled before it can be started.

Managing the Administration Service

Use the **Administration** page (**Home > System > Services > Administration**) to configure Trusted IP Addresses, set security on connections, and set the interval (in minutes) for which the appliance retains a connection before timing out. This service is always enabled and always running.

To modify the Administration service:

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

   The **Main Configuration** page appears.

2. Under **Supported Connections (Administration Protocol, CLI and HTTP Administration)**, select one or more of the following options:

   Unless otherwise noted, security for administration connections to the administration protocol, the command-line interface (CLI), and HTTP connections to the Administration Suite is determined here. Security for all regular HTTP connections is set on the **Main Configuration** page for the HTTP service (**Home > System > Services > HTTP > Main Configuration**) page. You can also use the **Set SSL** page (**Home > Security > SSL**) to make these specifications. For more information, see SSL.

   - **Cleartext (incoming)** - Unencrypted incoming administration connections (port 10143) are supported. This is selected by default.
   - **Cleartext (outgoing)** - Outgoing administration connections (port 10143) are not encrypted. This is selected by default,
   - **SSL (incoming - Administration Protocol and HTTP only)** - Encrypted incoming administration connections (port 10243) or the administration protocol and HTTP to the Administration Suite are supported.
   - **SSL (outgoing - Administration Protocol and HTTP only)** - Outgoing administration connections (port 10243) for the administration protocol and HTTP to the Administration Suite are encrypted.
   - **SSH (CLI only)** - Enables the use of SSH (Secure Shell) keys for administration connections to the CLI. You must have an SSH license and client.

3. In the **Timeout** text field, type the number of minutes the system will wait before a connection times out. The default is 10 minutes.
4. Click **Modify**.

Administration protocol connections with SSL prompt you to accept a certificate before completing the connection. CLI connections with SSH prompt you to accept a host key. HTTP connections with SSL display a **Cleartext/Secure** link. When the **Secure** link is clicked, the connection uses SSL.

Adding and Removing Trusted Admins

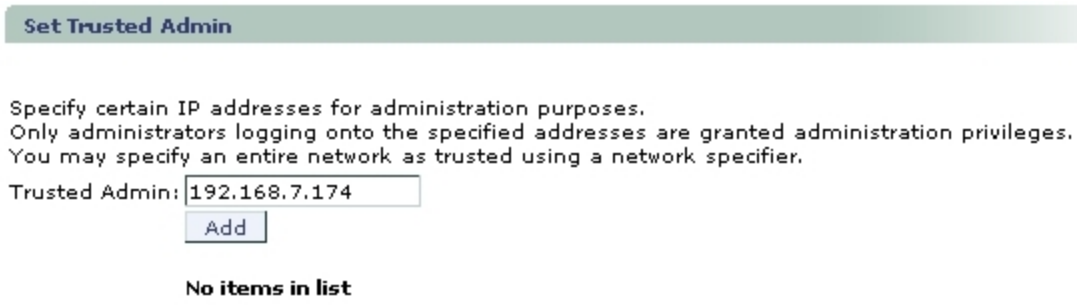
For security, you can specify certain trusted IP addresses, *Trusted Admins*, so only users logging into the administration service from these addresses are granted administration privileges. Once a Trusted Admin IP address is specified, if you connect from a non-trusted IP address, the administration pages do not work. For example, if you specified a single address as your only trusted IP address, someone logging in as Administrator from any other address would not be granted administrator privileges, despite the login name and correct password.

If you do not specify any trusted IP addresses, administration access is allowed from any host. For more information on Trusted Admins, see Managing Trusted Admins on page 103.

To add a Trusted Admin:

1. Go to **Home > System > Services > Administration > Trusted Admin**.

   The **Set Trusted Admin** page.



The Trusted Admin specifications you make on this page are instantiated on the **Set Trusted Admin** page under **Home > Security > Trusted Admin** and vice versa.

2. In the **Trusted Admin** text field, type the IP address of the network to which you want to restrict administration activity. You can use a network specifier as well. For more information, see About Trusted Network Specifiers on page 103).
3. Click **Add**.

The Trusted Admin list is updated with the new network and administration activity can only take place on that network. If you have not already added your client, you are prompted to do so before any other can be specified; this prevents accidental lock-out.

To remove a Trusted Admin:

1. Go to **Home > System > Services > Administration > Trusted Admin**.

   The **Set Trusted Admin** page.

2. Select the appropriate checkbox(es).
3. Click **Remove**.

   A confirmation page appears.

4. Click **Remove**.

Managing the Calendar Service

WebCal is a web-based application where users can schedule personal appointments and get notified as they occur. WebCal Direct allows you to license two calendar types: Personal and Group Calendar (i.e., GroupCal). Group Calendar is similar to Personal, but with a superset of functionality to schedule and notify workgroups. Also, calendar groups require the presence of an LDAP database (internal or external). For more information on Group Calendar and its functionality, see the *Mirapoint MOS Configuration Guide*.

If you have the proper licenses, you can enable Personal and/or Group Calendar for different classes of service (COS). For more information about setting up COS, see Managing Class of Service on page 297.

Use the **Calendar** page (**Home > System > Services > Calendar**) to enable, disable, start, or stop the Calendar service (i.e., for Personal or Group Calendar). On RazorGate appliances, the Calendar service is typically disabled.

The **Calendar** page only displays if WebCal is licensed. WebCal Direct Personal and Group Calendar, and COS, are licensed features. However, if you have licensed WebCal Corporate Edition, Group Calendar is included by default.

To modify the Calendar service:

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

   The **Calendar** page appears.

2. Click **Enable it/Disable it** to enable or disable the service. If the service is enabled click **Start it/Stop it** to start or stop the service. For more information, see About Enabling/Disabling and Starting/Stopping Services on page 30.
3. Set the **Schedule Mode**. How Calendar updates user calendars. Select one of the following modes from the drop-down menu:
   - **Server** - If this mode is selected, whenever a user creates an event or meeting and invites other users their calendars will immediately update to include the new event/meeting. Subsequent updates to the event/meeting are also reflected immediately in their calendars. This is the default setting.
   - **E-Mail** - If this mode is selected, whenever a user creates an event or meeting and invites other users their calendars will not immediately update to reflect the new event/meeting, each user will receive an email notification instead. The email notification includes action buttons (e.g., **Accept**, **Decline**, etc.) and a Calendar attachment (.ics file). An invited user's calendar will only update after the user reads the email and selects an action. If you have users using Microsoft Outlook with ConnectR or MCM, Mirapoint recommends selecting **E-Mail** mode.
4. In the **Timeout** text field, type how long Calendar can remain open without any action taken before losing its session ID. The default is 360 minutes.
5. In the **Remove events that are older than** text field, type how long user events can stay available in their Calendar. The default is 365 days.
6. Click **Modify**.

You can set many Calendar defaults on a domain basis using the domain-related Calendar pages under **Home > Domains > Calendar**. For more information, see Managing Calendar (WebCal) per Domain.

Managing the Directory Service

Use the **Directory** page (**Home > System > Services > Directory**) to enable, disable, start, or stop the LDAP service.

The **Directory** page only displays if Mirapoint Directory Server is licensed.

To modify the Directory service:

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

   The **Directory** page appears.
2. Click **Enable it/Disable it** to enable or disable the service. If the service is enabled click **Start it/Stop it** to start or stop the service. For more information, see About Enabling/Disabling and Starting/Stopping Services on page 30.

Managing the HTTP Service

Use the **HTTP** page (**Home > System > Services > HTTP**) and subsequent pages to set the default URL for the service and connection defaults, and to set up HTTP proxying. This service is always enabled and always running.

To modify the HTTP service:

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

   The **Main Configuration** page appears.

2. Set the following HTTP configuration defaults:

   - **http://*hostname* accesses** - From the drop-down menu, select a default application for when HTTP is accessed on that appliance. Your options depend on licensing but, in general, you can select one of the following applications:

     - **Administration Suite** - This is the default. If this option is not set as the default HTTP access, then the URL to access this UI is `http://hostname/miradmin`.
     - **Administration Suite (pre-3.4)** - If this option is not set as the default HTTP access, then the URL to access this UI is `http://hostname/acctadmin`.
     - **Calendar** (i.e., WebCal) - If this option is not set as the default HTTP access, then the URL to access this UI is `http://hostname/mc`.
     - **WebMail - Standard Edition** - If this option is not set as the default HTTP access, then the URL to access this UI is `http://hostname/wm`.
     - **WebMail - Corporate Edition v1** - If this option is not set as the default HTTP access, then the URL to access this UI is `http://hostname/em`.
     - **WebMail - Corporate Edition v2** - If this option is not set as the default HTTP access, then the URL to access this UI is `http://hostname/xm`.
     - **WebMail Portal** - If this option is not set as the default HTTP access, then the URL to access this UI is `http://hostname/pe`.

- **Cookies** - From the drop-down menu, select one of the following options:
  - **Disabled** - Cookies are not used.
  - **If supported** - Cookies can be used, if the connecting system supports them.
  - **Required** - Cookies are required; browsers must be set to accept cookies when using this method.
- **Supported Connections** - Select one or more of the following options:
  - **Cleartext (incoming)** - Non-encrypted incoming connections are supported. This is selected by default.
  - **Cleartext (outgoing)** - Outgoing connections are not encrypted. This is selected by default.
  - **SSL (incoming)** - Encrypted incoming connections are supported.
  - **SSL (outgoing)** - Outgoing connections are encrypted.

The HTTP supported connections selections you make on this page are instantiated on the **Set SSL** page under **Home > Security > SSL** and vice versa.

3. Click **Modify**.

Once your changes are instantiated, users will see the HTTP access that you selected when they browse to the specified URL.

Setting the LDAP Mode for the HTTP Service

The **Mode** page (**Home > System > Services > HTTP > Mode**) controls how the HTTP service employs LDAP proxy. Normally there is neither redirection nor proxying.

To set the LDAP mode for HTTP:

1. Go to **Home > System > Services > HTTP > Mode**.

   The **Mode** page appears.

2. Select one of the following modes. Your selection depends upon the appliance's configuration and licensing:

- **Normal** - The server does not perform HTTP redirection. This is selected by default.
- **LDAP Redirect** - Applications that support HTTP redirection use LDAP data to perform browser redirects (forwards). Such connections can be redirected only once.
- **LDAP Proxy** - The HTTP service acts as a proxy for applications that support HTTP redirection. This is useful for accessing a server behind a firewall. In this mode the system takes incoming HTTP connections and uses LDAP to find the destination appliance, then routes traffic between users' systems and their server.

Once the proxy is on, the IP address must be used to access the Administration Suite until next login.

3. (Optional) If you selected **LDAP Proxy**, you can modify the following settings:
   - **Max Header Size** - Maximum length of a request header line or URL. Max settings help prevent buffer overflow.
   - **Max Request Header Size** - Maximum size of the header portion of an HTTP request.
   - **Max Directory Traversals** - The maximum number of path components (`/../`) in a URL.
   - **Max Request Body Size** - Maximum size of the body portion of an HTTP request.
   - **Max Connections** - The number of simultaneous connections the proxy accepts before it starts refusing them.
   - **Proxy Timeout** - Maximum duration a connection can be idle before the proxy is allowed to close it.
   - **Destination Host** (This option displays if you do *not* have Mail Routing licensed) - Where all HTTP requests should be routed, if LDAP is not being used.
   - **Route URLs in LDAP** - Controls routing of unproxied URLs. The proxy uses domain-based routing to control which server provides information that the proxy cannot obtain from the session ID. Select one of the following options:
     - **On** - Enables LDAP routing for URLs without proxying information (images, login pages, and so forth).
     - **Off** (default) - Enables LDAP routing for unproxied URLs.
     - **Always** - Normal Mirapoint routing based on session IDs is not done. All back-end routing is done through LDAP. This improves performance if fronting a Microsoft Exchange Server.
4. Click **Modify**.

Managing the IMAP, NDMP, and POP Services

From the **About Services** page (**Home > System > Services**), if you have the proper licenses, you can configure the IMAP and POP mail services, as well as the NDMP backup service.

Additional information about the IMAP, POP, and NDMP services is provided in the following sections:

- Managing the IMAP Service on next page
- Managing the NDMP Service on page 39
- Managing the POP Service on page 40

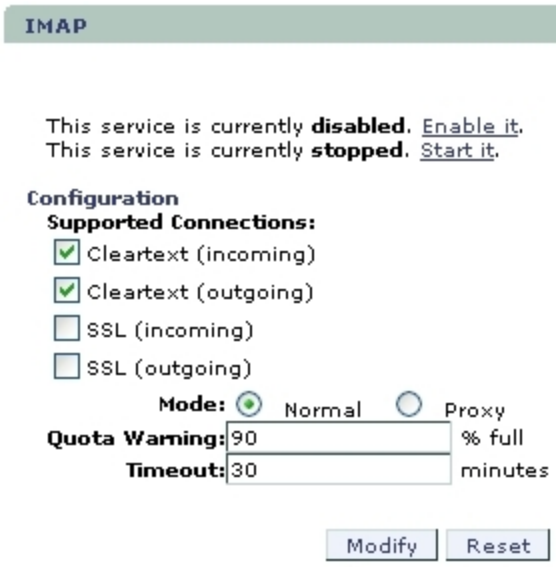
Managing the IMAP Service

Use the **IMAP** page (**Home > System > Services > IMAP**) to configure, enable, disable, start, or stop this mail service.

To modify the IMAP service:

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

   The **IMAP** page appears.



2. Click **Enable it/Disable it** to enable or disable the service. If the service is enabled click **Start it/Stop it** to start or stop the service. For more information, see About Enabling/Disabling and Starting/Stopping Services on page 30.
3. Under **Supported Connections**, select one or more of the following options:
   - **Cleartext (incoming)** - Non-encrypted incoming connections are supported. This is selected by default.
   - **Cleartext (outgoing)** - Outgoing connections are not encrypted. This is selected by default.
   - **SSL (incoming)** - Encrypted incoming connections are supported.
   - **SSL (outgoing)** - Outgoing connections are encrypted.
4. Select one of the following **Mode** options:
   - **Normal** - The IMAP service accepts IMAP connections providing access to folders on the local host only.
   - **Proxy** - The IMAP service acts as a proxy. For more information, see About IMAP Proxy Mode on the facing page.

5. In the **Quota Warning** text field, type the percentage (between 5 and 95) of a quota that must be exceeded on a folder before the IMAP service issues quota warnings to clients that have the folder open. For example, if this percentage is 95 and a particular folder has a quota of 100 MB, the IMAP service begins issuing quota warnings for the folder when its usage exceeds 95 MB.
6. In the **Timeout** text field, type the IMAP service idle timeout in minutes. The IMAP service closes any connection that remains idle for this period. To comply with the IMAP4 protocol (RFC 3501), you should set this value to 30 minutes or more.
7. Click **Modify**.

About IMAP Proxy Mode

In **Proxy** mode, the IMAP service acts as an IMAP proxy. When a user makes an IMAP connection to an IMAP proxy, the proxy uses an external LDAP database to determine the mail host where the user's email is stored. It then connects to the IMAP service on that mail host and passes IMAP commands and responses between the user's IMAP client and the IMAP service on the user's mail host for the duration of the user's IMAP connection.

For the IMAP proxy to work correctly, you must use the `Ldap Setquery` command-line interface (CLI) command to define the `User:Routingaddr` and `User:Mailhost` query specifications correctly for your LDAP database. For more information, type `Help About Ldap` in the CLI.

You can use the IMAP service in **Proxy** mode only if the LDAP Client Software license is installed on your appliance. Contact your Mirapoint Sales Representative for details.

Managing the NDMP Service

Use the **NDMP** page (**Home > System > Services > NDMP**) to configure, enable, disable, start, or stop this backup service.

To modify the NDMP service:

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

   The **NDMP** page appears.

2. Click **Enable it/Disable it** to enable or disable the service. If the service is enabled click **Start it/Stop it** to start or stop the service. For more information, see About Enabling/Disabling and Starting/Stopping Services on page 30.
3. From the **Data Management Application** (DMA) drop-down menu, select one of the following options:
   - **default** - A set of generic DMA settings. Defaults to version 3.
   - **Bakbone** - Defaults to version 4.
   - **Legato** - Defaults to version 3.
   - **Tivioli** - Defaults to version 4.
   - **Veritas** - Defaults to version 3.
4. In the **Preferred IP** text field, type the IP address the NDMP data service should use for 3-way backup or restore.
5. In the **Port** text field, type the TCP port number on which the NDMP service will listen for incoming connection requests. The default is 10000). Any value from 0 to 65535 is acceptable (no attempt to check for the supplied port being used by another service is made).
6. From the **Version** drop-down menu, select the maximum, also the default, NDMP protocol version used by the NDMP service. The new value takes affect on the next connection to the NDMP service. Possible values are 2, 3, or 4. The default depends on the **Data Management Application** selected.
7. Click **Modify**.

For more information on NDMP configuration settings, type `Help About Ndmp` in the CLI. For more information on backup and restore, see the *Mirapoint Backup and Restore Guide*.

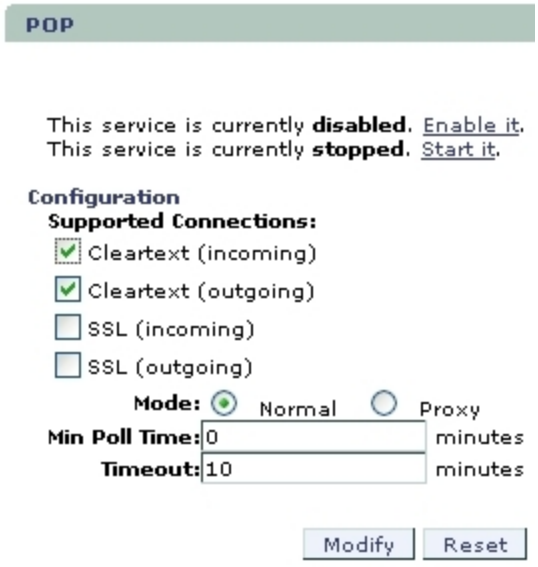
Managing the POP Service

Use the **POP** page (**Home > System > Services > POP**) to configure, enable, disable, start, or stop this mail service.

To modify the POP service:

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

   The **POP** page appears.



2. Click **Enable it/Disable it** to enable or disable the service. If the service is enabled click **Start it/Stop it** to start or stop the service. For more information, see About Enabling/Disabling and Starting/Stopping Services on page 30.
3. Under **Supported Connections**, select one or more of the following options:
   - **Cleartext (incoming)** - Non-encrypted incoming connections are supported. This is selected by default.
   - **Cleartext (outgoing)** - Outgoing connections are not encrypted. This is selected by default.
   - **SSL (incoming)** - Encrypted incoming connections are supported.
   - **SSL (outgoing)** - Outgoing connections are encrypted.
4. Select one of the following **Mode** options:
   - **Normal** - The POP service accepts POP connections providing access only to folders on the local host.
   - **Proxy** - The POP service acts as a proxy. For more information, see About POP Proxy Mode on next page.

5. In the **Min Poll Time** text field, type the time in minutes that must elapse between POP connections from a particular client. When a client closes a POP connection, this minimum interval must elapse before the POP service will give updated data to a new connection by that user. This allows you to prevent excessive polling from POP clients, which can degrade performance. A value of 0 (the default) disables this feature.
6. In the **Timeout** text field, type the POP service idle timeout in minutes. The POP service closes any connection that remains idle for this period. To comply with the POP3 standard (RFC 1939), you should set this value to 10 minutes or more.
7. Click **Modify**.

About POP Proxy Mode

In **Proxy** mode, the POP service acts as a POP proxy. When a user makes a POP connection to a POP proxy, the proxy uses an external LDAP database to determine the mail host where the user's email is stored. It then connects to the POP service on that mail host and passes POP commands and responses between the user's POP client and the POP service on the user's mail host for the duration of the user's POP connection.

For the POP proxy to work correctly, you must use the `Ldap Setquery` command to define the `User:Routingaddr` and `User:Mailhost` query specifications correctly for your LDAP database. For more information, type `Help About Ldap` in the CLI.

You can use the POP service in **Proxy** mode only if the LDAP Client Software license is installed on your appliance. Contact your Mirapoint Sales Representative for details.

Managing the SMTP, SNMP, and WebMail

From the **About Services** page (**Home > System > Services**), if you have the proper licenses, you can configure the SMTP mail delivery service, SNMP monitoring service, as well as the WebMail application services.

Additional information about the SMTP, SNMP, and WebMail services is provided in the following sections:

- Managing the SMTP Service below
- Managing the SNMP Service on page 49
- Managing the WebMail Service on page 52

Managing the SMTP Service

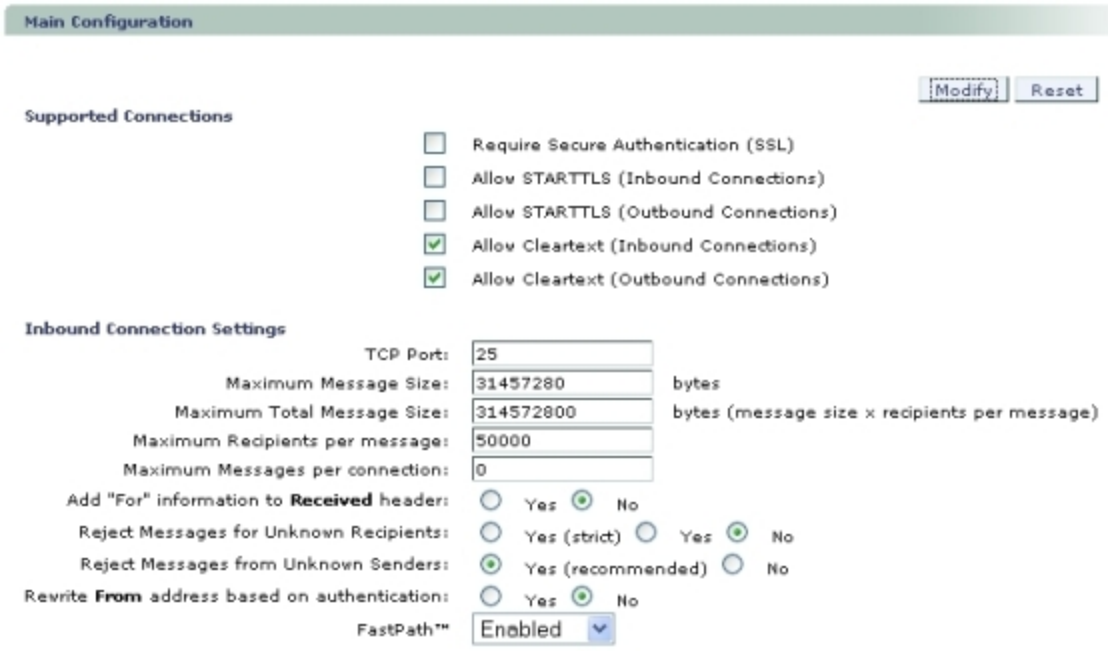
Use the **SMTP** page (**Home > System > Services > SMTP**) and subsequent pages to configure, enable, disable, start, or stop the mail delivery service. For more information, see About Enabling/Disabling and Starting/Stopping Services on page 30.

If you want to set the SSL version, cipher suite, or SMTPS, see the *Mirapoint Administration Protocol Reference*.

To modify the SMTP service:

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

   The **Main Configuration** page appears.



2. Under **Supported Connections**, select one or more of the following options:

   - **Require Secure Authentication (SSL)** - All communications must be authenticated through the AUTH login. For more information on SMTP AUTH, see RFC 2554.
   - **Allow STARTTLS (Inbound Connections)** - Encrypted incoming connections are supported.
   - **Allow STARTTLS (Outbound Connections)** - Outgoing connections are encrypted.
   - **Allow Cleartext (Inbound Connections)** - Unencrypted (i.e., cleartext) incoming connections are supported.
   - **Allow Cleartext (Outbound Connections)** - Outgoing connections are not encrypted (i.e., cleartext).

   Selecting **Allow Cleartext (Inbound Connections)** or **Allow Cleartext (Outbound Connections)** violates RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security). Make sure that you have read RFC 3207 and understand the implications of violating it before selecting these options.

3. Under **Inbound Connection Settings**, specify the following options (as needed):

- In the **TCP Port** text field, type the TCP port on which the SMTP service listens for incoming connections. Also known as the *Listen Port*.
- In the **Maximum Message Size** text field, type the maximum message size, in bytes, that the SMTP service accepts. The default is 31457280 bytes or 30 megabytes (MB). The service refuses messages larger than this value. 134217728 bytes (128 MB) is the maximum value you can enter. You can type `m` as the suffix for megabytes. For example, `128m` is accepted as 134217728 bytes.
- In the **Maximum Total Message Size** text field, type the maximum total size of the message in bytes (default is 314572800 bytes or 300 MB). This value is the product of the maximum message size times the maximum recipients per message. The service refuses messages larger than this value. This setting is independent of the **Maximum Message Size** setting. 1342177280 bytes (1280 MB) is the maximum value you can enter.
- In the **Maximum Recipients per message** text field, type the maximum number of recipients to whom the SMTP service will send a message. This setting refers to the number of recipients specified with SMTP, not the number of recipients after address expansion. The default value is 50,000 and cannot be set higher than that. If you change this setting, restart SMTP service for it to take effect.
- In the **Maximum Messages per connection** text field, type the maximum number of messages that can be transmitted in a single inbound SMTP session. The default is 0 (or unlimited). This can be set to any positive value up to and including 1000. After exceeding this limit, the connection is dropped and a 451 error results for the next recipient.
- For **Add "For" information to Received header** select **Yes** or **No**. The default is **No**. Whether or not to insert a `for` clause in the `Received` field of message headers. Setting this parameter to **Yes** tells the system to insert a line giving the intended recipient of each message; distinguishing between distribution list members.

  This has an impact on SMTP throughput and storage size, since a separate message for each recipient becomes necessary. A unique `for` header is generated for each unique envelope recipient, even if they are destined for the same user. The `for` header contains the original envelope recipient as received by SMTP, before any mail routing or mailgroup/DL expansion. Setting this parameter to **No** disables insertion of the `for` clause. The 4th line below shows an example of the `for` clause:

  ```
  Received: from omr.outside.com (omr.outside.com [10.0.0.1])
  by mail.example.com (Example Corp.)
  with ESMTP id AAA00001
  for juser@mail.example.com;
  Tue, 12 Dec 2000 11:43:49 -0800 (PST)
  ```

- For **Reject Messages for Unknown Recipients** select **Yes (strict)**, **Yes**, or **No**. This setting determines how to handle messages addressed to unknown local recipients. This setting uses one of the following options:

- **No** - All messages to unknown local recipients are allowed. The default is **No**.
- **Yes** - Message recipients are checked to see if they are routable to a local mailbox or, if LDAP routing is in use, via LDAP entry. Recipients that are not found locally or in LDAP (i.e., are not routable) are rejected; however, if your environment is configured to use a Local Message Router (LMR) (see SMTP - Routing Settings), messages are allowed for all recipients on all local domains.
- **Yes (strict)** - This option functions in the same manner as **Yes** but ignores the LMR setting. So, recipients must be routable to a local mailbox or via an LDAP entry in order to be allowed.

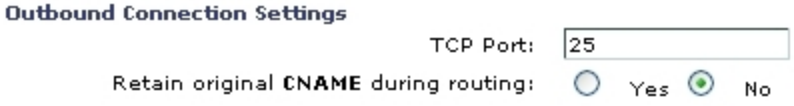
An address after `RCPT TO:` that is destined for a locally known domain, or where the domain portion of the address matches the current host, is considered a local address. Also, a recipient is also considered local if the address does not include a domain part (e.g., administrator).

When a message is rejected, a `User Unknown` error is returned to the sender if the SMTP service's **FastPath** setting is **Enabled**, and a `550 No such mailbox` if the setting is **Disabled**.

- For **Reject Messages from Unknown Senders** select **Yes** or **No**. The default is **Yes**. This setting determines whether the SMTP service performs sender validation by checking the identity given in the envelope `MAIL FROM` field. This can be set to **No** to accept mail from domains with mis-configured DNS. Blocking works with this option set to **No**. When set to **Yes**, if the sender's domain does not exist in DNS, or is in the blocked senders list, the SMTP service rejects the message.
- For **Rewrite From address based on authentication** select **Yes** or **No**. The default is **No**. This setting 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.
- From the **FastPath** drop-down menu, select one of the following options:
  - **Enabled** - Fastpath is used. This is selected by default.
  - **Disabled** - Sendmail is used.
  - **DirectPath** - DirectPath mode is used.

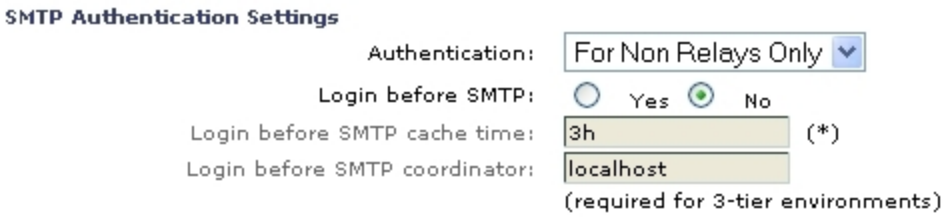
  Fastpath is the default mail transfer agent (MTA), replacing Sendmail. Fastpath attempts to minimize queuing by processing messages in-memory but resorts to fast queuing if necessary. DirectPath is a Fastpath mode that runs entirely in-memory. It does not support antispam, antivirus, autoprovisioning, autoreply, distribution list (DL) expansion, domain filtering, domain signature, forwarding, LDAP mailgroups, LDAP service interruptions, masquerade, more than 20 recipients, RBL header, or quarantine.

4. Under **Outbound Connection Settings**, specify the following options (as needed):



- In the **TCP Port** text field, type the TCP port on which the SMTP service establishes outgoing connections (default is 25). Also known as the *Connectport*.
- For **Retain original CNAME during routing** select **Yes** or **No**. The default is **No**. When set to **Yes**, the appliance retains the original CNAME during routing, rather than rewriting to the primary DNS A (Address) name.

5. Under **SMTP Authentication Settings**, you can specify whether SMTP authentication is offered (Mirapoint appliances always accept it). SMTP clients that use SMTP to authenticate themselves, giving their IMAP or POP login name and password, are then allowed to relay messages to other hosts. Specify the following options (as needed):

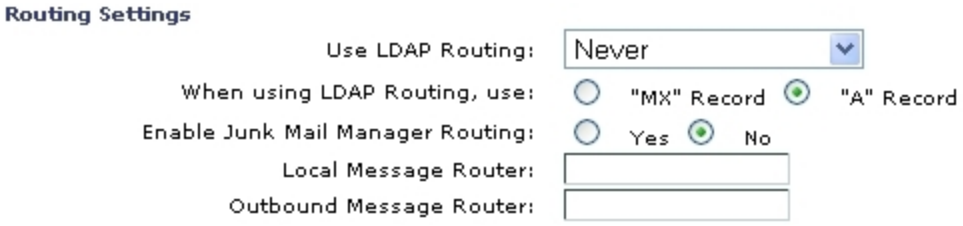


   - From the **Authentication** drop-down menu, select one of the following options:
     - **Disabled** - SMTP authentication is disabled.
     - **For Non Relays Only** - SMTP authentication is offered unless the IP address or host name of the connecting host is present in the relay list (see Relay List). Some mail clients require users always to authenticate themselves if the SMTP server supports authentication. By not offering authentication to relay hosts, this option allows users of those mail clients to connect from known hosts on the relay list without having to authenticate. This is selected by default.
     - **Off** - SMTP authentication is never offered.
     - **On** - SMTP authentication is always offered.
     - **Required** - SMTP authentication is always offered for all hosts, including those in the relay list. Moreover, authentication is required before acceptance of any `ESMTP` commands except `AUTH`, `EHLO`, `HELO`, `NOOP`, `RSET`, `STARTTLS`, and `QUIT`.
   - For **Login before SMTP** select **Yes** or **No**. The default is **No**. When this feature is set to Yes, and the Mirapoint appliance receives mail from a host that has logged into the POP or IMAP service recently, the host is allowed to send messages without further authentication. The value of `recently` can be changed with **Login before SMTP cache time** option. LDAP entries in multi-tier environments must contain fully-qualified host names.
   - In the **Login before SMTP cache time** text field, type the amount of time for which a Login before SMTP connection persists. The default is three hours (`3h`). The minimum time is one minute.
   - In the **Login before SMTP coordinator** text field, type the host that mediates Login before SMTP. The default is `localhost`.

6. Under **Mail Queue Settings**, specify the following options (as needed):

- In the **Warn about undelivered messages after** text field, type the period in hours that the SMTP service tries to deliver a message before sending a warning message to the sender indicating that the message has not yet been delivered. The default is 4 hours (4h).
- In the **Return messages that cannot be delivered in** text field, type the period in days that the SMTP service tries to deliver a message before sending a bounce message to the sender indicating that the message cannot be delivered. The default is 5 days (5d).
- In the **Maximum Delivery Status Notifications** text field, type the number of delivery status notification (DSN) messages that are sent to one sender in a domain. The default is 100 per day. When this limit is reached, a final DSN message is sent saying that no more status messages will be sent today. When this occurs, a count is kept of each sender, domain, recipient, and reason. The collected DSN information is sent out early the next day.

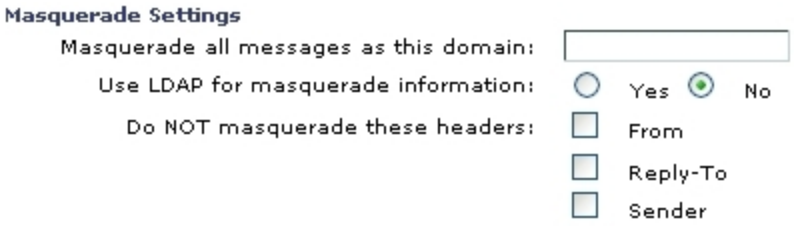
7. Under **Routing Settings**, specify the following options (as needed):



- From the **Use LDAP Routing** drop-down menu, select one of the following options:
  - **For All Messages** - Attempt LDAP routing for all messages, even those addressed non-locally. This reduces the number of domains you would need to create on the message router with the Local setting. It also permits antispam scanning of messages addressed non-locally.
  - **For Local Messages** - Route locally addressed messages (intended for mail domains and delegated domains) according to the LDAP values for `Mailhost` and `Routingaddr` (or equivalents).
  - **Never** - Routing is done by some other method than LDAP. This option is selected by default.
- For **When using LDAP Routing**, select one of the following options:
  - **"MX" Record** - The Mail Exchange (MX) record in DNS. MX records allow all mail for a domain to be routed to a host.
  - **"A" Record** - The Address (A) record in DNS. A records map the name of a machine to its numeric IP address. This option is selected by default.

- For **Enable Junk Mail Manager Routing** select **Yes** or **No**. The default is **No**. Routing is done based on LDAP routing using the `Smtp Set QuarantineJunk On` CLI command. So, all email is sent to the specified Junk Mail Manager (JMM) server, any messages that are not spam are then routed on to the mail server. For more information about the `Smtp Set QuarantineJunk` command, see the *Mirapoint Administration Protocol Reference*.
- In the **Local Message Router** (LMR) text field, type the host that can route messages for all hosts in your organization. Messages that appear local but are not deliverable on the local host are sent to the LMR for routing to the correct host. This is especially useful in multi-tier architectures involving multiple Mirapoint appliances, but is not compatible with domain-based routing.
- In the **Outbound Message Router** (OMR) text field, type the host where all outgoing mail must be relayed (sometimes known as the relay host). If you do not specify an OMR, the SMTP service connects directly to the hosts specified in the address of each message. It is best to configure your OMR with the same Mail Domains and Relay List as your other appliances.

8. Under **Masquerade Settings**, specify the following options (as needed):



- In the **Masquerade all messages as this domain** text field, type a DNS domain name that you want used in the **From** field for all outgoing messages, regardless of the actual originating host name. In conjunction with a relay host, the masquerade can also append a domain name to unqualified addresses (those not containing an at sign (@)). If local delivery is attempted for a message recipient but delivery fails, the domain portion of that address, everything following the at sign (@), is replaced by the masquerade domain. The message is then forwarded to the relay host.
- For **Use LDAP for masquerade information** select **Yes** or **No**. The default is **No**. Your masquerade information has been entered into your LDAP database.
- For **Do NOT masquerade these headers**, select one or more of the following options (as needed):
  - **From** - Prevents masquerade of **From** and **Resent-From** fields.
  - **Reply-To** - Stops masquerade of **Reply-To** and **Resent-Reply-To** fields.
  - **Sender** - Prevents masquerade of **Sender** and **Resent-Sender** fields.

9. Click **Modify**.

If the SMTP server supports AUTH, Netscape Messenger enforces its use. Consequently, users of Netscape Messenger must change their Outgoing mail server user name to be the same as their login name. Outlook Express allows people to use SMTP authentication if they want, but AUTH is not enforced by default. For more information about SMTP authentication, see RFC 2554.

Adding and Removing Mail Domains

A *mail domain* is a DNS domain for which a Mirapoint appliance accepts mail for local delivery to the primary domain or routing within the primary domain. For each mail domain, your DNS database must have an MX record referring to the Mirapoint appliance.

Domains that are designated as local are considered inbound, while all others are considered outbound domains.

Any DNS MX record you have created for a domain should be added to the list of local domains. For example, if you created a domain called `testdomain.com` and have it pointing to the appliance with an A record of `mirapoint.testdomain.com`, add `testdomain.com` to the list of local mail domains. The appliance allows you to add as many local mail domains as you need for routing of email.

To add a mail domain:

1. Go to **Home > System > Services > SMTP > Mail Domains**.

   The **Mail Domains** page appears.

2. In the **Mail Domain** text field, type the DNS domain name, the part after the at sign (@), that should receive incoming mail.
3. Click **Add**.

To remove a mail domain:

1. Go to **Home > System > Services > SMTP > Mail Domains**.

   The **Mail Domains** page appears.

2. Select the domain name you want to delete from the list.
3. Click **Remove**.

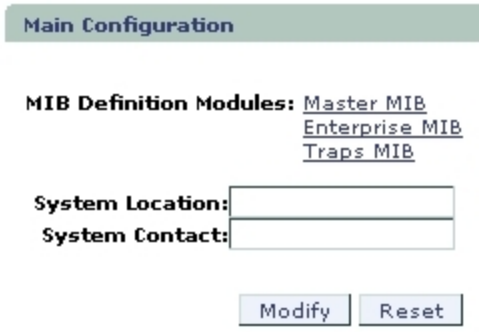
Managing the SNMP Service

Use the **SNMP** page (**Home > System > Services > SNMP**) and subsequent pages to configure, enable, disable, start, or stop this monitoring service. For more information, see About Enabling/Disabling and Starting/Stopping Services on page 30.

To configure the SNMP service:

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

   The **Main Configuration** page appears.



2. Access MIB definition files by clicking one of the MIB Definition Module links:
   - **Master MIB** - The MIB definition file for every MIB object supported by the appliance.
   - **Enterprise MIB** - The MIB definition file for proprietary MIB objects supported by the appliance, a subset of the Master MIB.
   - **Traps MIB** - The MIB definition file for trap MIB objects supported by the appliance, a subset of the Master MIB.

   When you click a link, a text file opens that you can load on to your appliance and use. SNMP MIBs are periodically updated. If you use SNMP to monitor your appliance, Mirapoint recommends downloading the MIB files from the appliance 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`.
3. In the **System Location** text field, type a text string describing to users of SNMP clients where your system is physically located.
4. In the **System Contact** text field, type the name, email address, or phone number of the person that users of SNMP clients can contact.
5. Click **Modify**.

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 configuration options on the **Hosts** page (**Home > System > Services > SNMP > Hosts**). If you do not explicitly define any access profiles, the SNMP service allows the public SNMP community read access to the entire MIB-II tree.

To add SNMP Hosts:

1. Go to **Home > System > Services > SNMP > Hosts**.

   The **Hosts** page appears.

2. Click **Add Host**.

   The **Add Hosts** page appears.

3. In the **Access Host** text field, type the fully-qualified domain name (FQDN) of the host to which you want to grant access to query SNMP on the system.
4. In the **Read Community** text field, type the community string that SNMP clients must specify to be allowed to query the system; space characters are not allowed.
5. Click **Ok**.

After a host is added, on the **Hosts** page you can edit the host's information by clicking the **Edit** icon (✎). To remove a host, click the **Delete** icon (✕).

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 appliance sends all SNMP Traps to all hosts in the Trap list. The same events that generate email alerts also generate Traps.

To add SNMP Traps:

1. Go to **Home > System > Services > SNMP > Traps**.

   The **Traps** page appears.

2. Click **Add Trap**.

   The **Add Traps** page appears.

3. In the **Destination Host** text field, type the fully-qualified domain name (FQDN) of the host to which SNMP traps should be sent.
4. In the **Traps Community** text field, type the community string for the Traps hosts list; space characters are not allowed.
5. Click **Ok**.

After a host is added, on the **Traps** page you can edit a trap's information by clicking the **Edit** icon (). To remove a trap, click the **Delete** icon ().

Managing the WebMail Service

Use the **WebMail** page (**Home > System > Services > WebMail**) to configure, enable, disable, start, or stop this service and additional WebMail features.

The **WebMail** page only displays if WebMail Direct Standard Edition or Corporate Edition is licensed.

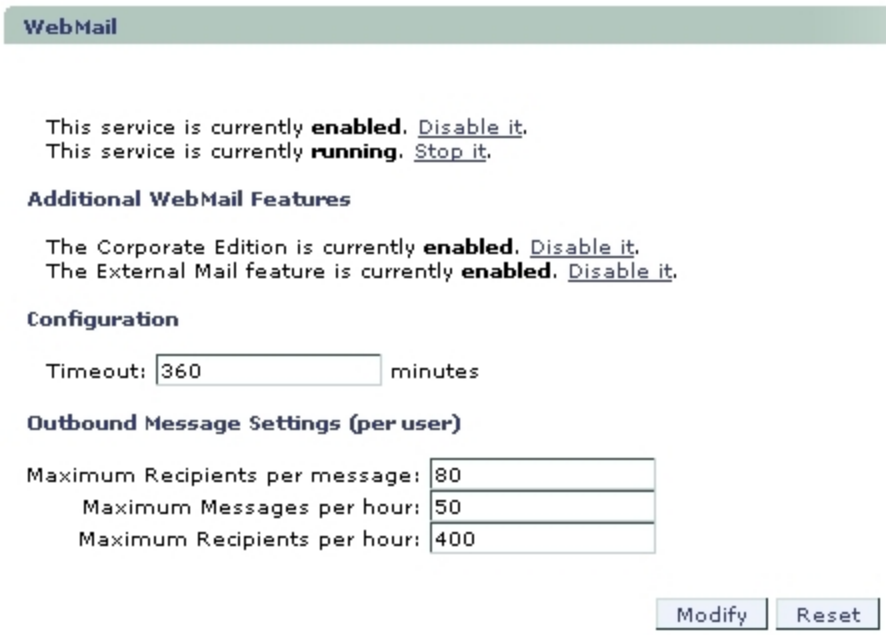
About Corporate Edition WebMail/WebCal

There is a client-like version of WebMail/WebCal called the Corporate Edition. This is a licensed feature that provides many ease-of-use features similar to a mail client. The access point is `http://hostname/em`. For more information, see the WebMail Corporate Edition online help.

To configure the WebMail service:

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

   The **WebMail** page appears.



2. Click **Enable it/Disable it** to enable or disable the service. If the service is enabled click **Start it/Stop it** to start or stop the service. For more information, see About Enabling/Disabling and Starting/Stopping Services on page 30.
3. Under **Additional WebMail Features**, use the **Enable it/Disable it** link to enable or disable **Corporate Edition** and the **External Mail feature**.
4. Under **Configuration**, in the **Timeout** text field, type the WebMail service idle timeout in minutes. The WebMail service automatically logs out any user whose connection remains idle for the specified number of minutes. The default is 360 minutes, and the minimum timeout is 3 minutes.
5. Under **Outbound Message Settings (per user)**, specify the following options:
   - In the **Maximum Recipients per message** text field, type the maximum number of recipients per sent email. The default is 80.
   - In the **Maximum Messages per hour** text field, type the maximum number of messages per hour that can be sent for a given user. The default is 50.
   - In the **Maximum Recipients per hour** text field, type the maximum number of recipients to which mail can be sent in an hour, for a given user. The default is 400.

   When a user tries to send a message that exceeds any of these limits, WebMail (Corporate and Standard Edition) displays the following error message in the **Compose** window, "`This account is over its mail-sent quota. Contact your administrator.`", and an alert is generated for the administrator. If alerts are generated, the administrator will only receive one alert per user every 30 minutes.
6. Click **Modify**.

To set WebMail (Standard Edition, Corporate Edition) as the default HTTP access for the appliance, see Managing the HTTP Service on page 35.

Managing User Accounts

This chapter describes how to provision and manage an appliance's user accounts, including how to assign roles, set account defaults, and assign a class of service (COS).

Use the **Add User** page (**Home > System > Users**) to modify user accounts, including the class of service (COS) for an account (if COS is enabled), or to add, find, rename, or delete a user.

The following topics are included:

- About Users and Administrators below
- User Account Requirements on the facing page
- Adding Users on page 57
- Finding Users on page 59
- Editing Users on page 60
- Deleting Users on page 60
- Viewing Presence/Last Login Times on page 61
- Bulk Provisioning Users on page 61

About Users and Administrators

A *user* is a person who has an account on the system; an administrator is a user with special privileges. An *account* consists of login name and password, and a main folder (i.e., Inbox). A user's 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 within the appliance folder named `user`. Additional information associated with each user account includes calendar data, WebMail settings, personal address book, personal dictionary, and forward and autoreply settings.

An *Administrator* is a user with special privileges. A default administrative user account with the **Administrator** role is configured during the initial set up the appliance, however, there are several types of administrative roles that you can assign to a user:

- A **Quarantine Administrator** can create content filters using the **Send to Quarantine folder** filter action, which allow the user to manage messages, attachments, addresses. For more information on the **Quarantine Administrator**, see About the Quarantine Administrator User on the facing page.
- 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.

When a non-administrative user (i.e, a user with no administrative role) logs in to the Administration Suite, they see only the **Account** pages. Non-administrative users can perform the following account management tasks on their own accounts using these pages or the WebMail **Options** 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

A **QuarantineAdmin** user account (with the specific username `QuarantineAdmin`) is the default quarantine administration account. You can create this account on the Setup Wizard's **Set QuarantineAdmin User Account** page or the **Add User** page. If you create the account using the Setup Wizard, it is automatically granted the **Quarantine Administrator** role.

If you use the **Add User** page to create a Quarantine Administrator account (for example, `user.QA.`*`folder`*), remember to manually grant the account the **Quarantine Administrator** role. If you want to create a Quarantine Administrator account for a delegated domain, select the domain first and then use that domain's **Add User** page.

Once you grant a user the **Quarantine Administrator** role, you can create content filters using the **Send to Quarantine folder** filter action, which allow the user to manage messages, attachments, addresses. For more information on the **Send to Quarantine folder** filter action, see How Antivirus Quarantine Works on page 107 and Creating Advanced Content Filters on page 173.

When a user with the **Quarantine Administrator** role logs into WebMail, they have an additional command button in their mail toolbar, **Deliver**. Quarantine Administrators use the **Deliver** option to release selected quarantined messages back into the mail queue. Users created in delegated domains, including Quarantine Administrator users, are restricted to the delegated domain in which they were created.

You can log in to the Quarantine Administrator's WebMail interface from the Administration Suite, by going to **Home > Quarantine**.

Only messages that received the **Send to Quarantine folder** filter action are eligible for the **Deliver** option. 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.

If RAPID Antivirus is licensed on your appliance, any Quarantine Administrator logging in to WebMail will also see a **Virus Scan** button. The **Virus Scan** option allows messages quarantined by RAPID Antivirus to be returned to the mail stream and scanned by one of the other antivirus engines. For more information, see How Antivirus Quarantine Works on page 107 and Managing RAPID Antivirus on page 120.

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.

Mirapoint appliances also support international login names. For example, in the username `soutien-clientèle`, the e-grave (è) would be encoded as `&AOg-: soutien-client&AOg-le`.

To support periods (.) in user folder addresses, you can create user names with underscores (_), for example `Firstname_Lastname`, and incoming mail for `Firstname.Lastname` is automatically 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` CLI 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 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 are allowed but are generally not used:

- & (ampersand)
- ' (single quote)
- * (asterisk)
- / (slash mark)
- = (equal sign)
- ? (question mark
- ^ (circumflex)
- { (open brace) and } (close brace)
- ~ (tilde)

Reserved Login Names

Login names are case-insensitive. You cannot create user accounts with the following reserved names:

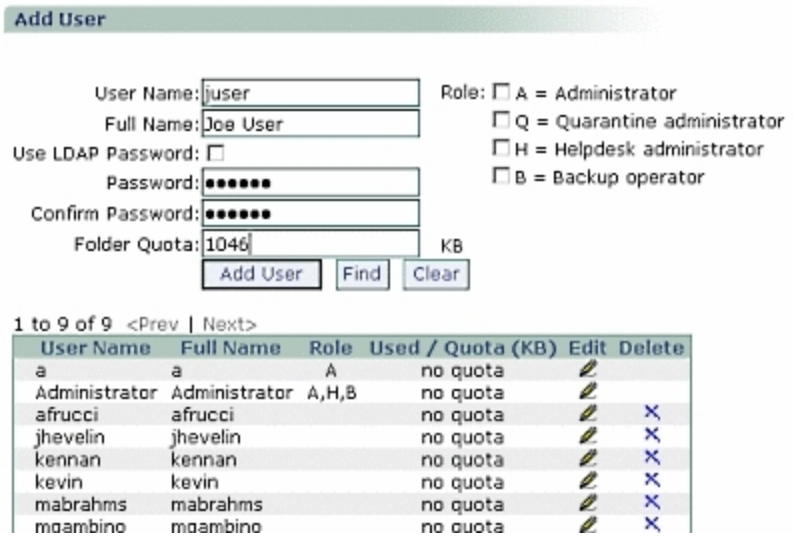
- administrator—Users with special privileges.
- administrators—An account for all administrators.
- anonymous—By convention, users accessing an appliance with this login name do not have to enter a password. Anonymous logins are not permitted.
- anybody—A wildcard name.
- anyone—A wildcard name.
- nobody—A user account with severely restricted privileges.
- user—A wildcard name.

Adding Users

Once you have added a new, or selected an existing, domain, use the **Add User** page to add, find, or modify users, including setting folder quotas, and assigning administrator privileges.

On a RazorGate, the number of users is limited to 20. This number can be increased by updating the license. Typically, 20 is usually sufficient, because only administrators need access to a RazorGate.

Figure 6 Add User Page



To add a user:

1. Go to **Home > System > Users**.

   The **Add Users** page appears.

2. In the **User Name** text field, type the name for the account. This name becomes the name of that user's folder under the appliance's `user` folder, the first part of their email address, and their login name.

3. For **Role**, by default, all of the options are deselected to create a regular user account. You can select one or more of the following checkboxes to create an administrative user account:

   If you designate a user as an administrator, also add the user to the `Service Reporting` distribution list (DL). For information about adding users to distribution lists, see Adding Members to and Removing Members from a Distribution List on page 65.

   - **A = Administrator** - This user has access to the full Administration Suite 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.
   - **Q = Quarantine administrator** - This user has special access to WebMail and can examine, release to the mail queue, reject (i.e., delete without notifying the addressee), or rescan (only available for RAPID-quarantined mail) messages that received the **Send to Quarantine folder** filter action. For more information, see About the Quarantine Administrator User on page 55.
   - **H = Helpdesk administrator** - This user has limited privileges within the Administration Suite's **Domains**-related pages. Also, the **Mail**, **Logins**, **Security**, and **Folders** logs for domains are available to them.

4. In the **Full Name** text field, type the user's firstname and lastname. The full name is displayed in messages alongside the username.
5. Select one of the following password options:
   - **Use LDAP Password** - Select this checkbox if your LDAP database is set up with passwords the appliance can access. If you select this checkbox, you will not be able to manually type in a password. However, if the LDAP GUI is enabled, the **Use LDAP Password** checkbox does not display, and whatever password is manually typed in is written to LDAP automatically.
   - **Password** - Type in the a password for the user in the text field. If you use this option, the password is not applied to your LDAP database. It is local to the appliance.
   - **Confirm Password** - Re-type the password.
6. In the **Folder Quota** text field, type a quota for that user's folder on the appliance in kilobytes (KB). All of their sub-folders are included in the total set quota. You can completely remove a quota from a folder by typing in a `-1`. For more information, see Changing a User's Folder Quota on next page.
7. In the **JMM Folder Quota** text field, type in how many spam messages (in kilobytes, KB) this Junk Mail Manager (JMM) user account can accept before being over-quota. This option only displays if you have selected JMM as a Class of Service (COS) for this user. For more information, see Managing Class of Service on page 297.
8. In the **Alias(es)** text field, type the fully-qualified domain name (FQDN) for the alias. Use this option to set up alias email addresses for your users. The alias's domain must exist in LDAP and mail addressed to the alias must be fully qualified. This option only displays if you have LDAP GUI enabled. For more information, see the *Mirapoint MOS Configuration Guide*.
9. From the **Class of Service** drop-down menu, select one of the configured COSs. This option only displays if you have enabled and configured COS.
10. Click **Add User**.

    The appliance grants the selected user the specified privileges and COS settings, and the username is displayed in the table.

    Instead of adding users one at a time using the **Add User** page, you can also enable bulk user provisioning by enabling LDAP autoprovisioning in the CLI and writing a script. For more information, see Bulk Provisioning Users on page 61.

Finding Users

To find a user:

1. Go to **Home > System > Users**.

   The **Add Users** page appears.
2. In the **User Name** text field, type in a name. You can also use wildcards in the search string. For more information on using search wildcards, see Using Patterns and Wildcard Characters on page 191.
3. Click **Find**.

Editing Users

You can edit a user account at any time in order to change a user password, folder quota, role, and so forth.

To edit a user:

1. Go to **Home > System > Users**.

   The **Add Users** page appears.

2. In the table, click the **Edit** icon (✎) for the user you want to modify. You might need to click **Prev** and **Next** to page through the list of names as needed, or type in a username and click **Find** to display only those users matching the specified name.

   The **Edit User** page appears with that user's data.

3. Click **OK**.

You can completely remove a quota from a folder by typing in a `-1`. For more information, see Changing a User's Folder Quota below.

The **Add Users** page displays a message confirming the modification.

Changing a User's 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 (megabytes), that Inbox folder, plus all its sub-folders, 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.

Deleting Users

To delete a user:

1. Go to **Home > System > Users**.

   The **Add Users** page appears.

2. In the table, click the **Delete** icon (✕) for the user your want to remove. You might need to click **Prev** and **Next** to page through the list of names as needed, or type in a username and click **Find** to display only those users matching the specified name.

   A confirmation page displays.

3. Click **Delete**.

A warning message, `Not in LDAP, deleting locally`, displays if the user you are deleting was added locally, not with the LDAP-enabled page.

Viewing Presence/Last Login Times

To view the activity of an end user, you can look at the **User Audit Trail** report. For more information, see Viewing the User Audit Trail Report on page 276. Another way to view the logins of a user is through the **Detailed Mail Logs** report. For more information, see Viewing Detailed Mail Logs on page 264.

Bulk Provisioning Users

Rather than adding users one at a time using the **Add User** page (**Home > System > Users**), you can enable LDAP autoprovisioning, write a script to convert your existing user database into LDAP, and import those user records into internal LDAP. For more information about LDAP autoprovisioning, see the *Mirapoint MOS Configuration Guide*.

To bulk provision users:

1. Access the command-line interface (CLI) by telneting to your appliance on the default telnet port (port 23) and logging in as the Administrator:

   ```
   OK hostname.domain.com admind 4.2 server ready
   User: Administrator
   Password: password
   OK User logged in
   ```

2. Use the following command to enable LDAP autoprovisioning:

   ```
   Ldap Set Autoprovision On
   ```

   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 values) data in Mirapoint AddressBook Format, you can run a Perl script to convert that data into LDAP Data Interchange Format (LDIF). The 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" ;
}
```

In this script, default passwords are created by spelling the user's name backwards and appending an `88`. You can change this line in the script to create a different password, if necessary. Furthermore, encourage all users to change their default passwords as soon as possible.

4. Once you have converted the data to LDIF using the Perl script, place it into an accessible file on an FTP or HTTP server.
5. Now import it to your LDAP server using the `Dir Importldif` command. The following 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
   ```

   Test the configuration by logging in as a newly created user. The user's Inbox, folders, and Junk Mail Filter should be present after a successful login.

Managing Distribution Lists

This chapter describes how to provision and manage an appliance's distribution lists (DLs). Information on reserved DL names and DL naming conventions is also provided.

A *distribution list* is a named list of email addresses specifying user accounts and their respective folders. When you send a message to a DL, the message is automatically sent to all the user addresses on the list.

The following topics are included:

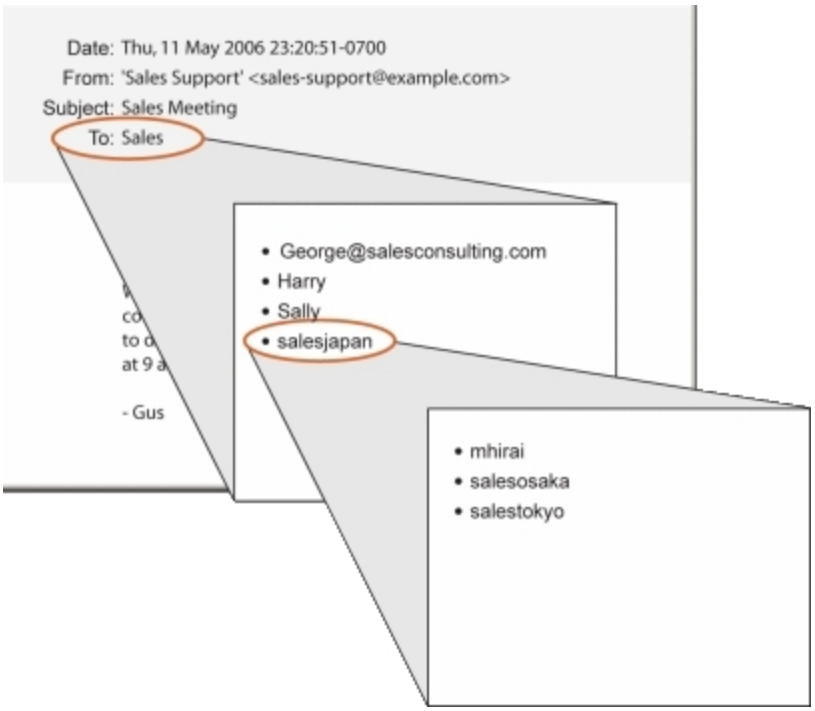
- About Distribution Lists on the facing page
- Creating and Deleting Distribution Lists on page 64
- Adding Members to and Removing Members from a Distribution List on page 65
- Finding Existing Users and Distribution Lists on page 67

About Distribution Lists

A DL is a named list of email addresses. When you send a message to a DL, the message is forwarded to all addresses on the list. DLs are used to group users together into convenient mailing lists. They can also be used as aliases for individual users.

Each entry (or member) in a DL can be the login name of a registered user, the name of another DL, a folder name (that uses the plus character (+), as in `+archive@example.com`), or any valid email address. For example, you might define a DL named `Sales` that has the members shown in Figure 7 on page 63.

Figure 7 Distribution List Example



In this example, `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 members `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 and numbers as well as hyphen (-), dot (.), and underscore (_) characters. DL names are case-insensitive and can be no longer than 64 characters.

If a DL is being used as an alias for an individual user, the DL is processed before the user. 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.

Reserved Distribution List Names

You cannot create DLs with the following reserved names:

- system-alerts
- backup-alerts
- backup-status
- daily-reports
- weekly-reports
- postmaster
- abuse (Can be deleted)
- mailer-daemon (Postmaster included by default. Can be deleted)
- operator (Can be deleted)
- schedule-output
- virus-alerts
- system-*anything*
- nobody (Can be deleted)

The first five names are reserved for DLs used by the appliance. The **postmaster** DL is required by RFCs 2821 and 2822. These DLs are created during installation. You cannot delete them (except where indicated), but you can add or delete members. The **Administrator** user account is included by default in each appliance-specific DL.

DLs, like user and folder names, are stored internally as modified UTF-7 (Unicode Transmission Format 7-bit).

Each entry in a distribution list can be the login name of a registered user, the name of another DL, a folder name (use the plus sign (+) as in `+archive@example.com`), or a remote address.

Creating and Deleting Distribution Lists

A distribution list (DL) has no assigned members when it is first added. Once you have added the distribution list, you then add users or other distribution lists as members.

Some appliance-created DLs cannot be deleted. For more information, see Reserved Distribution List Names above.

To create a DL:

1. Go to **Home > System > Distribution Lists**.

   The **Add Distribution List** page appears.

2. In the **DL Name** text field, type a unique name for the list you are creating.
3. Click **Add**.

   After creating the DL, you must add members to it. For more information, see Adding Members to and Removing Members from a Distribution List below.

To edit a DL:

1. Go to **Home > System > Distribution Lists**.

   The **Add Distribution List** page appears.

2. Click the **Edit** icon (✎) for the DL you want to add members to. For more information, see Adding Members to and Removing Members from a Distribution List below.

To delete a DL:

This procedure deletes a DL whether or not it is empty. You do not receive a warning before the information is deleted, and you will not be able to recover the information afterward.

1. Go to **Home > System > Distribution Lists**.

   The **Add Distribution Lists** page appears.

2. Select the name of the DL you want to remove. Click **Prev** and **Next** to page through the list of names, as needed. Non-removable system-created DLs do not have a checkbox by their name.
3. Click **Remove**.

Adding Members to and Removing Members from a Distribution List

Adding a user's email address to a distribution list (DL) ensures that this person receives any mail that is set to this list name. You can add local or LDAP users, remote users, or other distribution lists.

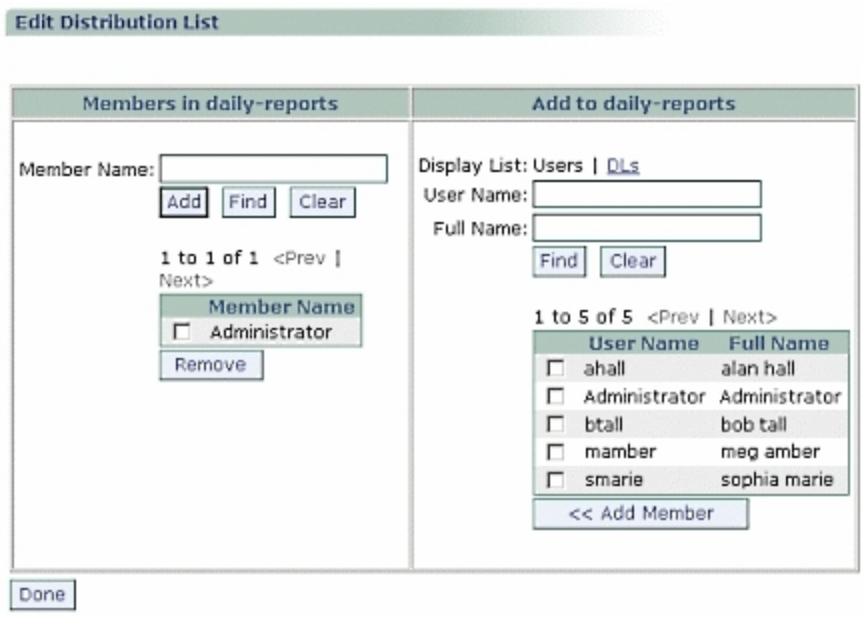
To add/remove users to a DL:

1. Go to **Home > System > Distribution Lists**.

   The **Add Distribution List** page appears.

2. Click the **Edit** icon (✎) for the DL you want to modify. Click **Prev** and **Next** to page through the list of DL names, as needed.

   The **Edit Distribution List** page appears.



3. From the **Add to *DL name*** area, select the checkbox next to the name of the user you want to add, then click **Add Member**. Click **Prev** and **Next** to page through the list.

   Or,

   If you know the username or if the member is remote, you can add the user manually using the **Members in *DL name*** area.

   a. Type in the name in the **Member Name** text field. For a remote user, enter the email address (including the at-sign (@)).
   b. Click **Add**.

   Even if a user is added to the DL, their name will still display in the **Add to *DL name*** area. You can remove a user from the **Members in *DL name*** area by selecting the checkbox and clicking **Remove**.

To add/remove DLs to a DL:

1. Go to .

The **Add Distribution Lists** page appears.

2. Click the **Edit** icon (✎) for the DL you want to modify. Click **Prev** and **Next** to page through the list of DL names, as needed.

   The **Edit Distribution List** page appears.

3. In the **Add to *DL name*** area, the **Display List** option lets you choose to see a list of **Users** or **DLs**.
4. Select the checkbox(es) for the DL(s) that you want to add. Click **Prev** and **Next** to page through the list.
5. Click **Add Member**.

   You can remove a DL from the **Members in *DL name*** area by selecting the checkbox and clicking **Remove**.

Finding Existing Users and Distribution Lists

When finding users and distribution lists, 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 (.).

To find an existing user when adding members to a DL:

1. Go to **Home > System > Distribution Lists**.

   The **Add Distribution List** page appears.

2. Click the **Edit** icon (✎) for the DL you want to modify. Click **Prev** and **Next** to page through the list of DL names, as needed.

   The **Edit Distribution List** page appears.

3. For the **Display List** option, make sure that **Users** is selected.
4. Type into one or both of the following text fields:

   - **User Name** - If you know the username for the account (e.g., jdoe)
   - **Full Name** - If you know the full name for the user (e.g., John Doe)

   You can use wildcards within the text fields.

5. Click **Find**.

To find an existing distribution list:

1. Go to **Home > System > Distribution Lists**.

   The **Add Distribution List** page appears.

2. In the **DL Name** text field, type in the name of the DL you are looking for.
3. Click **Find**.

You can also search for DLs when adding members to another DL.

1. Go to **Home > System > Distribution Lists**.

   The **Add Distribution List** page appears.

2. Click the **Edit** icon (✎) for the DL you want to modify. Click **Prev** and **Next** to page through the list of DL names, as needed.

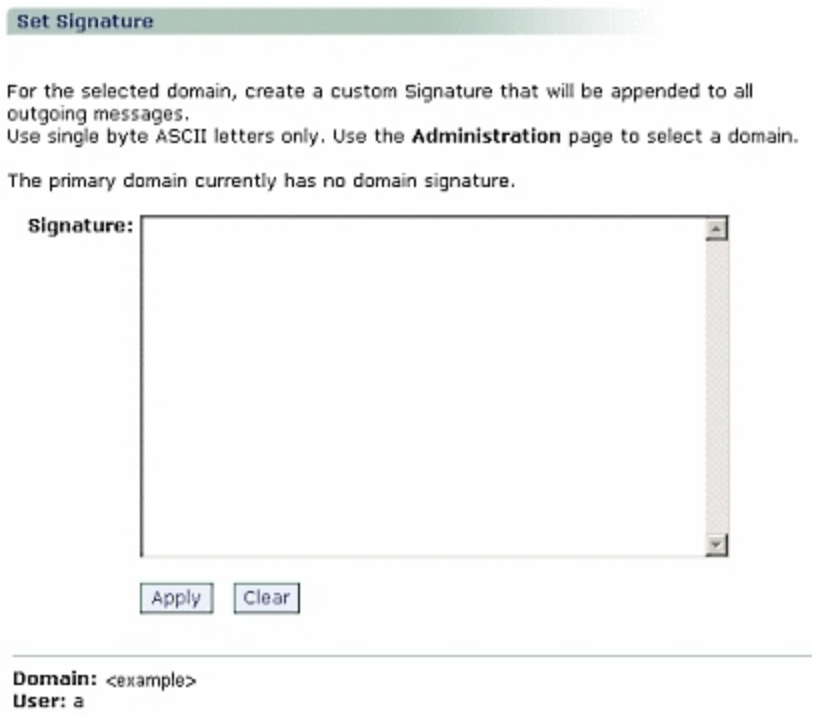
   The **Edit Distribution List** page appears.

3. For the **Display List** option, click **DLs**.
4. In the **DL Name** text field, type in the name of the DL you are looking for. You can use wildcards within the text field.
5. Click **Find**.

Creating a Mail Signature

The **Set Signature** page (**Home > System > Signature**) lets you create a 7-bit ASCII signature for all email traffic emanating from that domain. This page displays only after you have selected a delegated domain or have logged in as a Domain Administrator. Most mailers automatically append the signature to the body of the message. However, the signature might appear to the email recipient as an attachment, depending on how the mailer handles multi-part MIME messages.

Figure 8 Set Signature Page



To create a mail signature:

1. Go to **Home > System > Signature**.

   The **Set Signature** page appears.

2. Customize the text in the **Signature** text block as desired. There is a 1024 7-bit byte limit on the size of the signature.
3. Click **Apply**.

The signature you applied is appended to all outgoing mail from that domain. To remove the mail signature, click **Clear**.

Choosing a Routing Method

The **Choose Routing Method** page (**Home > System > Routing**) and associated pages provides a way to change your routing configuration without using the Setup Wizard. You can select a different routing method and configure it or make changes to your current routing method configuration.

The options that display on this page depend on your appliance's licensing, hardware, and configuration. The Mail Routing license is automatically applied to the appliance.

Additional information about selecting a routing methods is provided in the following sections:

- Selecting a Routing Method below - Manage your routing configuration. You must select one of the following routing options:
  - Route via Local Message Router on page 71 - The **Route via Local Message Router** page is displayed by default if, for some reason, the Mail Routing license is not available on the appliance.
  - Route via Local Routing Table on page 72
  - Route via LDAP Server with Mirapoint Schema on page 73
  - Route via Microsoft Active Directory on page 75
  - Route via Other LDAP Server with Non-Mirapoint Schema on page 76

Once a routing method is selected, the following links are available via the **Choose Routing Method** page:

- User Queries - Only displays for one of the LDAP Routing choices.
- Mail Group Queries - Only displays for one of the LDAP Routing choices.
- Mail Host Mapping - Only displays if the **Route via Microsoft Active Directory** method is selected and Junk Mail Manager (JMM) is disabled.

Selecting a Routing Method

If you have Mail routing (i.e., LDAP routing) licensed, the **Choose Routing Method** page displays. Specify a routing method. After you have made your selection the page changes to provide you with further options.

If you change your routing method after initially configuring it, you might be asked to confirm your selection before being directed to the appropriate page.

Table 9 Routing Method Decision Table

If this configuration...	Then use...	Notes
Does not have access to the local routing table or LDAP	Route via Local Message Router on the facing page	This routing method only displays if you do *not* have Mail Routing (i.e., LDAP routing) licensed, and you do *not* have Junk Mail Manager (JMM) enabled.
Can forward to different servers based on domain name, but has no LDAP server access	Route via Local Routing Table on page 72	Deployments with few Message Servers and routers, and lacking access to an LDAP server, are the best candidates for the local routing table. This routing method creates a local, LDIF-based routing table, and should *not* be used in conjunction with other LDAP based setups.
Will use an LDAP Server with the Mirapoint schema	Route via LDAP Server with Mirapoint Schema on page 73	This routing method offers highly flexible options; the base DN (distinguished name) and default records can be instantiated for you.
Will use an LDAP server with Active Directory	Route via Microsoft Active Directory on page 75	This routing method offers highly flexible options; the base DN and default records can be instantiated for you.
Will use an LDAP server with a different, non-Mirapoint schema	Route via Other LDAP Server with Non-Mirapoint Schema on page 76	This routing method requires you to manually add certain records; the base DN and default records can *not* be instantiated for you.

For more information about setting up LDAP, see the *Mirapoint MOS Configuration Guide*.

About Mail Domain Routing

The **Mail Domain Routing** area on the non-Local Message Router routing method pages, provide the following options for LDAP lookups on message addresses:

These options only display if Junk Mail Manager (JMM) is disabled and the **Use LDAP Routing** option is set to **All Messages** or **Local Messages** on the SMTP **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**).

- **All domains** - Does an LDAP lookup whenever mail arrives; if the domain is not in LDAP, then no MX record lookup is done. This option is for situations where the domain list changes very often and it is easier to perform an LDAP lookup on all recipients rather than try to continually update the domain list on all mail routers; however, this option can stress your LDAP server(s). In the case of local routing table routing, this option could be used to reject all mail that is not addressed to a local domain.
- **Known domains only** (default) - Does an LDAP lookup whenever mail arrives that is addressed to a known domain (the mail and delegated domains configured locally). This is a time saver and reduces load on your LDAP server, and can also help foil denial-of-service (DoS) attempts. If the domain is not found in LDAP, then an MX record lookup is done.

Route via Local Message Router

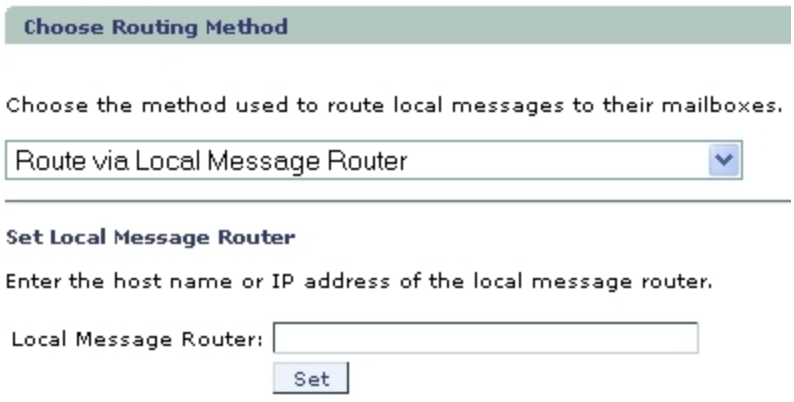
If you do not have Mail Routing (i.e., LDAP routing) licensed, the **Route via Local Message Router** page displays instead of the **Choose Routing Method** page. This routing method directs the appliance to refer all routing to the message router you specify. The LMR (local message router) can route messages to all hosts in your organization. Messages that are not deliverable on the local host are sent to this LMR for routing to the correct host. Local message routing is useful in deployments involving multiple systems where message servers do not have access to routing information (local routing table) or LDAP. A LMR is usually located inside the firewall. It can route messages for all hosts in your organization.

To configure the Route via Local Message Router routing method:

1. Go to **Home > System > Routing > Routing Method**.

   The **Route via Local Message Router** page appears or the **Choose Routing Method** page appears depending on your licensing.

2. If the **Choose Routing Method** page appears, select **Route via Local Message Router** from the drop-down menu. If not, skip to step 3.
3. In the **Local Message Router** text field, type the name of a single mail server that can accept all incoming messages from this appliance. When you have a single mail server, the LMR is that mail server.



4. Click **Set**.

Route via Local Routing Table

If this appliance can forward to different servers based on domain name, local routing table routing is an excellent choice as it provides a quick, simple setup. If you use this method you should make sure that all of your appliances are configured with the same local routing table information. You can specify separate mail servers for individual email addresses, or a single mail server destination for an entire domain.

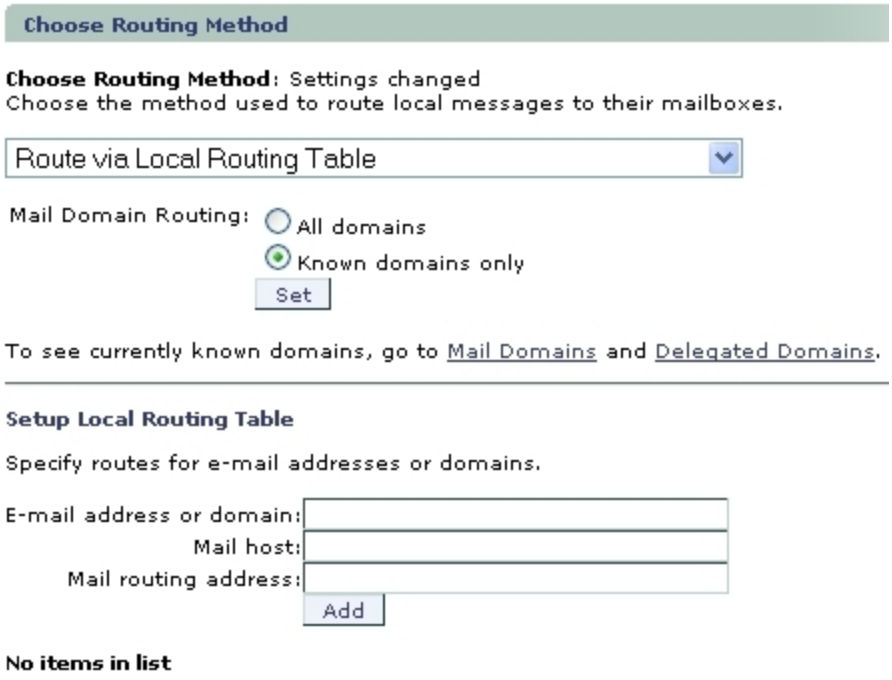
The local routing table uses the local LDAP capabilities, and should *not* be used in conjunction with other LDAP-based deployments.

To configure the Route via Local Routing Table routing method:

1. Go to **Home > System > Routing > Routing Method**.

   The **Choose Routing Method** page appears.

2. Select **Route via Local Routing Table** from the drop-down menu.
3. The page redisplays with the following options:



- **Mail Domain Routing** - For more information, see About Mail Domain Routing on page 70
- **E-mail address or domain** - To route all messages for a domain to a given mail server, type the domain name. You need to repeat this procedure for all supported domains. To route user messages to different domains and mail hosts, type the user name with the fully-qualified domain name (FQDN). For more information, see Local Routing Table Examples below.
- **Mail Host** - The Message Server where the user folder resides; it is equivalent to the LDAP `MailHost` attribute. With local routing, it is usually not necessary to specify both mail host and routing address. To route messages for a domain, type the mail server or router for that domain. To route user messages, leave this blank.
- **Mail Routing Address** - The actual user name, followed by an at-sign (@), and the name of the mailhost or domain where the user folder resides. This is equivalent to the LDAP `MailRoutingAddress` attribute. With domain-based local routing, this specification is usually not necessary, but sometimes certain users have a unique mail routing address. To route messages for a domain, leave this blank. To route user messages, type the user's full address.
- **Junk Mail Manager Host** (This option only displays if JMM is enabled) - For each domain that you are adding for which JMM is to handle spam, enter the JMM host for that domain. If the domain is local to the appliance, you can type `localhost`.

4. Click **Add**.

To edit the local routing table, click the **Edit** icon (✎) in the list box and make your changes.

Local Routing Table Examples

Routing Messages for Domains Example:

If Big Company buys out Small Company, you can route email to both from a single message router by specifying that domain `@bigcompany.com` goes to **Mail Host** `mail.bigcompany.com` while domain `@smallco.com` goes to **Mail Host** `smallco.bigcompany.com`. (There is no **Mail Routing Address** in this example.)

Routing Messages for Users Example:

To route messages addressed to `Joe.User@smallco.com` to his folder on `smallco.bigcompany.com`, specify this address as the **Email address or domain**, and `juser@smallco.bigcompany.com` as the **Mail Routing Address**.

Route via LDAP Server with Mirapoint Schema

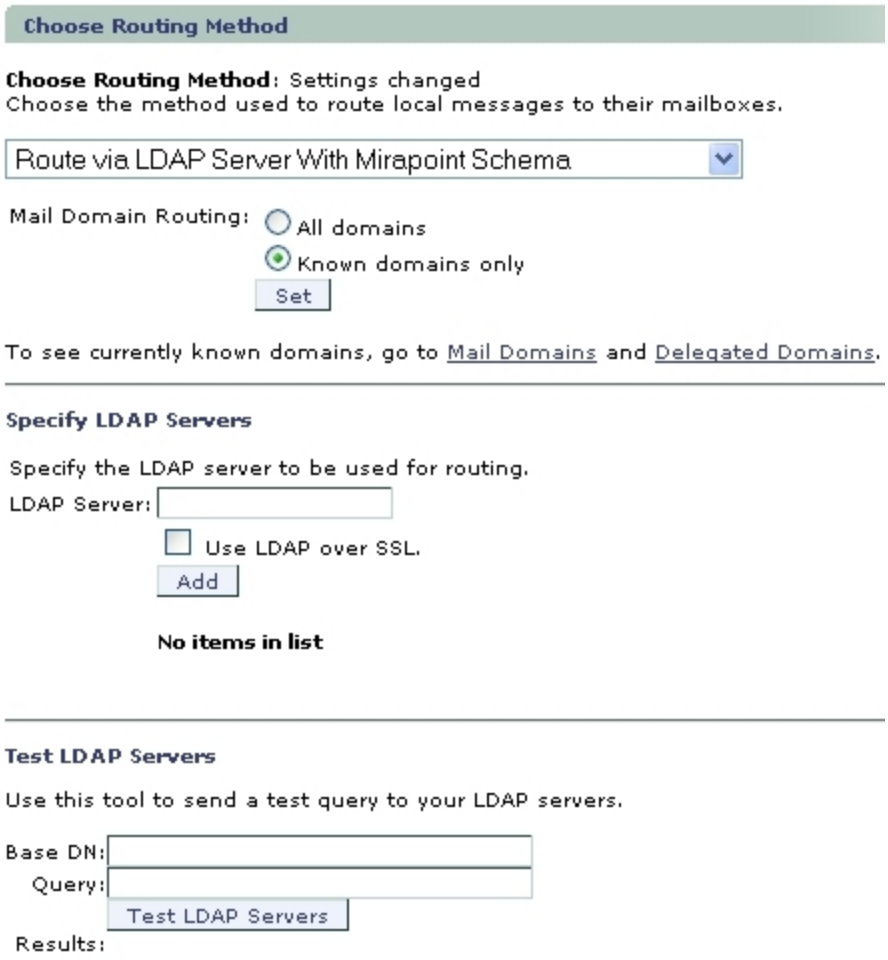
The **Route via LDAP Server with Mirapoint Schema** routing method is the most flexible option, and offers the considerable advantage of a centralized database, but requires an LDAP server to be configured on your network with the Mirapoint LDAP schema. On the inbound router, addresses are looked up in the LDAP database and routed to the correct host. User services can be classified and customized with database attributes. LDAP specifies where to route messages according to the values for the configured LDAP attributes `Mailhost` and `RoutingAddr`. This is the most complicated method and requires that you make the following specifications as described.

To configure the Route via LDAP Server with Mirapoint Schema routing method:

1. Go to **Home > System > Routing > Routing Method**.

   The **Choose Routing Method** page that appears.

2. Select **Route via LDAP Server with Mirapoint Schema** from the drop-down menu.
3. The page redisplays with the following options:



   - **Main Domain Routing** - For more information, see About Mail Domain Routing on page 70.
   - **Specify LDAP Servers** - The hostname of the LDAP servers to be used for LDAP queries. You can send a test query to an LDAP server as well.
   - **Use LDAP over SSL** - Select this if you want LDAP queries to be made over connections using Secure Sockets Layer (SSL). If this checkbox is selected, a protocol prefix of `ldaps://` is automatically prepended to the query string. If this checkbox is not selected, `ldap://` is prepended.

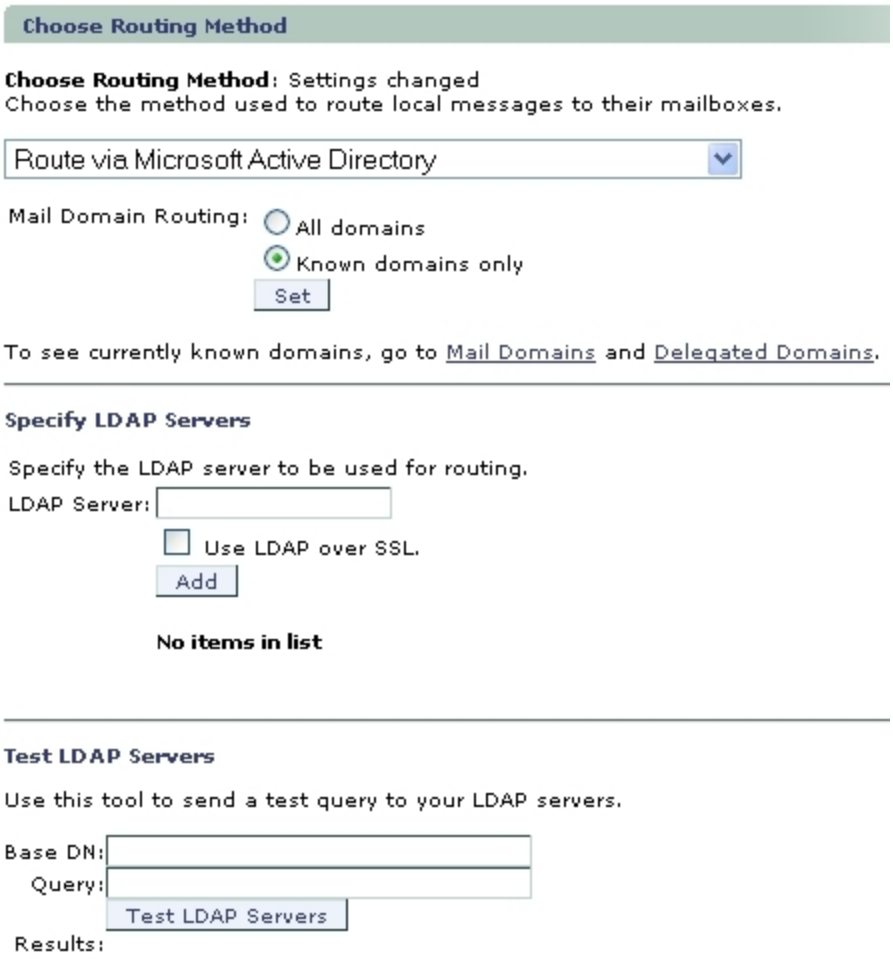
4. Click **Add**.

Once added, you can use the **Test LDAP Servers** area to send a test query to your LDAP server.

Route via Microsoft Active Directory

For the **Route via Microsoft Active Directory** routing method, on the inbound router, addresses are looked up in the Active Directory database and routed to the correct host, often based on the user's `mail` attribute. User services can be classified and customized with database attributes.

Figure 10 Choose Routing Method - Route via Microsoft Active Directory



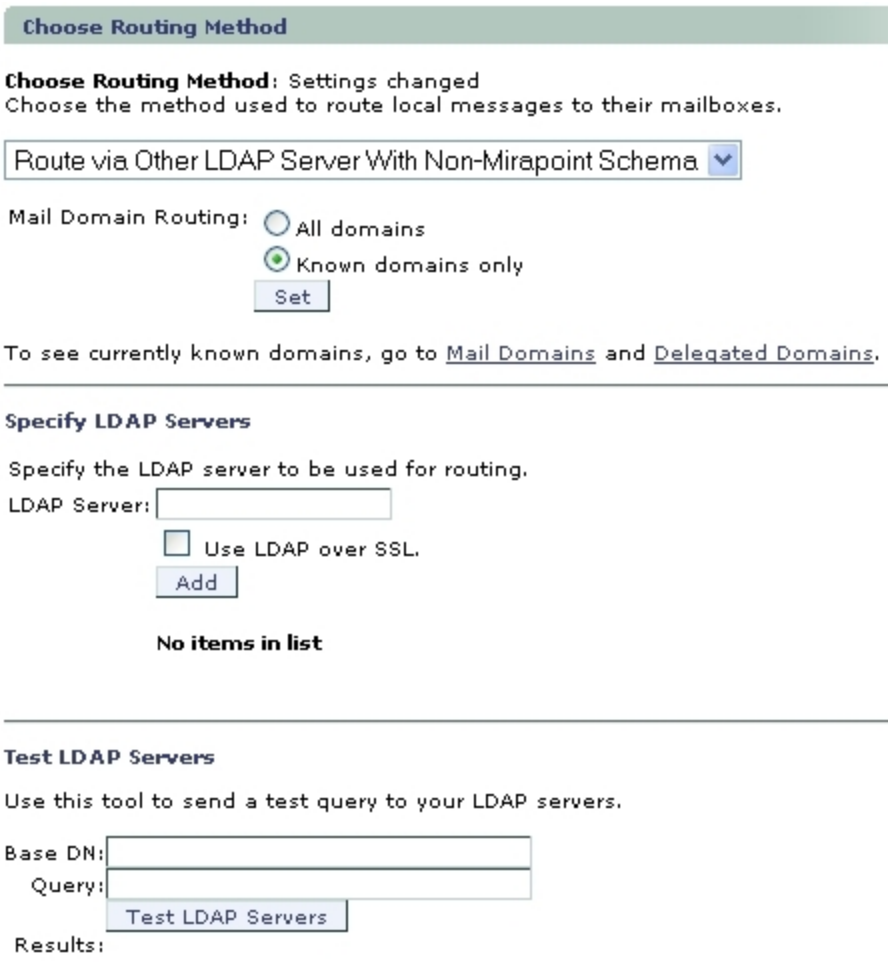
This routing method is configured in the same way as **Route via LDAP Server with Mirapoint Schema** method. Follow the steps described in Route via LDAP Server with Mirapoint Schema on page 73, Configuring LDAP User Queries on page 77, and Configuring LDAP Mail Group Queries on page 78. You will need the name of your **Active Directory LDAP server**, and the **Credentials** data.

If you are using the Setup Wizard, the wizard is typically able to retrieve the other settings for you with the exception of the **Credentials**, which must be manually entered. For more information, see Using the Setup Wizard on page 13.

Route via Other LDAP Server with Non-Mirapoint Schema

The **Route via Other LDAP Server with Non-Mirapoint Schema** routing method is configured in the same way as Route via LDAP Server with Mirapoint Schema with the important distinction that the system cannot instantiate the base DN (distinguished name) and default records for you. You might need to contact Mirapoint Professional Services for help.

Figure 11 Choose Routing Method - Route via Other LDAP Server with Non-Mirapoint Schema



You will need the name of your LDAP server, and you will need to specify your Directory Information Tree (DIT) structure and LDAP attributes for `Mailhost` and `RoutingAddr`. These specifications are discussed in detail in the *Mirapoint MOS Configuration Guide*. You should only make these specifications after you have planned and tested your LDAP service.

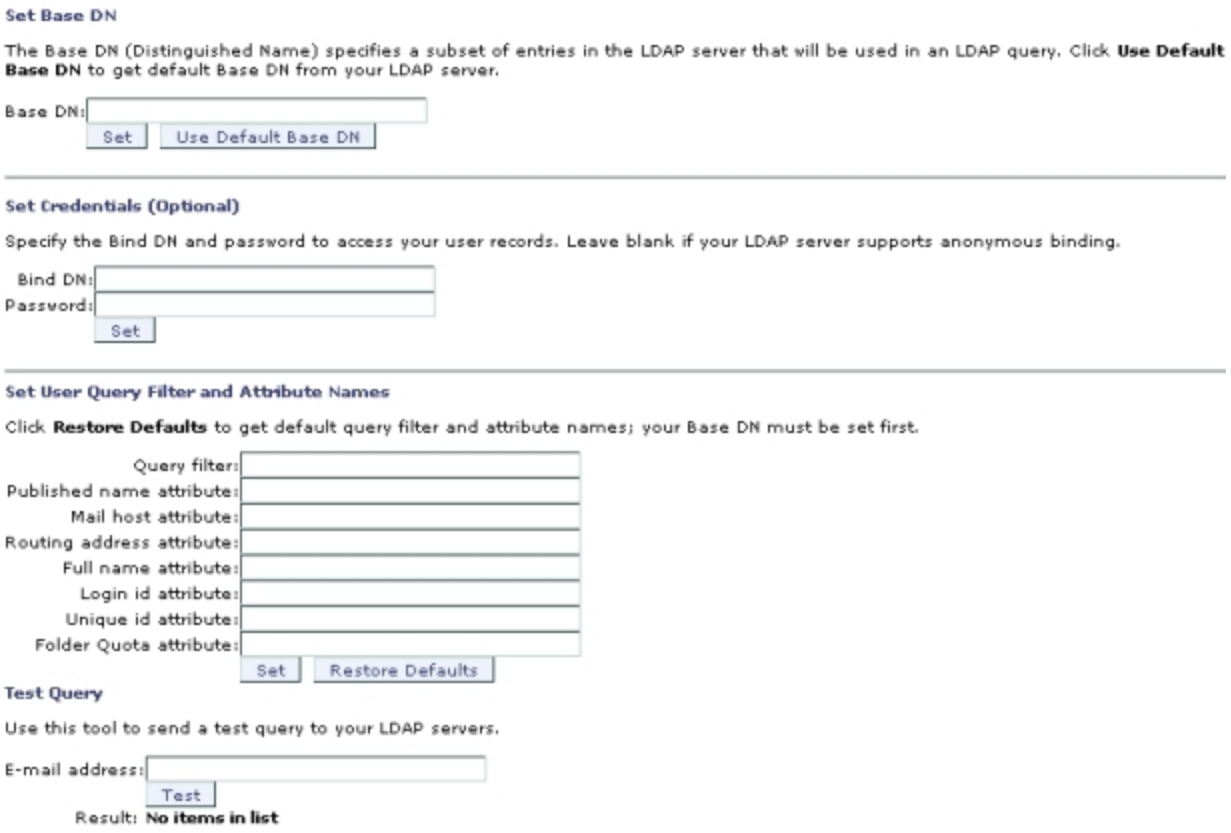
Configuring LDAP User Queries

You should only make these specifications after you have planned and tested your LDAP service. Configuring LDAP User Queries is discussed in detail in the *Mirapoint MOS Configuration Guide*. For more information on query filter and attribute names, see the *Mirapoint Message Server Administrator's Guide* and the *Mirapoint Administration Protocol Reference*.

To configure the LDAP user queries for a routing method:

1. Go to **Home > System > Routing > User Queries**.

   The **LDAP User Queries** page appears.



2. In the **Base DN** text field, type the location in the DIT where the LDAP query should begin. Click **Use Default Base DN** to instantiate this option.
3. Click **Set**.

4. Under the **Set Credentials (Optional)** section, type in the **Bind DN** and **Password** in the text fields. This is the configured DN and password set for the LDAP database superuser. Usually, this is not needed for Mirapoint LDAP schemas. For more information, see the *Mirapoint MOS Configuration Guide* or type `Help About Dir` in the command-line interface (CLI).
5. Click **Set**.
6. Under the **Set User Query Filter and Attribute Names** section, type in the appropriate information for the following attributes: (If you clicked **Use Default Base DN** in step 1, this information was instantiated for you.)
   - **Query Filter**
   - **Published name attribute**
   - **Mail host attribute**
   - **Routing address attribute**
   - **Full name attribute**
   - **Login id attribute**
   - **Unique id attribute**
   - **Folder quota attribute**
7. Click **Set**.

Once set, you can use the **Test Query** area to send a test query to your LDAP server.

Configuring LDAP Mail Group Queries

LDAP mail group queries are discussed in detail in the *Mirapoint MOS Configuration Guide*. You should only make these specifications after you have planned and tested your LDAP service.

If you are using the Setup Wizard to set the LDAP mail group queries, it creates a database named `mira_route_top_db`.

To configure the LDAP mail group queries for a routing method:

1. Go to **Home > System > Routing > Mail Group Queries**.

   The **LDAP Mail Group Queries** page appears.

2. In the **Base DN** text field, type the location in the DIT where the LDAP query should begin. Click **Use Default Base DN** to instantiate this option.
3. Click **Set**.
4. Under the **Set Credentials (Optional)** section, type in the **Bind DN** and **Password** in the text fields. This is the configured DN and password set for the LDAP database superuser. For more information, see the *Mirapoint MOS Configuration Guide* or type `Help About Dir` in the command-line interface (CLI).
5. Click **Set**.
6. Under the **Set User Query Filter and Attribute Names** section, type in the appropriate information for the following attributes: (If you clicked **Use Default Base DN** in step 1, this information was instantiated for you.)
   - **Query Filter**
   - **Mail group attribute**
   - **Allowed domain attribute**
   - **Allowed broadcaster attribute**
7. Click **Set**.
8. Type in the **Mail group member attribute** in the text field and select one of the following options: (If you clicked **Use Default Base DN** in step 1, this information was instantiated for you.)

- **Attribute contains e-mail address**
- **Attribute contains distinguished name**

9. Click **Add**.

Once added, you can use the **Test Query** area to send a test query to your LDAP server.

Configuring Domain to Mail Host Mapping

The **Domain to Mail Host Mapping** page (**Home > System > Routing > Mail Host Mapping**) displays only if the **Route via Microsoft Active Directory** routing method is selected and Junk Mail Manager (JMM) is disabled.

To configure mail host mapping:

1. Go to **Home > System > Routing > Mail Host Mapping**.

   The **Domain to Mail Host Mapping** page appears.

2. For every mail domain for which this appliance will route mail, specify the following:
   - **Domain Name** - The name of the mail domain.
   - **Mail Host** - The name of the mail server or host for that domain.
3. Click **Add**.

Changing Your Password

Use the **Change Your Password** page (**Home > System > Password**) to change your own password. A password is a secret text string (numbers and letters) that is case-sensitive and up to 80 characters long. When users forget their passwords, an administrator or a delegated domain administrator can establish a new password using the **Add User** page. For more information, see Editing Users on page 60

To change your password:

1. Go to **Home > System > Password**.

   The **Change Your Password** page appears.

2. In the **Old Password** text field, type in your old password.
3. In the **New Password** text field, type in your new password.
4. In the **Confirm Password** text field, re-type your new password.
5. Click **Change Password**.

You also have the option of changing your password using the Setup Wizard. For more information, see Changing Your Password on page 15.

Using Utilities

Use the utilities-related administration pages (**Home > System > Utilities**) allow you to check and/or fetch licenses, set up service reporting, and check the Messaging Operating System (MOS) version or look for updates.

The **About Utilities** page provides the following links:

- License - View current license information and obtain new licenses.
- Service Reporting - Configure Service Reporting.
- Updates - View current installed updates information, obtain new updates, and configure updates notifications.

Managing Licenses

Use the **License** page (**Home > System > Utilities > License**) to apply license keys. A PDF document containing all your license keys is emailed to the designated "ship to" contact. You can also download and apply license keys using the **Install Licenses** option or the `License Fetch` command within the command-line interface (CLI). For more information, see Automatically Applying a License on next page and the *Mirapoint Administration Protocol Reference*.

If you have forgotten your license key, use the License Key Look Up tool on the Mirapoint Technical Support website. You must have a Support website login ID and password, your appliance's serial number, and the host ID number. You can email key-help@mirapoint.com to set up a Support website account. If you cannot locate your license keys, email key-request@mirapoint.com for assistance.

Additional information about licenses is provided in the following sections:

- Automatically Applying a License below
- Manually Applying a License below
- What Happens When Antivirus/Antispam Licenses Expire? on the facing page

Automatically Applying a License

Click **Install Licenses** to automatically download and apply license keys; Internet connectivity is required. If a license has not yet been applied to the appliance, clicking **Install Licenses** will apply it. All keys downloaded from the Mirapoint license server are encrypted for security and this operation honors HTTP proxy settings.

To see all of the license keys available to you, click **Show License Keys**. The license key table will reload with a new column showing the key for each installed license. The link also changes to **Hide License Keys** so you can remove the column from the table, if desired.

Manually Applying a License

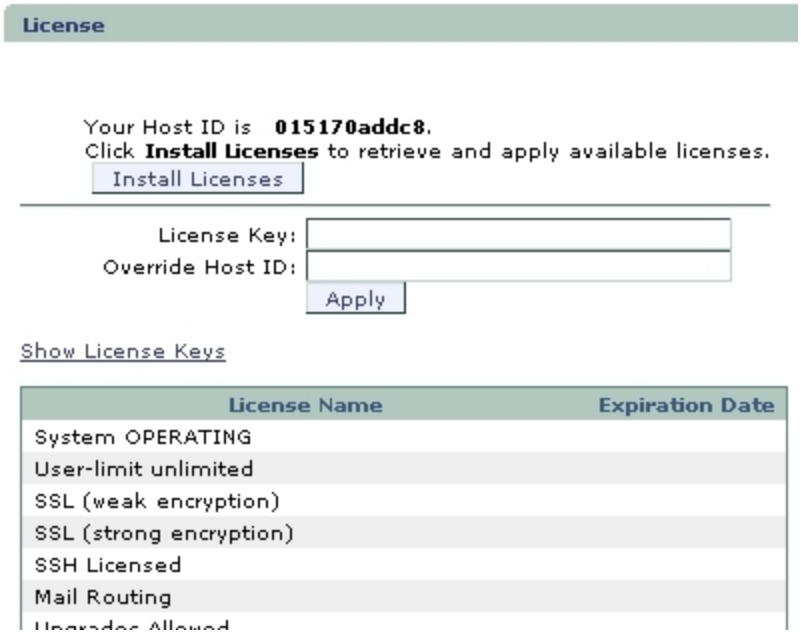
When applying a new license you might need to manually add the license key and override the set host ID for that license. This might be necessary under the following circumstances:

- When swapping primary and secondary heads in a failover system.
- After replacing the network interface card due to a failure.
- During a disaster recovery after having installed new hardware.

To manually apply a license:

1. Go to **Home > System > Utilities > License**.

   The **License** page appears.



2. In the **License Key** text field, type in the key for the license you want to install.
3. In the **Override Host ID** text field, type in the host ID that was originally used to install the license.
4. Click **Apply**.
5. After the license is applied, you must reboot the appliance.

The license is now available on the current host.

What Happens When Antivirus/Antispam Licenses Expire?

On expiration of these licenses the following actions occur:

- Antivirus (AV) - The antivirus engine(s) continue to run but signature-based antivirus scanners (e.g., Sophos, F-Secure) cannot update the pattern files.
- Antispam (AS) - The antispam engine(s) stop scoring mail and Signature Edition cannot get updates.
- MailHurdle (MH) - MailHurdle continues to run but cannot get updates to allowed misbehaving mailers.

After applying an antivirus license, go to the **Antivirus Updates** page for that antivirus scanner and click **Update Now** to get the latest files for that scanner. For more information, see Managing Antivirus Scanning on page 105.

Service Reporting and Updating the Appliance

The **Service Reporting** page (**Home > System > Utilities > Service Reporting**) allows you to add the `customercare@mirapoint.com` address to the **system-alerts** and **weekly-reports** distribution lists (DLs). If you disable service reporting, the `customercare@mirapoint.com` address is removed from these two DLs. Service Reporting is enabled by default.

These alerts and reports do not reveal the contents of the email messages on your appliance.

To enable service reporting:

1. Go to **Home > System > Utilities > Service Reporting**.

   The **Service Reporting** page appears.

2. Click **Enable it**.

If service reporting is already enabled, the page displays **Disable it**. When Service Reporting is enabled, the `customercare@mirapoint.com` address is added to the **system-alerts** and **weekly-reports** DLs.

3. Under the **Update Contact Information** area, in the **Contact Information** text block, type the contact names, email and/or postal addresses, and phone numbers as appropriate.

The contact information allows Mirapoint Customer Services to contact these individuals quickly if a problem is detected in the **system-alerts** or **weekly-reports** sent to `customercare@mirapoint.com`.

4. Click **Update**.
5. Under the **Set Alerts Recipients** area, in the **E-mail Address** text field, type an email address that will receive alerts.

6. Click **Add**.

The new address is added to the **Alerts recipients** table. Add as many addresses as needed. You can remove addresses by selecting them in the table and clicking **Remove**.

7. Under the **Set Reports Recipients** area, in the **E-mail Address** text field, type an email addresses that will receive reports.

8. Click **Add**.

   The new address is added to the **Reports recipients** table. Add as many addresses as needed. You can remove addresses by selecting them in the table and clicking **Remove**.

Updating the Appliance

Use the **Update Information** page (**Home > System > Utilities > Updates > Update Information**) to view current version information, recommended and installed updates, to install and remove updates, and to view patch notes on updates.

The **Update Information** page shows your installed updates as well as any recommended, and not currently installed, updates. The **Update Information** page can advertise system updates for inapplicable hardware platforms. Read the relevant release notes before applying any update.

The following options are available:

- Click the update **Description** (if available) to open the patch note for that update.
- Click the **Uninstall** icon () to remove an update from your appliance.
- Click the **Install** icon () to begin the installation process for an update.

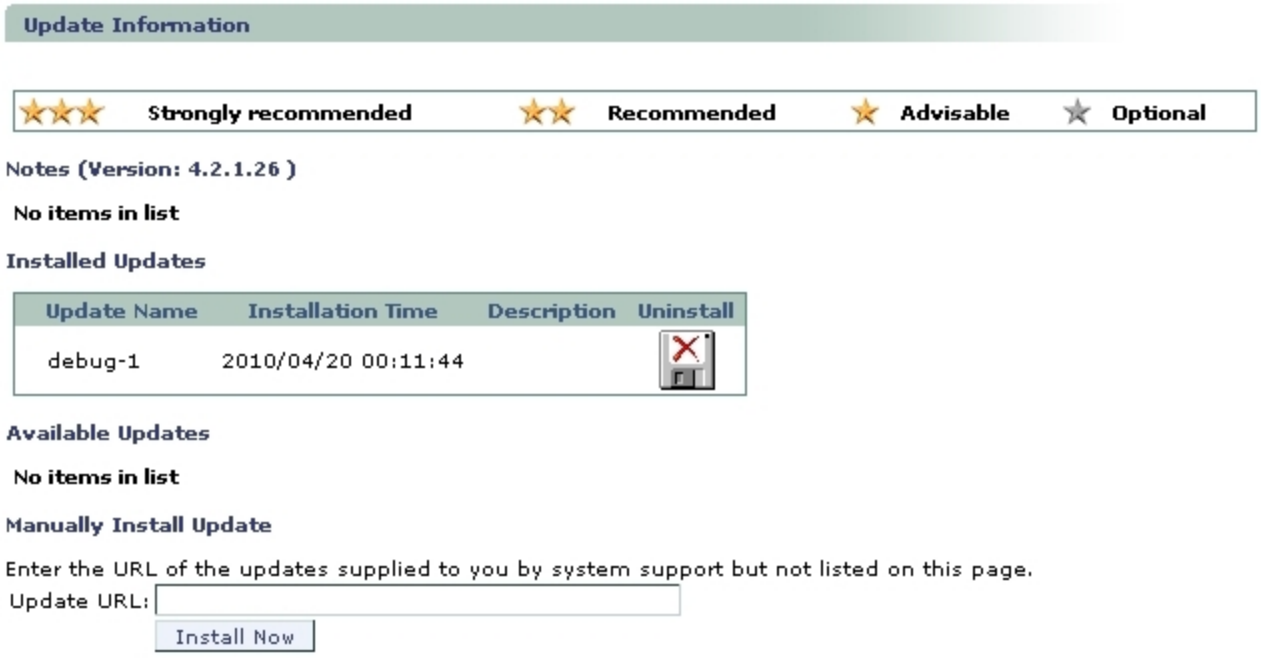
Manually Installing an Update

You can manually install an update that is not displayed on the **Update Information** page.

To manually install an update:

1. Go to **Home > System > Utilities > Updates**.

   The **Update Information** page appears.



2. Under **Manually Install Update**, in the **Update URL** text field, type in the URL to the update. You can obtain the URL from Mirapoint Technical Support.
3. Click **Install Now**.

The inactivity timeout is 15 minutes. After 15 minutes, an error displays, `Can't find update status`. However, usually, the update has successfully finished.

Using Update Check

Use the **Update Check** page (**Home > System > Utilities > Updates > Update Check**) to set up automatic checks for updates or to perform a manual, immediate check.

To check hourly for updates:

1. Go to **Home > System > Utilities > Updates > Update Check**.

   The **Update Check** page appears.

2. Select the **Check hourly for available updates** checkbox.
3. In the **Send notification to** text field, type an email address where the notification will be sent.
4. Click **Apply**.

The appliance sends an email to the specified person notifying them when an update becomes available.

To check for an update immediately:

1. Go to **Home > System > Utilities > Updates > Update Check**.

   The **Update Check** page appears.

2. Click **Check Now**.

The appliance performs an update check and refreshes the **Update Information** page if there are any new available updates.

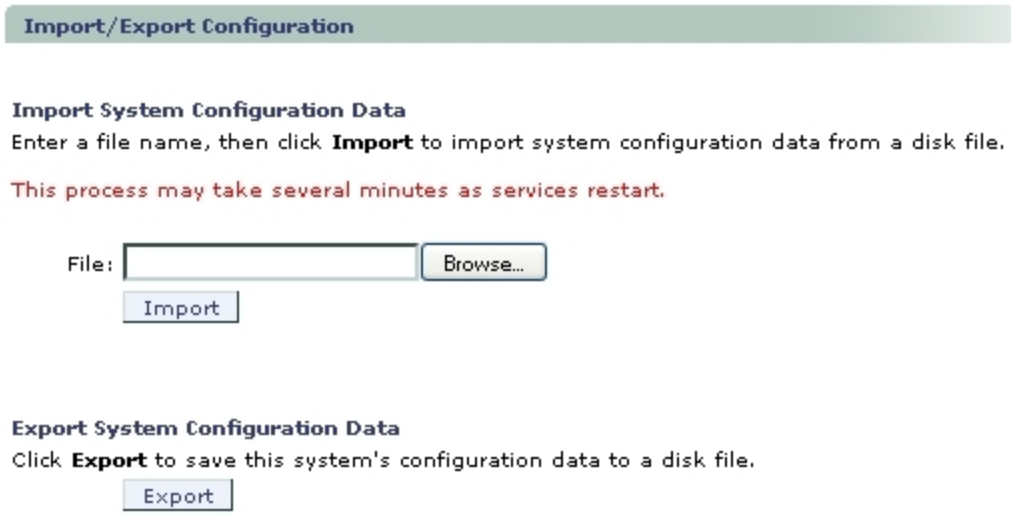
Importing and Exporting Configuration Data

Use the **Import/Export Configuration** page (**Home > System > Import/Export**) to import or export the appliance's configuration data. This can be useful as part of a backup strategy. For more information about backup and restore functionality, see the *Mirapoint Backup and Restore Guide*.

To import configuration data:

1. Go to **Home > System > Import/Export**.

   The **Import/Export Configuration** page appears.



2. In the **File** text field, type in the name of the file or use **Browse** to navigate to the file.
3. Click **Import**.

A message displays indicating the completion or any problems with the import.

To export configuration data:

1. Go to **Home > System > Import/Export**.

   The **Import/Export Configuration** page appears.

2. Click **Export**.

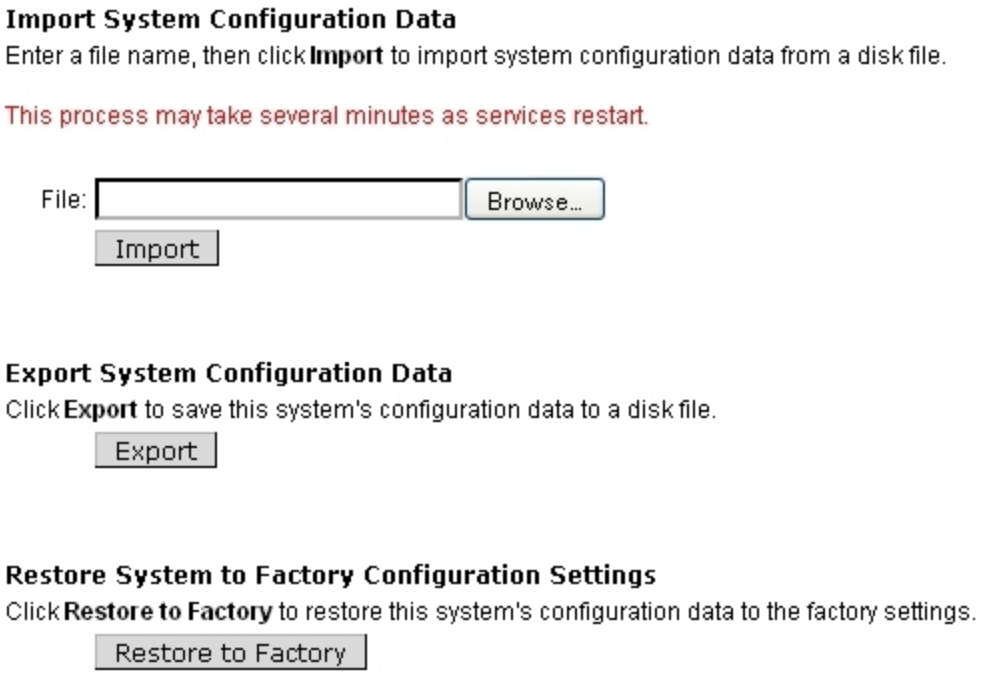
   A file download dialog box displays.

3. Save the file.

To restore configuration data:

1. Go to **Home > System > Import/Export**.

   The **Import/Export Configuration** page appears.



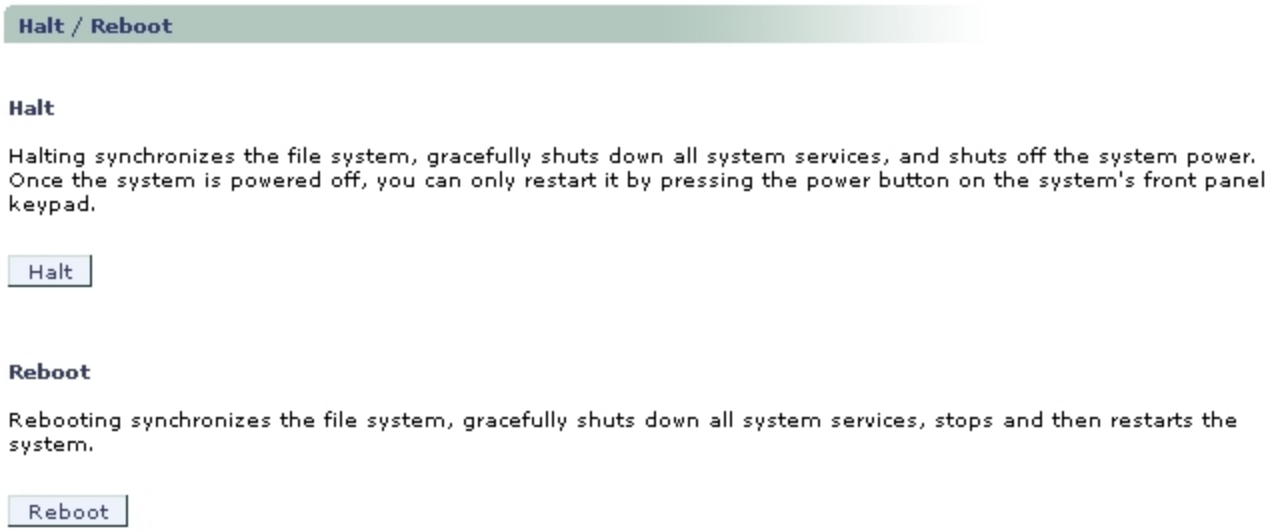
2. Click **Restore to Factory**.

A message displays indicating completion and the appliance's configuration is returned to its factory state.

Halting and Rebooting the Appliance

Use the **Halt/Reboot** page (**Home > System > Halt/Reboot**) to halt or reboot your system in a graceful way.

Figure 12 Halt/Reboot Page



- **Halt** - Synchronizes the file system, gracefully shuts down all system services, and shuts off the appliance's power. After you click **Halt**, the appliance waits one minute before shutting down, giving you time to log out. Once the appliance is powered off, you can only restart it by pressing the power button on the appliance's front panel keypad.
- **Reboot** - Synchronizes the file system, gracefully shuts down all system services, and reboots the appliance. Do this when a reboot is required to instantiate an update or some other installation, after completing a reattach operation, or after completing a standby operation.

Chapter 3: Managing Security Settings

This chapter discusses Mirapoint security features, how to use the MailHurdle, antivirus and antispam options, including Junk Mail Manager (JMM).

The following topics are included:

- Using Security Features below
- Managing Certificates on page 97
- Managing SSL Connections on page 101
- Managing Trusted Admins on page 103
- Managing Antivirus Scanning on page 105
- Managing Antispam Scanning on page 125
- Managing MailHurdle on page 148
- Managing Junk Mail Manager on page 155

Using Security Features

Security implementation tasks are presented in this section. There are four layers of security to consider: network security, inbound message handling, message content control, and outbound message handling.

Mirapoint recommends reading the *Mirapoint Site Planning Guide* for an in-depth conceptual explanation of each security layer.

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 command-line interface (CLI) 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 to set:

- TCP rate limiting - For more information, see the *Mirapoint MOS Configuration Guide*.

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. For more information, see Managing the Reject List on page 145.
- Relay domains - To prevent open relaying (unwanted use of your network), specify which IP addresses or domains can use your network. For more information, see Managing the Relay List on page 144.
- Real-time Blackhole List (RBL) - You can make use of various services on the Internet keeping track of spamming domains. For more information, see Managing RBL Host Lists on page 146.

SMTP Layer Security

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

All possible SMTP actions or Mirapoint appliance options are not included in this example. Also, this example uses HELO rather than EHLO. The possible responses to EHLO are much longer and more varied.

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.

1. An email is sent to a Mirapoint appliance: SMTP connection occurs on port 25.

   RazorGate TCP connection limits can help prevent Denial of Service (DoS) Attacks. For more information, see the *Mirapoint MOS Configuration Guide* and *Mirapoint RazorGate Administrator's Guide*.

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, and 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 the RBL host list, blocked senders list, blocked addresses lists (content filters), SSL enforcement, SMTP authentication enforcement, LDAP masquerade, and sender checking. These restrictions are set on the **Set RBL Host List** page (**Home > Antispam > RBL Host List**), **Set Blocked Senders** page (**Home > Antispam > Blocked Senders**), **Blocked Addresses Filter** page (**Home > Content Filtering > Blocked Addresses**), and the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**).

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 SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**), disallow open relays on the **Set Relay List** page (**Home > Antispam > Relay List**), and configure MailHurdle on the administration pages accessed at **Home > Antispam > MailHurdle**.

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
    ```

Inbound Message Handling Layer

Security features for inbound message handling include the following:

- TLS encryption - Uses encryption for added privacy of messages. This is set on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**) by selecting the **Allow STARTTLS (Inbound Connections)** checkbox.
- SMTP authentication - Requires that all users connecting to the mail service must be authenticated. This is set on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**) by selecting the **Require Secure Authentication (SSL)** checkbox.

If you want to set the SSL version, cipher suite, or SMTPS, see the *Mirapoint Administration Protocol Reference*.

- SMTP sender check - Requires that the sender has a valid domain. This is set on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**) by setting the **Reject Messages from Unknown Senders** option to **Yes**.
- SMTP recipient check - Requires that mail recipients be valid users. This is set on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**) by setting the **Reject Messages for Unknown Recipients** option to **Yes**.
- 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 on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**) by setting the **Rewrite From address based on authentication** option to **Yes**.

For more information on all SMTP-related options, see Managing the SMTP Service on page 42

Message Content Handling Layer

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. For more information, see About Filter Priorities and Ordering on page 174.
- Antivirus scanning - Configure up to three antivirus engines to keep viruses out. For more information, see Managing Antivirus Scanning on page 105.
- 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.

  For more information, see Managing Antispam Scanning on page 125.

- Domain Message filters - These filters operate on all mail incoming to a particular domain or set of domains. For more information, see Managing Delegated Domains.
- 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** option on the HTTP service's **Main Configuration** page (**Home > System > Services > HTTP > Main Configuration)** to **Required**. This secures user information by requiring cookies for all sessions.

Outbound Message Handling Layer

Outbound message control includes the following functionality:

- 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 by selecting the **Require Secure Authentication (SSL)** checkbox on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**).
- Sender Normalization to SMTP AUTH - 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 SMTP AUTH. This is set by selecting **Yes** for the **Re-write From address based on authentication** option on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**).
- 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 by selecting **Yes** for the **Reject Messages for Unknown Recipients** option on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**).
- 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 ampersand (@). The `Exception Add` CLI command's `senderisauth` attribute normalizes the username, while masquerade settings normalize the domain name. This is set by using the **Masquerade all messages as this domain** option on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**). For more information on `Exception Add`, see the *Mirapoint Administration Protocol Reference*.
- 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). This is set by using the **Maximum Message Size** option on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**).

Configuring Multi-Listeners

Mirapoint appliances can listen for SMTP connections on multiple ports and interfaces at once. For example, if you wanted 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, e.g., 10.1.1.25, that would be the default port for message transfer. However, if you also want to accept mail submissions on the agreed-upon port 587. You would use the following CLI command:

```
Smtp Addlistener *:587
```

To add to this example, you can have a different Message Server at IP address 10.3.3.5 that has a second ethernet interface attached. On the primary interface, port 25, you could plan to run MailHurdle, Antivirus, Antispam, and filtering, but you also want this appliance to accept email quickly from trusted users on a local network. In this case, 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. So, you would use the following command:

```
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`. For more information, type `Help About Smtp` in the CLI and see RFC 2476.

Configuring NIC Failover

NIC failover allows an appliance to switch seamlessly to a second network connection if the first one fails.

To configure NIC failover on a Mirapoint appliance:

1. Obtain a second drop from the same advertised network and attach the cable to Port1 on the appliance back panel. (This assumes that 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 using the following command:

   ```
   Netif Addlogical "" Failover
   ```

   With null-string argument, the appliance automatically manages the namespace for logical ports, usually creating `logical0` to start, but you will need to use 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. For example:

   ```
   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 the `Netif Set` command. There is currently a limit of two physical ports per logical port.

4. Verify if the first-bound port was previously associated with an IP address:
   - If so, the logical port was automatically bound to its IP address.
   - If not, associate the logical port with its assigned IP address using the following command (IP 10.0.11.8 is used as an example):

     ```
     Netif Bind logical0 10.0.11.8/16
     ```

     The physical port that was bound second (i.e., Port1) should not have an IP address assigned to it.
5. The `Netif Setlogical` command controls parameters of operation. For example, you can select whether NIC failover continues to use the standby port after active port failure (`Activebackup` is 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 viewed using the **Logs/Reports**-related administration pages (**Home > Logs/Reports**). Currently the Log command in the CLI (and the 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 using telnet, and observe messages in the system log.

Using Domain Keys Identified Mail Security

The Domain Keys Identified Mail (DKIM) protocol provides email authentication that uses public-key cryptography and key server technology to permit verification of the source and contents of messages by either Mail Transfer Agents (MTAs) or Mail User Agents (MUAs).

DKIM lets a domain owner claim ownership of messages claiming to be from that domain. DKIM either validates incoming messages, signs outgoing messages, or both, for a domain, and can mark them accordingly. DKIM provides two validation functions:

- Signing - for messages originating from the current domain, which adds one of two headers to a message; `DKIM-Signature` or `X-Mirapoint-DKIM`.
- Verification - for messages received by the current domain, if the verify option action is set to tag verified messages, an `X-Mirapoint-DKIM` header is added a message.

When verification is enabled, an `MTA.DKIM.ACTION` message is logged whenever a message is processed for DKIM signature verification. The log message includes the action taken, Message-ID, Queue-ID, and any associated errors.

DKIM must be configured using the command-line interface (CLI). For more information about the `DKIM` command and its various CLI sub-commands, see the *Mirapoint Administration Protocol Reference* and the *Mirapoint MOS Configuration Guide*.

Managing Certificates

Mirapoint offers SSL server certificates and access to a Certificate Authority (CA) or Trusted Third Party. Digital certificates are a service that you can provide to connecting users so they know they are connecting to the correct server. The process uses public key cryptography.

The **Certificates** page (**Home > Security > Certificates**) provides information on currently installed certificates and the options to download your current certificate or install a new certificate.

If setting the SSL version, cipher suite, or SMTPS, is desired, see the *Mirapoint Administration Protocol Reference*.

Additional information about certificates is provided in the following sections:

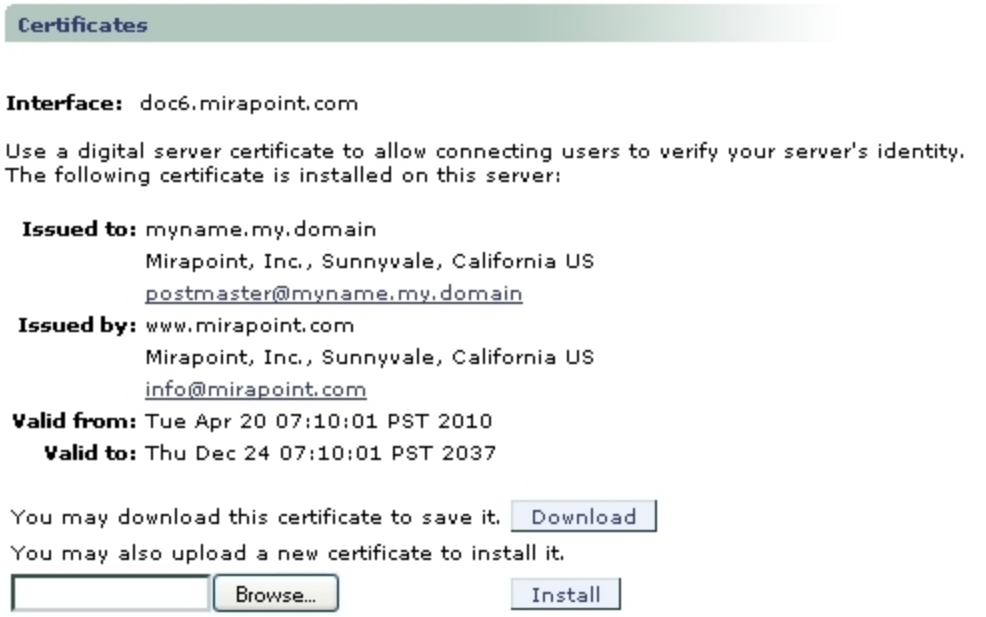
- Viewing Installed Certificate Information below
- Downloading and Installing Certificates on the facing page
- Editing and Downloading a Certificate Signing Request on page 99
- Viewing and Installing an Intermediate CA Certificate on page 100
- Selecting the Certificate Interface on page 101
- Recovering a Certificate on page 101

Viewing Installed Certificate Information

To view installed certificate information:

1. Go to **Home > Security > Certificates**.

   The **Certificates** page appears.



2. The following fields are displayed if a certificate is already installed on your appliance:
   - **Issued to**: To whom the certificate was issued.
   - **Issued by**: From whom the certificate was issued.
   - **Valid from**: The date the certificate was issued.
   - **Valid to**: The date the certificate expires.

Downloading and Installing Certificates

If you have already obtained a certificate you can download it to save it.

To download a certificate:

1. Go to **Home > Security > Certificates**.

   The **Certificates** page appears.

2. Click **Download**.

   A dialog box appears. You can then open the certificate or save it to a directory.

To install a certificate:

1. Go to **Home > Security > Certificates**.

   The **Certificates** page appears.

2. In the text field, type in the pathname with the filename of the certificate or click **Browse** and navigate to the file.
3. Click **Install**.

Editing and Downloading a Certificate Signing Request

A Certificate Signing Request (CSR) is a text file generated by a web server that contains the following information:

- Information about the organization (i.e., organization name, country, etc.).
- The web server's public key.

Use the **Certificate Signing Request** page (**Home > Security > Certificates > Certificate Signing Request**) to view this information or to generate a new certificate request by modifying the information.

To edit a CSR:

1. Go to **Home > Security > Certificates > Certificate Signing Request**.

   The **Certificate Signing Request** page appears.

2. Modify the necessary text fields under the **Subject** and **Issuer** columns within the table for the following rows:

- **Common Name**
- **E-mail Address**
- **Organization/Company**
- **Organizational Unit/Department**
- **Locality/City**
- **State**
- **Country**

3. Click **Ok**.

You can also download the CSR form and save it for future certificate requests.

To download the CSR form:

1. Go to **Home > Security > Certificates > Certificate Signing Request**.

   The **Certificate Signing Request** page appears.

2. Click **Download**.

   A dialog box appears. You can then open the form or save it to a directory.

Viewing and Installing an Intermediate CA Certificate

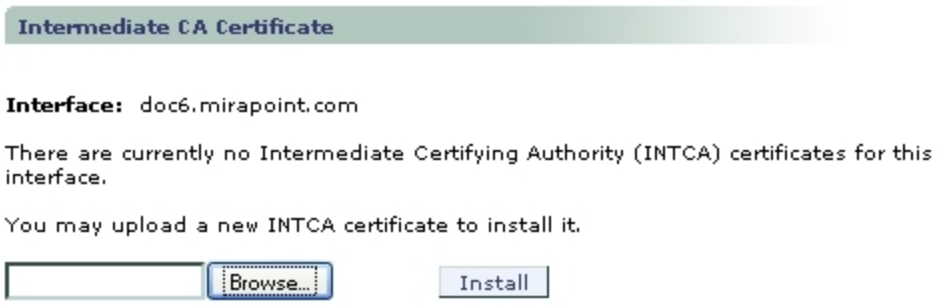
The appliance also accepts SSL certificates that are signed by an Intermediate CA (i.e., chained root certificates). However, Intermediate CAs are not implicitly trusted by all web browsers, so you must install the proper Intermediate CA Certificate in order to avoid web browser errors.

You can use the **Intermediate CA Certificate** page (**Home > Security > Certificates > Intermediate CA Certificate**) or the `ssl setintca` command in the command-line interface (CLI) to install or view the Intermediate Certifying Authority (INTCA) certificate. For more information, see the *Mirapoint Administration Protocol Reference* or the Mirapoint Support Knowledge Base.

To install an intermediate CA certificate:

1. Go to **Home > Security > Certificates > Intermediate CA Certificate**.

   The **Intermediate CA Certificate** page appears.



2. In the text field, type in the pathname with the filename of the intermediate certificate or click **Browse** and navigate to the file.
3. Click **Install**.

Selecting the Certificate Interface

Use the **Select Interface** page (**Home > Security > Certificates > Select Certificate**) to select which interface the certificate should apply to.

To select which interface the certificate applies to:

1. Go to **Home > Security > Certificates > Select Certificate**.

   The **Select Certificate** page appears.

2. In the **Interface** text field, type in the fully-qualified domain name (FQDN) or the IP address of the interface.
3. Click **Set**.

   If the text field is left blank, the certificate operates on the primary system interface.

Recovering a Certificate

You might need to recover a certificate after a disaster recovery. Use the **Recover Certificate** page (**Home > Security > Certificates > Recover Certificate**) to recover a certificate from a certain interface. A message displays if there are no available certificates to recover.

Managing SSL Connections

Secure Sockets Layer (SSL) is a protocol designed to provide encrypted communications on the Internet. HTTPS, IMAPS, and POPS are some protocols used over SSL. Mirapoint uses SSL for secure connections to WebMail Direct and the Administration Suite. For more information on SSL, see the *Mirapoint MOS Configuration Guide*.

If want to set the SSL version, cipher suite, or SMTPS, see the *Mirapoint Administration Protocol Reference*.

Specifying SSL Connections

You can specify which connections on your network use **SSL** or **Cleartext**. Mirapoint appliances support incoming and outgoing SSL for **Admin** (Administration Protocol only), **IMAP**, **POP**, **SMTP**, and **HTTP** (depending on licensing). IMAP and POP SSL connections can be configured with message proxies on the **IMAP** (**Home > System > Services > IMAP**) or **POP** pages (**Home > System > Services > POP**).

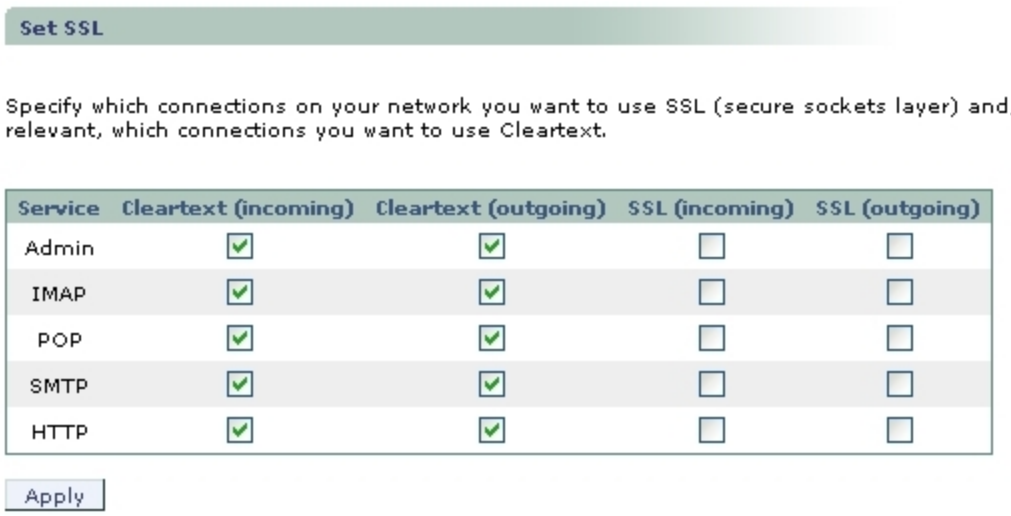
SMTP SSL connections through the AUTH login can be configured on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**). HTTP SSL connections with LDAP proxy can be configured on the HTTP service's **Main Configuration** page (**Home > System > Services > HTTP > Main Configuration**). For more information, see Managing the SMTP Service on page 42 and Managing the HTTP Service on page 35.

Outgoing SSL is also available for LDAP through the command-line interface (CLI). For more information, type `Help About Ldap` in the CLI. You can also set CLI connections to use SSH on the Administration service's **Main Configuration** page (**Home > Services > Administration > Main Configuration**). For more information, see Managing the Administration Service on page 30.

To specify SSL for each connection type:

1. Go to **Home > Security > SSL**.

   The **Set SSL** page appears.



2. Within the table, select the checkbox next to the **Service** (i.e., connection type) that will use SSL.
3. Click **Apply**.

HTTP connections with SSL display a **Cleartext/Secure** link on the login page. When the **Secure** link is clicked, the connection uses SSL. Administration Protocol, IMAP, and POP connections with SSL prompt you to accept a certificate before completing the connection. Setting SMTP connections to use SSL enables the `Smtp Set Security Starttls` command, however, you still need to issue the command from the CLI. For more information, type `Help Smtp Set Security` in the CLI and see the *Mirapoint Administration Protocol Reference*.

Specifications made on the **Set SSL** page are instantiated on the service-related administration pages (**Home > System > Services**), and vice versa.

If you are adjusting the SSL connections on a RazorGate, be sure to remember what the supported connections are for the message store (e.g., Message Server) so that you can properly configure your RazorGate to support those connections. For example, if your message store does not allow incoming cleartext connections, then you need to make sure that your proxy (e.g., RazorGate) does not send outbound messages in cleartext to that message store.

When you change the name of an appliance (i.e., hostname or DNS domain name), the appliance regenerates its certificate and email clients display new trusted certificate warning messages. The warnings displayed and their wording depends on the email client used.

Managing Trusted Admins

For security, you can specify certain trusted IP addresses, so only users logging into the Administration service from these addresses are granted administration privileges. Once a Trusted Admin IP address is specified, if you are connect from a non-trusted IP address, then the administration pages do not work. For example, if you specified a single address (such as 192.168.0.1) as your only trusted IP address, someone logging in as Administrator from any other address would not be granted administrator privileges, despite the login name and correct password.

If you do not specify any trusted IP addresses, administration access is allowed from any host.

Additional information about Trusted Admins is provided in the following sections:

- About Trusted Network Specifiers below
- Specifying a Trusted Admin List on the facing page

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 of:

`dotted-quad/mask-bits`

Where `dotted-quad` is an IP address in four-part 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 quad must match. If mask-bits is 16, the first two quads must match, and so forth.

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. For example, if `192.18.0.0/24` is the only trusted network specifier, a client connecting from `192.18.0.76` is granted access (the first three quads match), but a client connecting from `192.18.5.76` is denied access (the third quad does not match).

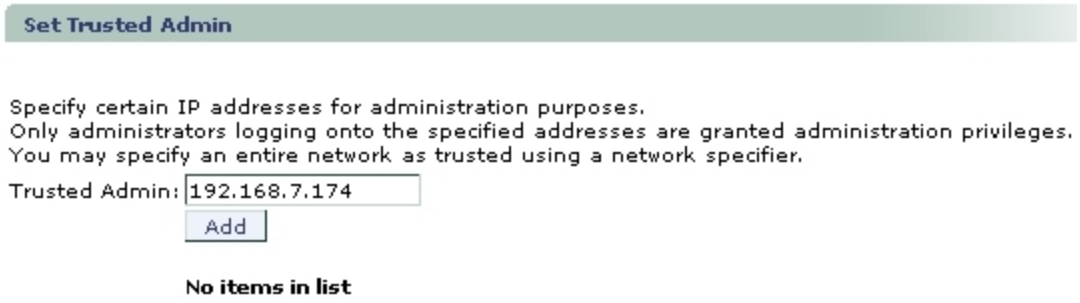
Specifying a Trusted Admin List

The Trusted Admin specifications you make here are instantiated on the **Set Trusted Admin** page (**Home > System > Services > Administration > Trusted Admin**) and vice versa.

To add a Trusted Admin:

1. Go to **Home > Security > Trusted Admin**.

   The **Set Trusted Admin** page appears.



2. In the **Trusted Admin** text field, type the IP address of the network to which you want to restrict administration activity. You can use a network specifier. For more information, see About Trusted Network Specifiers on previous page.
3. Click **Add**.

The Trusted Admin list is updated with the new network and administration activity can only take place on that network. If you have not already added your client, you are prompted to do so before any other network can be specified, this prevents accidental lock-out.

To remove a Trusted Admin:

1. Go to **Home > Security > Trusted Admin**.

   The **Set Trusted Admin** page appears.

2. Select the appropriate checkbox from the list.
3. Click **Remove**.

   A confirmation page appears.

4. Click **Remove**.

Managing Antivirus Scanning

The antivirus scanning utility searches incoming and outgoing messages for viruses. Messages are scanned before leaving the mail queue. Antivirus scanning can be performed at any stage of the mail stream where antivirus is turned on. The scanner can use up to three engines to catch viruses. How many antivirus engines are available to you depends on your licensing. Currently, Mirapoint offers three antivirus solutions:

- Sophos - A signature-based antivirus methodology. Within hours from the time a virus appears on the Internet, Sophos has added it to its pattern files. Sophos updates should, therefore, be scheduled at the briefest time setting allowed.
- F-Secure - A signature-based antivirus methodology. F-Secure also generally adds viruses to its pattern files within hours of their appearance. F-Secure updates should also take advantage of the briefest time setting.
- RAPID - A predictive-based antivirus methodology.

The **About Antivirus** page (**Home > Antivirus**) provides the following links:

- Sophos Antivirus - Provides links to the Sophos antivirus engine's configuration pages.
- F-Secure Antivirus - Provides links to the F-Secure antivirus engine's configuration pages.
- RAPID Antivirus - Provides links to the RAPID antivirus engine's configuration pages.

Additional information about antivirus scanning is provided in the following sections:

- About Signature-based Antivirus below
- About Predictive-based Antivirus on the facing page
- How Antivirus Features Are Applied on the facing page
- About Cleanable vs. Non-cleanable Viruses on page 107
- How Antivirus Quarantine Works on page 107

About Signature-based Antivirus

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. So, it is important to schedule pattern file updates as often as possible. You can schedule automatic updates for Sophos and F-Secure on their respective **Antivirus Update** pages. For more information, see Updating Sophos Antivirus on page 112 and Updating F-Secure Antivirus on page 117.

About Predictive-based Antivirus

RAPID Antivirus uses an entirely different methodology that is predictive-based. 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 Antivirus does not use a pattern file but requires a periodic engine update to counter emerging threats.

RAPID does not attempt to verify that potential virus outbreaks are, in fact, viruses, so the only action option for RAPID Antivirus is quarantine. An administrator with the **Quarantine Administrator** role, can examine those messages quarantined by RAPID to make sure that they are truly viruses.

How Antivirus Features Are Applied

Mirapoint recommends running at least one signature-based antivirus engine along with the predictive-based antivirus engine (i.e., RAPID Antivirus). You should *not*run the predictive-based antivirus engine by itself. RAPID Antivirus *must* be used in conjunction with a signature-based antivirus engine (i.e., Sophos or F-Secure).

When a signature-based and predictive-based antivirus engines are enabled on the appliance, antivirus scanning is applied in the following order:

1. Signature-based antivirus (Sophos or F-Secure Antivirus) scans the message.

   If the message is quarantined by Sophos or F-Secure Antivirus and you have an quarantine email address specified on the **Antivirus Configuration** page (**Home > Antivirus > *virus scanner* > Configuration**) , the appliance sends a copy of the original message, as an attachment, to the specified quarantine email address for later analysis. After a copy is sent, the appliance proceeds to handle the original message as specified by other settings.

2. Predictive-based antivirus (RAPID Antivirus) scans the message.

   If the message is quarantined by RAPID Antivirus, the appliance takes the original message and sets it aside for a period of time in the quarantine folder specified on the **Antivirus Configuration** page (**Home > Antivirus > RAPID Antivirus > Configuration**) . After the delay period has elapsed, the message is re-scanned by the signature-based antivirus engine (unless the Quarantine Administrator manually delivers the message).

   Setting aside the original message allows the appliance to delay messages that might contain newly-created viruses. This allows the signature-based antivirus engine time to provide an update in response to the new threat.

   For more information, see How Antivirus Quarantine Works on next page.

The X-headers within the message envelope helps differentiate what processes have been applied to the message. For example:

- If a virus was not found by any antivirus engine, then no headers are applied to the message.
- If a virus was found by the signature-based antivirus engine, then the `X-Mirapoint- Virus: VIRUSFOUND` header is applied to the message.
- If the message is quarantined by RAPID Antivirus, re-scanned by a signature-based antivirus engine, and a virus was found during the res-can, then the `X-Mirapoint-Virus: VIRUSFOUND` and `X-Mirapoint-RAPID: potential virus`headers are applied to the message.
- If the message is quarantined by RAPID Antivirus, re-scanned by a signature-based antivirus engine, and a virus was not found during the re-scan, then only the `X-Mirapoint-RAPID` header is applied to the message.

For more information on X-headers, see About Message Envelopes and Headers on page 238.

About Cleanable vs. Non-cleanable Viruses

Antivirus scanning configuration requires making specifications for actions to be taken on infected attachments, non-cleanable infected attachments, and selecting a quarantine email address. Antivirus scanning 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 appliance tries to automatically clean cleanable viruses if you select one of the **Auto Clean** options. For more information, see Configuring Sophos Antivirus on page 109 and Configuring F-Secure Antivirus on page 114.

How Antivirus Quarantine Works

The antivirus quarantine process typically works differently than the content filtering quarantine process. The address you specify as the signature-based antivirus engine's (i.e., Sophos or F-Secure) quarantine email address, i.e., **Antivirus Quarantine E-mail Address**, receives a virus quarantine message, which contains a copy of the original virus-contaminated message as an attachment. So, the message can be examined and deleted, but should not be released from the quarantine. Messages quarantined by the predictive-based antivirus engine (RAPID) potentially contains live viruses, so they are safely released for re-scanning by one of the signature-based scanners after a delay period has elapsed.

For Sophos or F-Secure Antivirus, the antivirus quarantine email address should either be a local address or an address that does not subject the message to more antivirus scanning. For these signature-based antivirus engines, the quarantine email 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.

However, for RAPID Antivirus, it is essential that you quarantine messages to an account that has the **Quarantine Administrator** role. This is important for RAPID-scanned messages because predictive scanning is not based on identified viruses but, rather, on potential virus outbreaks. Therefore, you want those messages to be examined and possibly returned to the mail stream.

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 Managing Quarantine Messages on page 124.

The default RAPID Antivirus quarantine address, `user.administrator.RapidAV`, sends messages to the `RapidAV` sub-folder of the administrator's WebMail on that appliance (the sub-folder is automatically created when the first message is received). An administrator can examine all messages quarantined by the predictive-based antivirus engine for investigative reasons and possibly return selected messages to the mail stream using the **Deliver** and/or **Virus Scan** actions. If the **Virus Scan** option is used, the messages will be scanned by one of the signature-based engines

Keep in mind that the administrator should use the **Virus Scan** option after a time period that allows for any updates to occur on the signature-based antivirus engine. 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 6 hours after the message was first quarantined. In this way, the signature-based engine(s) have time to discover the virus, add it to their database, and your appliance has time to install the update. Automatic release of RAPID-quarantined messages occurs 8 hours after quarantining. This setting can be changed using the `CLI Antivirus Set Quarantinedelay` command. For more information, see the *Mirapoint Administration Protocol Reference*.

When using the quarantine filter action, Mirapoint recommends using a local address to prevent the mail from getting re-scanned.

For more information about automatically releasing quarantined messages, type `Help About Antivirus` in the command-line interface (CLI). For information about the content filtering quarantine action, see Creating Advanced Content Filters on page 173.

Managing Sophos Antivirus

Use the Sophos Antivirus administration pages to configure the antivirus engine, including setting up notifications and updates. To better understand how Sophos works, see About Signature-based Antivirus on page 105.

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

The **About Sophos Antivirus** page (**Home > Antivirus > Sophos Antivirus**) provides the following links:

- Configuration - Specify what attachments should be scanned, whether the quarantine function should be used and a quarantine address where messages with viruses can be sent, and what actions the system should take upon finding a virus.
- Notifications - Specify who should get notified when and with what information.
- Updates - Specify how often the utility should get updated virus pattern information. You can also choose to perform an immediate, manual update.

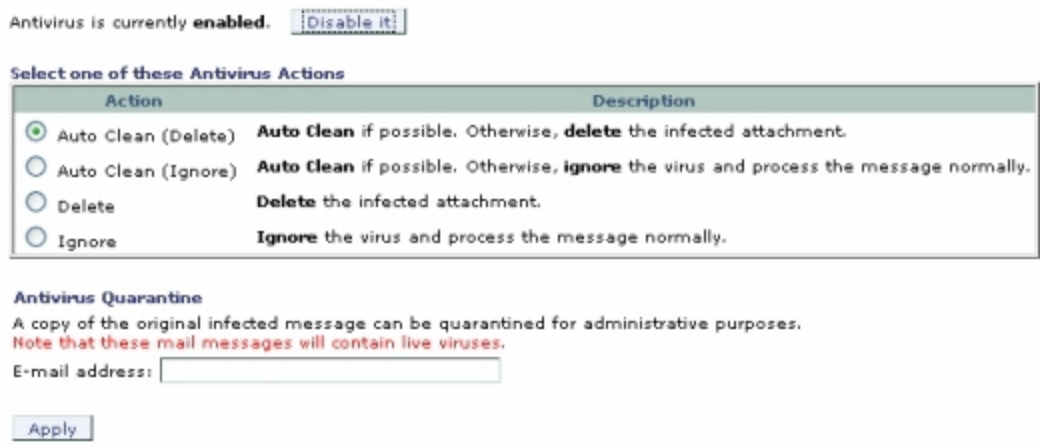
Configuring Sophos Antivirus

Sophos Antivirus scanning configuration requires making specifications for actions to be taken on infected attachments, non-cleanable infected attachments, and specifying a quarantine email address.

To configure Sophos Antivirus scanning:

1. Go to **Home > Antivirus > Sophos Antivirus > Configuration**.

   The **Antivirus Configuration** page appears.



2. If the antivirus scanning is not already enabled, click **Enable it**.

   Antivirus scanning must be enabled in order to configure the utility.

3. In the **Select one of these Antivirus Actions** area, choose one of the following settings:

   - **Auto Clean (Delete)** - The utility attempts to clean the attachment of the virus. If the attachment cannot be cleaned, it is deleted. The appliance 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 utility attempts to clean the attachment of the virus. If the attachment cannot be cleaned, it is ignored. The appliance logs that a virus was found and sends the message with the attachment, either cleaned or unchanged, to the intended recipient(s). Mirapoint does not recommend this option.
   - **Delete** - The appliance logs that a virus was found and sends the message with the attachment deleted, even if cleanable, to the intended recipient(s).
   - **Ignore** - The appliance logs that a virus was found and sends the message with the attachment unchanged to the intended recipient(s). Mirapoint does not recommend this option.

4. (Optional) Under the **Antivirus Quarantine** area, in the **E-mail Address** text field, specify an antivirus quarantine email address of an administrator account local to the appliance. For more information, see How Antivirus Quarantine Works on page 107.
5. Click **Apply**.

Regardless of the antivirus action selected during configuration, if a virus is found, original messages are modified with a header (`X-Mirapoint-Virus`) and a warning banner indicating that a virus was found and what action was taken (i.e., `cleaned`, `ignored`, or `deleted`). The message includes the virus name and you can go to http://www.sophos.com or http://www.f-secure.com to learn more about that virus. For more information, see About Cleanable vs. Non-cleanable Viruses on page 107.

If you specified a quarantine email address, your selected actions are taken and any message found to contain a virus is forwarded to the specified address.

An important step in the configuration process is setting the updates schedule. New viruses are discovered each day and added to the pattern file against which the scanning is done. Setting a daily updates schedule ensures that the utility operates at maximum protection. For more information, see Updating Sophos Antivirus on page 112.

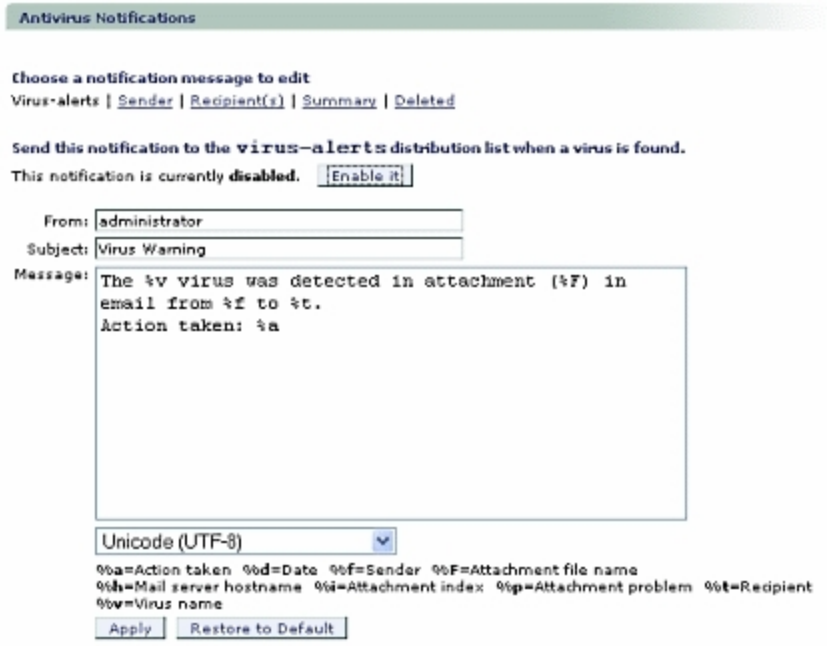
Configuring Sophos Antivirus Notifications

Antivirus notifications must be specified in order for notices to be sent to the correct parties.

To specify Sophos Antivirus scanning notifications:

1. Go to **Home > Antivirus > Sophos Antivirus > Notifications**.

   The **Antivirus Notifications** page appears.



2. Under the **Choose a notification message to edit** area, select one of the following notification types:

- **Virus-alerts** - When a virus is detected, this notification is sent to the **virus-alerts** distribution list (DL). This is selected by default.
- **Sender** - When a virus is detected, this notification is sent to the message sender.
- **Recipient(s)** - When a virus is detected, this notification is sent to the message recipient(s).

The following two notification types allow you to customize what is inserted in the notification(s) 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 into the top of the body of the message.
- **Deleted** - When a message containing a virus is delivered with the virus deleted, either **Auto Clean (Delete)** or **Delete** was the action, this notification is inserted in place of the deleted attachment.

3. For each of the notification types, click **Enable it** to turn on the notification.

   The notification type must be enabled before it can be sent.

4. 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 (This might include blind carbon copy (Bcc) recipients).

     Use the `%t` code with the administrator notification message. Do *not* add it to **Sender** or **Recipient(s)** notification types, because doing so could expose confidential information about distribution list (DL) memberships or Bcc recipients.

   - `%v` (virus name) - The virus name and number.
5. Select a character set for the notification type from the drop-down menu. The default is **Unicode (UTF-8)**.
6. Click **Apply**.

   If you click **Restore to Default**, your changes to the selected notification message are removed and the factory set message re-displays. Clearing the text fields also resets the notification to the default message.

Updating Sophos Antivirus

Antivirus updates ensure optimal performance over time. Use the **Antivirus Updates** page (**Home > Antivirus > Sophos Antivirus > Updates**) to set up a schedule. This is an important part of the configuration process, as new viruses are discovered each day and added to the pattern file against which the scanning is done.

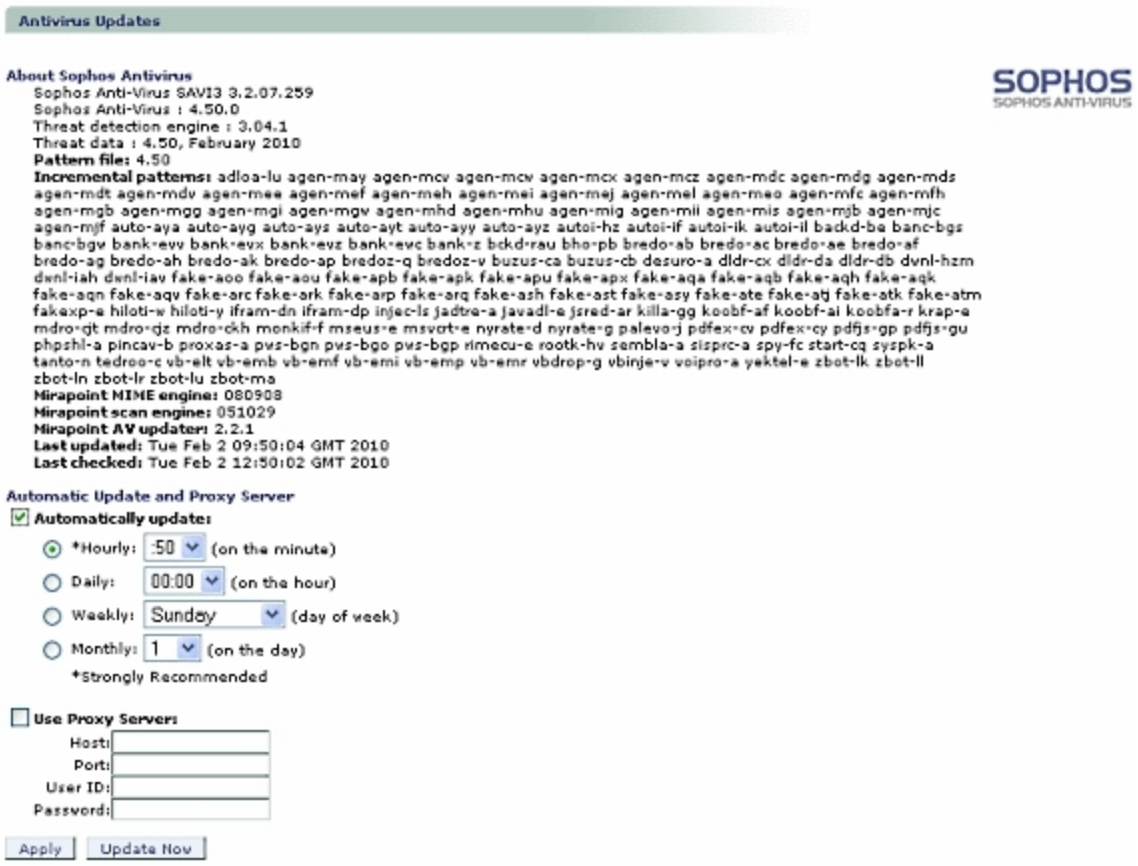
You should update the virus scanning pattern on an hourly basis. New viruses are discovered each week and added to the pattern file against which the scanning utility operates at maximum protection. Updating the pattern file does not inhibit appliance performance.

Checking Current Version Information

To check the antivirus version information:

1. Go to **Home > Antivirus > Sophos Antivirus > Updates**.

   The **Antivirus Updates** page appears.



2. Under **About Sophos Antivirus**, the following information as well as the version number of that antivirus pattern file is displayed:
   - **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 MIME engine**: The version of the current Multipurpose Internet Mail Extension interpreter.
   - **Mirapoint scan engine**: The version of the current scan engine.
   - **Mirapoint AV updater**: The version of the current updater.
   - **Last updated**: The date of the utility's last update.
   - **Last checked**: The date the utility was last checked for an update.

Getting an Immediate Sophos Antivirus Update

To get an immediate antivirus update:

1. Go to **Home > Antivirus > Sophos Antivirus > Updates**.

   The **Antivirus Updates** page appears.

2. Click **Update Now**.

The utility immediately accesses and updates itself with the latest virus pattern file. The page redisplays with a message indicating that the update is complete.

Setting Up Automatic Sophos Antivirus Updates

To set up automatic antivirus updates:

1. Go to **Home > Antivirus > Sophos Antivirus > Updates**.

   The **Antivirus Updates** page appears.

2. Under the **Automatic Update and Proxy Server** area, select the **Automatically update** checkbox and select one of the following options:
   - **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.

Mirapoint recommends using the **Hourly** option to ensure that the utility operates at maximum protection.

3. (Optional) If you use a proxy server to reach the Internet, select the **Use Proxy Server** checkbox. In the appropriate text fields, type the **Host** name, **Port** number, **User ID**, and **Password** required by your proxy for access to the Internet. Once applied, the utility will retrieve the updated pattern file via the specified proxy.
4. Click **Apply**.

Managing F-Secure Antivirus

Use the F-Secure Antivirus administration pages to configure the antivirus engine, including setting up notifications and updates. To better understand how F-Secure works, see About Signature-based Antivirus on page 105.

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

The **About F-Secure Antivirus** page (**Home > Antivirus > F-Secure Antivirus**) provides the following links:

- Configuration - Specify what attachments should be scanned, whether the quarantine function should be used and a quarantine address where messages with viruses can be sent, and what actions the system should take upon finding a virus.
- Notifications - Specify who should get notified when and with what information.
- Updates - Specify how often the utility should get updated virus pattern information. You can also choose to perform an immediate, manual update.

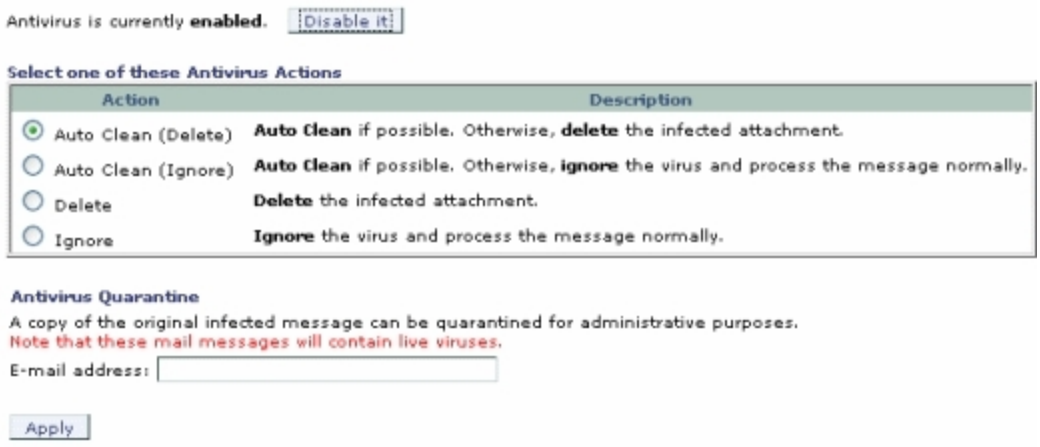
Configuring F-Secure Antivirus

Configuring F-Secure antivirus scanning requires making specifications for actions to be taken on infected attachments, non-cleanable infected attachments, and specifying a quarantine email address.

To configure F-Secure Antivirus scanning:

1. Go to **Home > Antivirus > F-Secure Antivirus > Configuration**.

   The **Antivirus Configuration** page appears.



2. If the antivirus scanning is not already enabled, click **Enable it**.

   Antivirus scanning must be enabled in order to configure the utility.

3. In the **Select one of these Antivirus Actions** area, choose one of the following settings:

   - **Auto Clean (Delete)** - The utility attempts to clean the attachment of the virus. If the attachment cannot be cleaned, it is deleted. The appliance 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 utility attempts to clean the attachment of the virus. If the attachment cannot be cleaned, it is ignored. The appliance logs that a virus was found and sends the message with the attachment, either cleaned or unchanged, to the intended recipient(s). Mirapoint does not recommend this option.
   - **Delete** - The appliance logs that a virus was found and sends the message with the attachment deleted, even if cleanable, to the intended recipient(s).
   - **Ignore** - The appliance logs that a virus was found and sends the message with the attachment unchanged to the intended recipient(s). Mirapoint does not recommend this option.

5. (Optional) Under the **Antivirus Quarantine** area, in the **E-mail Address** text field, specify an antivirus quarantine email address of an administrator account local to the appliance. For more information, see How Antivirus Quarantine Works on page 107.
6. Click **Apply**.

   Regardless of the antivirus action selected during configuration, if a virus is found, original messages are modified with a header (`X-Mirapoint-Virus`) and a warning banner indicating that a virus was found and what action was taken (i.e., `cleaned`, `ignored`, or `deleted`). The message includes the virus name and you can go to http://www.sophos.com or http://www.f-secure.com to learn more about that virus. For more information, see About Cleanable vs. Non-cleanable Viruses on page 107.

   If you specified a quarantine email address, your selected actions are taken and any message found to contain a virus is forwarded to the specified address.

An important step in the configuration process is setting the updates schedule. New viruses are discovered each day and added to the pattern file against which the scanning is done. Setting a daily updates schedule ensures that the utility operates at maximum protection. For more information, see Updating F-Secure Antivirus on next page.

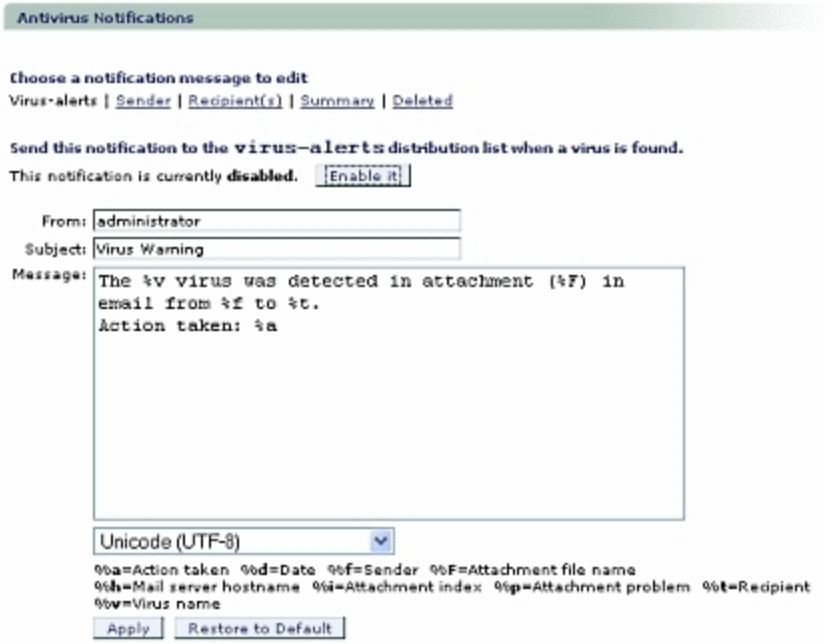
Configuring F-Secure Antivirus Notifications

Antivirus notifications must be specified in order for notices to be sent to the correct parties.

To specify F-Secure Antivirus scanning notifications:

1. Go to **Home > Antivirus > F-Secure Antivirus > Notifications**.

   The **Antivirus Notifications** page appears.



2. Under the **Choose a notification message to edit** area, select one of the following notification types:
   - **Virus-alerts** - When a virus is detected, this notification is sent to the **virus-alerts** distribution list (DL). This is selected by default.
   - **Sender** - When a virus is detected, this notification is sent to the message sender.
   - **Recipient(s)** - When a virus is detected, this notification is sent to the message recipient(s).

   The following two notification types allow you to customize what is inserted in the notification(s) 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 into the top of the body of the message.
- **Deleted** - When a message containing a virus is delivered with the virus deleted, either **Auto Clean (Delete)** or **Delete** was the action, this notification is inserted in place of the deleted attachment.

3. For each of the notification types, click **Enable it** to turn on the notification.

   The notification type must be enabled before it can be sent.

4. 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 (This might include blind carbon copy (Bcc) recipients).

Use the `%t` code with the administrator notification message. Do *not* add it to **Sender** or **Recipient(s)** notification types, because doing so could expose confidential information about distribution list (DL) memberships or Bcc recipients.

   - `%v` (virus name) - The virus name and number.

5. Select a character set for the notification type from the drop-down menu. The default is **Unicode (UTF-8)**.
6. Click **Apply**.

   If you click **Restore to Default**, your changes to the selected notification message are removed and the factory set message re-displays. Clearing the text fields also resets the notification to the default message.

Updating F-Secure Antivirus

Antivirus updates ensure optimal performance over time. Use the **Antivirus Updates** page (**Home > Antivirus > F-Secure Antivirus > Updates**) to set up a schedule. This is an important part of the configuration process, as new viruses are discovered each day and added to the pattern file against which the scanning is done.

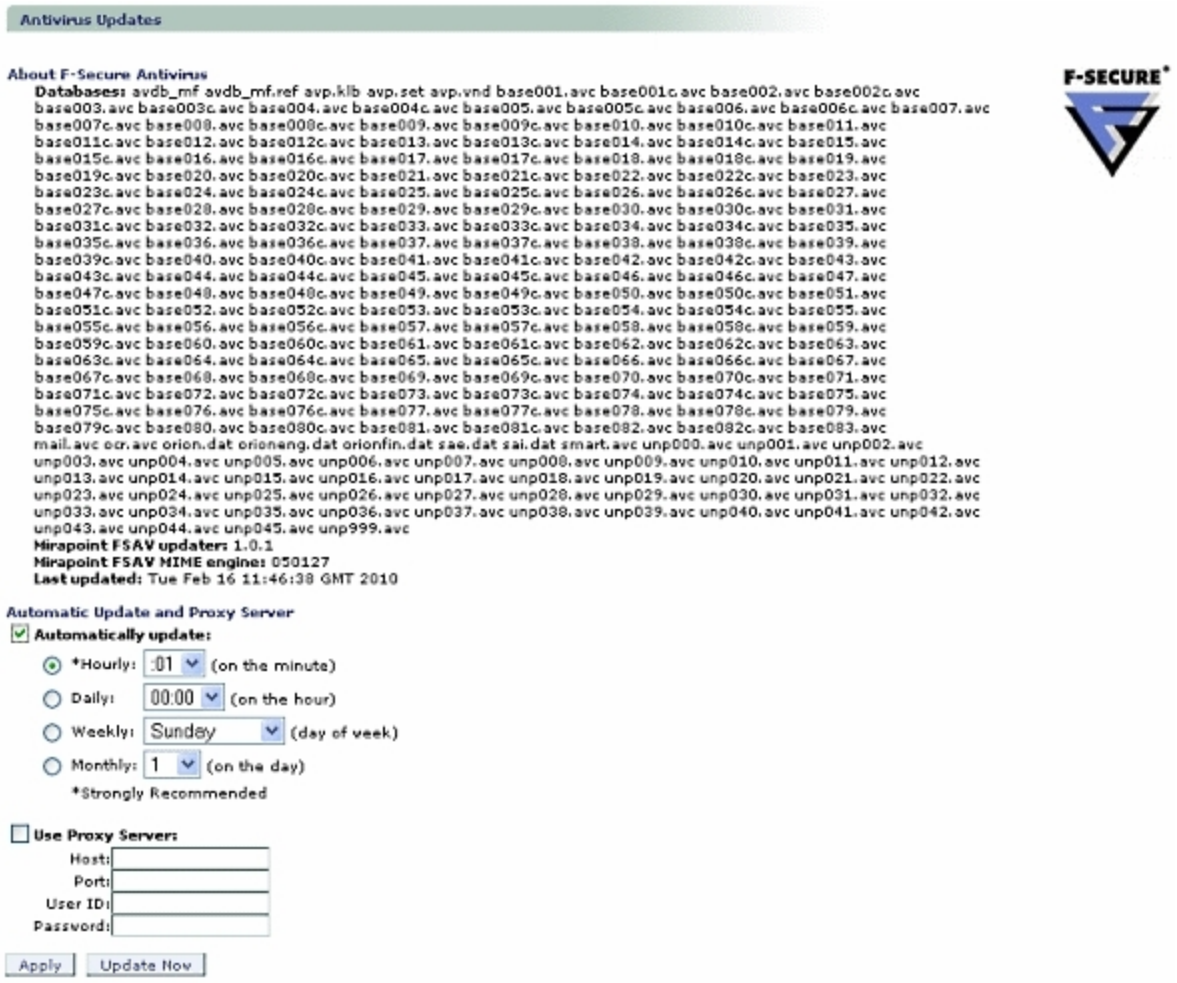
You should update the virus scanning pattern on an hourly basis. New viruses are discovered each week and added to the pattern file against which the scanning is done. Scheduling hourly updates ensures that the scanning utility operates at maximum protection. Updating the pattern file does not inhibit appliance performance.

Checking Current Version Information

To check the antivirus version information:

1. Go to **Home > Antivirus > F-Secure Antivirus > Updates**.

   The **Antivirus Updates** page appears.



2. Under **About F-Secure Antivirus**, the following information as well as the version number of that antivirus pattern file is displayed:

   - **Databases**: The viruses that have been added to the utility with each update it has performed since the last version was obtained. Note: This value only displays when applicable.
   - **Mirapoint FSAV updater**: The version of the current updater.
   - **Mirapoint FSAV MIME engine**: The version of the current MIME (Multipurpose Internet Mail Extension) interpreter.
   - **Last updated**: The date of the utility's last update.

Getting an Immediate F-Secure Antivirus Update

To get an immediate antivirus update:

1. Go to **Home > Antivirus > F-Secure Antivirus > Updates**.

   The **Antivirus Updates** page appears.

2. Click **Update Now**.

The utility immediately accesses and updates itself with the latest virus pattern file. The page redisplays with a message indicating that the update is complete.

Setting Up Automatic F-Secure Antivirus Updates

To set up automatic antivirus updates:

1. Go to **Home > Antivirus > F-Secure Antivirus > Updates**.

   The **Antivirus Updates** page appears.

2. Under the **Automatic Update and Proxy Server** area, select the **Automatically update** checkbox and select one of the following options:

   - **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.

Mirapoint recommends using the **Hourly** option to ensure that the utility operates at maximum protection.

3. (Optional) If you use a proxy server to reach the Internet, select the **Use Proxy Server** checkbox. In the appropriate text fields, type the **Host** name, **Port** number, **User ID**, and **Password** required by your proxy for access to the Internet. Once applied, the utility will retrieve the updated pattern file via the specified proxy.
4. Click **Apply**.

Managing RAPID Antivirus

Use the RAPID Antivirus administration pages to configure the RAPID antivirus scanner, including setting up notifications and updates. RAPID Antivirus uses IP Addresses to determine a potential virus outbreak, so it is important that your Relay List of acceptable IP Addresses is up-to-date so as not to incur any unnecessary delays. For more information about how RAPID Antivirus works, see About Predictive-based Antivirus on page 106.

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

The **About RAPID Antivirus** page (**Home > Antivirus > RAPID Antivirus**) provides the following links:

- Configuration - Specify what scoring severity should be used and a quarantine address where messages with potential viruses can be sent.
- Notifications - Specify who should get notified when and with what information.
- Updates - Specify how often the utility should get updated virus pattern information. You can also choose to perform an immediate, manual update.

Configuring RAPID Antivirus

Specifying a quarantine email address is required when configuring RAPID Antivirus scanning. The default quarantine email address, `user.administrator.RapidAV`, is a sub-folder of the administrator's WebMail account. The sub-folder is automatically created when the first quarantined message is received. You can change this default address to any valid WebMail account with the **Quarantine Administrator** role. For more information, see How Antivirus Quarantine Works on page 107.

To configure RAPID Antivirus scanning:

1. Go to **Home > Antivirus > RAPID Antivirus > Configuration**.

   The **Antivirus Configuration** page appears.

2. If the antivirus scanning is not already enabled, click **Enable it**.

   Antivirus scanning must be enabled in order to configure the utility.

3. In the **E-mail Address** text field, type the email address of an administrator account local to the appliance. You must use an account that has the **Quarantine Administrator** role assigned it.

   The default quarantine email address is a sub-folder of the administrator's WebMail account (`user.administrator.RapidAv`). However, you can use any valid address (`user.`*`username`*`.`*`folder`*) from an account with the **Quarantine Administrator** role. For more information, see How Antivirus Quarantine Works on page 107.

Automatic release of RAPID-quarantined messages occurs 8 hours after quarantining. This can be changed using the command-line interface (CLI). For more information, type `Help About Antivirus` in the CLI.

4. Click **Apply**.

   RAPID Antivirus classifies all email messages as either `No Virus`, `Low`, `Medium`, or `High` probability of virus. All message marked `Medium` or `High` are automatically quarantined to the specified email address; the others are delivered normally. 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.

An important step in the configuration process is setting the updates schedule. Setting a daily updates schedule ensures that the utility operates at maximum protection. For more information, see Updating RAPID Antivirus on the facing page.

Configuring RAPID Antivirus Notifications

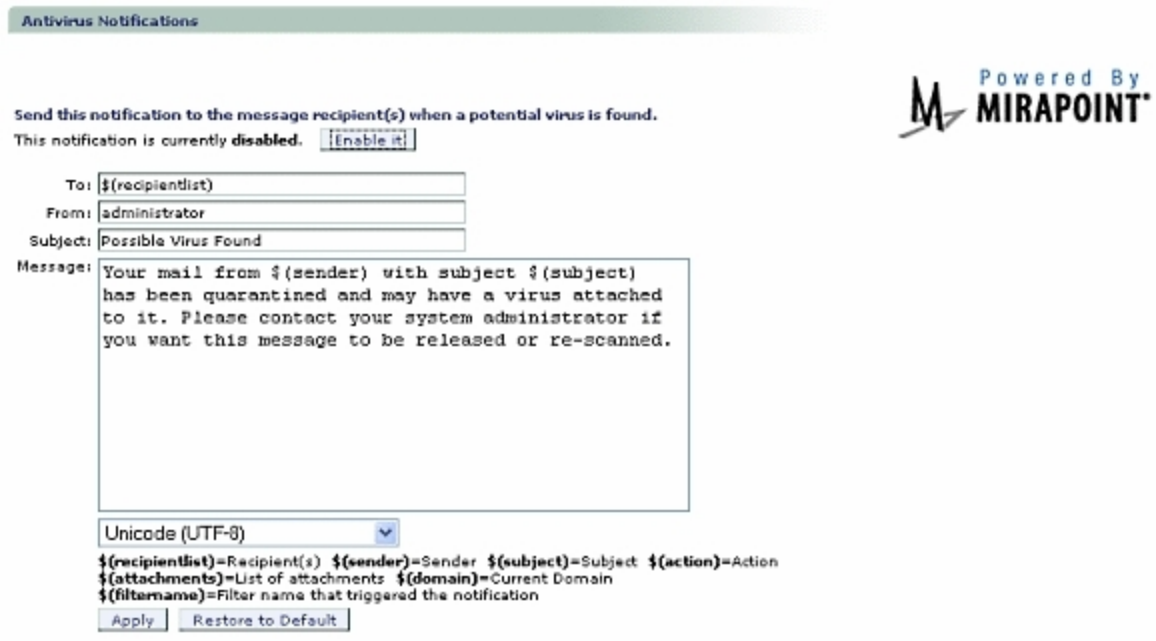
Mirapoint highly recommends that RAPID Antivirus notifications be configured to let users know that their email is being quarantined due to a potential virus.

All messages should remain in quarantine for six to eight hours to give the signature-based engines time to update their pattern files. RAPID will quarantine most un-encrypted messages with attachments, so the RAPID Antivirus Quarantine Administrator can expect to receive periodic requests, from notified recipients, to release a message.

To specify RAPID Antivirus scanning notifications:

1. Go to **Home > Antivirus > RAPID Antivirus > Notifications**.

   The **Antivirus Notifications** page appears.



2. Click **Enable it** to turn on notifications.

   This option must be enabled before notification messages can be sent.

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:

   - `$(recipientlist)` Recipient(s) - The To header of the recipient(s) of the message.
   - `$(sender)` Sender - The From header of the sender of the message.
   - `$(subject)` Subject - The Subject line of the message.
   - `$(action)` Action - This will always be `Quarantined`.
   - `$(attachments)` List of attachments - The names of any attachments to the message.
   - `$(domain)` Current Domain - The domain in which the RAPID Antivirus scanning was done.
   - `$(filtername)` Filter name - The filter that triggered the notification.

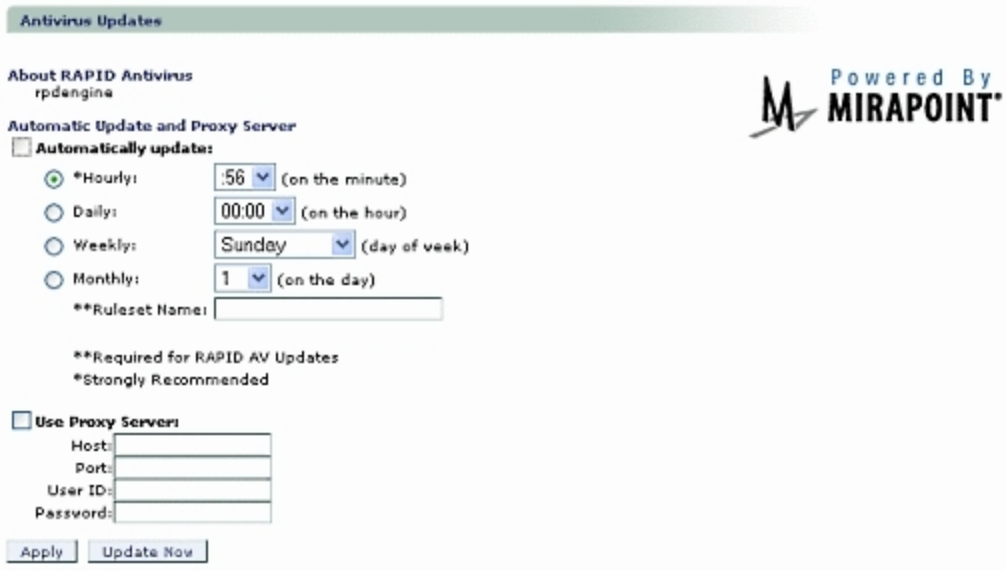
4. Click **Apply**.

   If you click **Restore to Default**, your changes to the selected notification message are removed and the factory set message re-displays. Clearing the text fields also resets the notification to the default message.

Updating RAPID Antivirus

Antivirus updates ensure optimal performance over time. Use the **Antivirus Updates** page (**Home > Antivirus > RAPID > Updates**) to set up a schedule. RAPID Antivirus 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.

Figure 13 RAPID Antivirus - Antivirus Updates Page



Checking Current Version Information

To check the antivirus version information:

1. Go to **Home > Antivirus > RAPID Antivirus > Updates**.

   The **Antivirus Updates** page appears.

2. Under **About RAPID Antivirus**, information about the current ruleset displays.

Getting an Immediate RAPID Antivirus Update

To get an immediate antivirus update:

1. Go to **Home > Antivirus > RAPID Antivirus > Updates**.

   The **Antivirus Updates** page appears.

2. Select the ruleset that you want to update.
3. Click **Update Now**.

   The utility immediately accesses and updates itself with the latest ruleset. The page redisplays with a message indicating that the update is complete.

Setting Up Automatic RAPID Antivirus Updates

To set up automatic antivirus updates:

1. Go to **Home > Antivirus > RAPID Antivirus > Updates**.

   The **Antivirus Updates** page appears.

2. Under the **Automatic Update and Proxy Server** area, select the **Automatically update** checkbox and select one of the following options:

   - **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.

Mirapoint recommends using the **Hourly** option to ensure that the utility operates at maximum protection.

3. (Optional) Specify a **Ruleset Name**.

Mirapoint occasionally adds named rulesets that you can access through the Mirapoint Technical Support website.

   The new ruleset displays in a list below. Click the ruleset's **Delete** icon (✕) to remove it.

4. (Optional) If you use a proxy server to reach the Internet, select the **Use Proxy Server** checkbox. In the appropriate text fields, type the **Host** name, **Port** number, **User ID**, and **Password** required by your proxy for access to the Internet. Once applied, the utility will retrieve an updated ruleset via the specified proxy.
5. Click **Apply**.

Managing Quarantine Messages

Use the **About Quarantine Administration** page (**Home > Quarantine**) to access the Quarantine Administrator's WebMail (`user.QuarantineAdmin` folder) and the messages sent to it by content filters using the **Send to Quarantine folder** action with that address. This address (`user.QuarantineAdmin`) can also receive RAPID antivirus emails, if so specified on the **Antivirus Configuration** page (**Home > Antivirus > RAPID Antivirus > Configuration**).

Additionally, there is an antivirus quarantine option for messages triggering the RAPID antivirus quarantine. The default RAPID quarantine address, `user.administrator.RapidAV`, sends matching messages to the WebMail `RapidAV` sub-folder of the administrator's account on that appliance. However, any administrator or quarantine administrator logging on to WebMail on a system licensed with RAPID antivirus, will now see an option, **Virus Scan**, that allows RAPID-quarantined messages to be returned to the mail stream for another scan by one of the other antivirus engines. For more information, see How Antivirus Quarantine Works on page 107.

Accessing the Quarantine Administrator's WebMail

If you have not already created the `QuarantineAdmin` user in the Setup Wizard, use the **Add Users** page (**Home > System > Users**) and add an Administrator user named `QuarantineAdmin`. The system auto-creates the `user.QuarantineAdmin` folder when the first mail that receives a filter **Send to Quarantine folder** action with `user.QuarantineAdmin` address, arrives. To access the `QuarantineAdmin` account, log in to WebMail with the login account you created or click the **Open Quarantine Administrator's WebMail** link on the **About Quarantine Administration** page. For more information, see Managing User Accounts on page 54 and the WebMail online help.

After you log in to WebMail with the account you created, the following administrative options are available:

- Use the **Delete** option to permanently delete messages from quarantine. No copy is sent to the intended recipient(s).
- Use the **Deliver** option to release messages from quarantine. They are sent to the intended recipient(s) with no indication that they were in quarantine. If you select a non-content filtering or antispam quarantined message and click **Deliver**, a message displays. Only content filtering or antispam quarantined messages can be delivered back to the mail stream.
- Use **Virus Scan** option to return RAPID antivirus quarantined messages to the mail stream to be scanned by one of the other antivirus engines. If you select a non-RAPID antivirus quarantined message and click **Virus Scan**, a message displays. Only RAPID antivirus quarantined messages can be delivered back to the mail stream for re-scanning.

These options are available for all users granted the **Quarantine Administrator** or **Administrator** role. However, the **Virus Scan** option only displays when RAPID Antivirus is licensed on the appliance.

Managing Antispam Scanning

Antispam scanning is a licensed software option. If other or additional antispam scanning is done upstream, these configurations re-write previous UCE (unsolicited commercial email) scores or lists. Antispam scanning is done before content filtering. Domain-level filters and lists are always applied before user-level filters and lists.

Antispam scanning can use one or more engines (depending on licensing) to categorize mail as junk mail (i.e, spam): Principal Edition, Premium Edition, or Signature Edition RAPID Antispam. Which antispam engine you use depends on which licenses you have applied. For more information about each engine, see Signature Edition, Principal Edition, and Premium Edition on page 130.

The **About Antispam** page (**Home > Antispam**) provides the following links:

- Configuration - Enable/disable antispam scanning, specify how severely the utility should judge incoming mail for spam, and set other defaults.
- Updates - Specify how often the utility should update spam information. You can also choose to perform a manual update that causes an immediate update.
- Allowed Senders - Specify certain senders from whom mail should never receive the configured **Junk Mail Filter** action.
- Blocked Senders - Specify certain senders from whom mail should always receive the configured **Junk Mail Filter**action.
- Allowed Mailing Lists - Specify certain recipient addresses whose mail should never receive the configured **Junk Mail Filter** action.

For more information about the Junk Mail Filter, see About the Junk Mail Filter on page 132.

- 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 antispam license.
- Reject List - Specify networks from which messages will be rejected at the SMTP prompt. Does not require an antispam license.
- RBL Host List - Specify that all incoming messages be checked against the Realtime Blackhole List (RBL) Internet service. Does not require an antispam license.
- MailHurdle - Enable/disable the MailHurdle antispam scanning utility and setup configuration options.

For information about Junk Mail Manager (JMM), see Managing Junk Mail Manager on page 155.

About Antispam Scanning

The **Antispam Configuration** page (**Home > Antispam > Configuration**) allows you to make specifications for a junk mail scanning severity threshold, as well as setting warning, explanation, and reporting options.

Additional information about antispam scanning is provided in the following sections:

- Configuring Antispam Scanning on next page
- Signature Edition, Principal Edition, and Premium Edition on page 130
  - Using MultiScan Antispam on page 131
  - About the Junk Mail Filter on page 132
- How Antispam Features Are Applied on page 132
- About Antispam Scanning and Threshold on page 133

Configuring Antispam Scanning

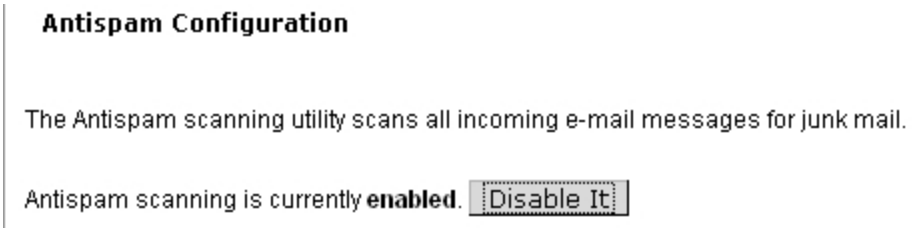
You must have a valid license before you can configure antispam scanning.

To configure antispam scanning:

After applying your license(s) for antispam, make sure that you to go the **Antispam Updates** page for that licensed engine and click **Update Now** to get the most recent files. For more information, see Updating Antispam on page 134.

1. Go to **Home > Antispam > Configuration**.

   The **Antispam Configuration** page appears.

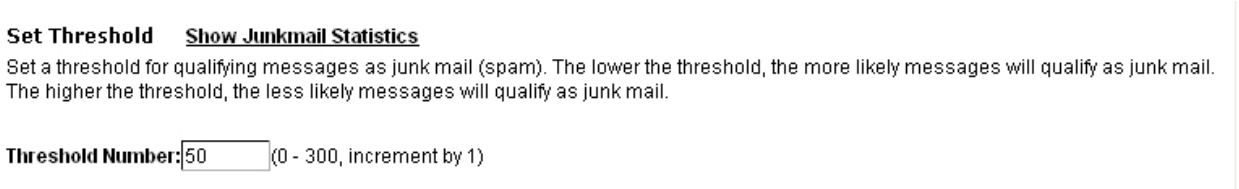
2. If the antispam scanning is not already enabled, click **Enable it**. Antispam scanning must be enabled in order to configure the utility.

   Enabling antispam scanning automatically creates a default end-user **Junk Mail Filter** accessible via WebMail. For more information, see About the Junk Mail Filter on page 132.

   Antispam scanning is done only on the local appliance. However, selecting the Scan messages for any recipient checkbox enables outbound scanning and inbound scanning on the appliance. For more information, see step 9.

   If Class of Service (COS) is not enabled, antispam scanning will run for all users. If COS is enabled and antispam services are under COS control, antispam scanning only runs for users with antispam listed in their `miService` LDAP attribute. For more information, see Managing Class of Service on page 297.

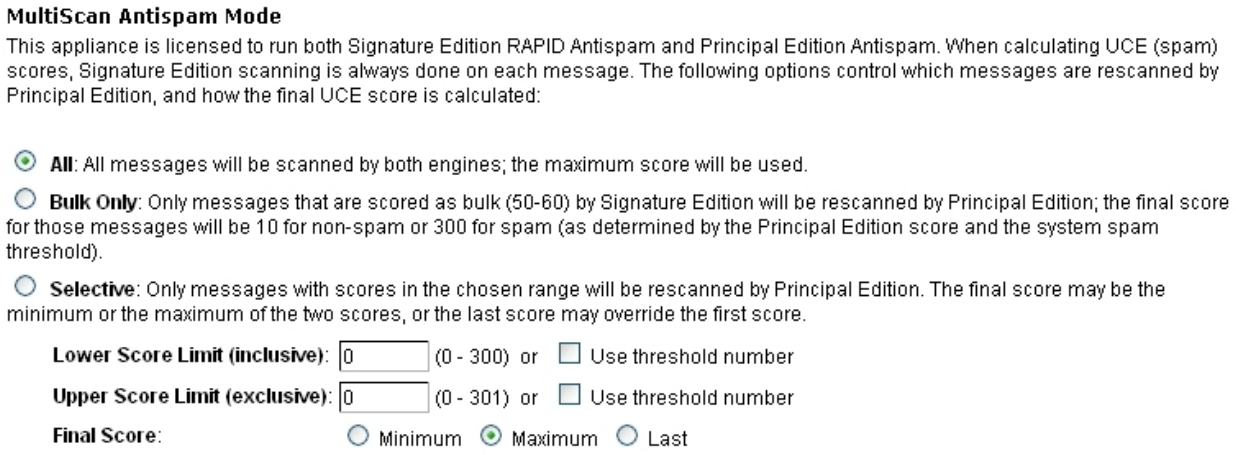
3. Under the **Set Threshold** section, in the **Threshold Number** text field, Mirapoint recommends accepting the default threshold of 50. This setting adjusts the antispam scoring severity. You can adjust the severity by incrementing or decrementing the number by 1.



However, lower values cause the scan to score more mail as spam, increasing possible false-positives. Higher values causes the scan to score less incoming mail as spam, increasing possible false-negatives. For more information, see About Antispam Scanning and Threshold on page 133.

4. (Optional) Click **Show Junkmail Statistics** to see your appliance's current **Incoming Mail Messages versus Junk Mail Messages** performance graph. Click **Hide Junk Mail Statistics** to hide the graph. For more information on the graph, see Viewing Junk Mail Statistics on page 284.

5. (Optional) If you are running Signature Edition RAPID Antispam with Principal Edition Antispam *or* with Premium Edition Antispam on this appliance, the **MultiScan Antispam Mode** section displays. When calculating the spam score, Signature Edition scanning is always performed on each message. The options under this section only control which messages are re-scanned by Principal Edition or Premium Edition, and how the final score is calculated. For more information, see Signature Edition, Principal Edition, and Premium Edition on page 130 and Using MultiScan Antispam on page 131.



To configure MultiScan Antispam, select one of the following radio buttons:

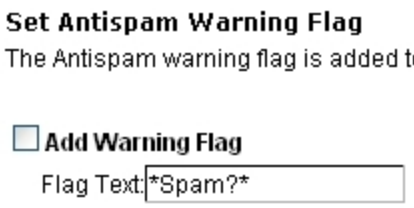
- **All** - Selecting this option ensures that all messages are scanned using Signature Edition with Principal Edition *or* with Premium Edition, and that the **Final Score** is always the **Maximum**. Meaning, the maximum of the two scores from each engine is used as the final spam score.
- **Bulk Only** - Selecting this option ensures that only messages that are scored as `bulk` (50-60) by Signature Edition will be rescanned by Principal Edition or Premium Edition. The final spam score for those messages will be 10 for `non spam` or 300 for `spam` (as determined by the Principal Edition or Premium Edition score and the **Threshold Number** you set in step 3).
- **Selective** - If you selected this radio button set the following options:
  - In the **Lower Score Limit (inclusive)** text field, type the lower score limit in the range or select the **Use threshold number** checkbox to use the **Threshold Number** you set in step 3. The number must be between 0 and 300. The default is 0.
  - In the **Upper Score Limit (exclusive)** text field, type the upper score limit in the range or select the **Use threshold number** checkbox to use the **Threshold Number** you set in step 3. The number must be between 0 and 301. The default is 0.

If you select the **Use threshold number** checkbox for the lower score limit, the upper score limit defaults to 0, and vice versa. Also, you cannot set an upper and lower limit to the same value, unless the value is 0.

If you set both upper and lower limits to 0, then only messages classified as `bulk` (scores 50-59) are rescanned. If the rescan score from Principal Edition or Premium Edition is larger than the specified threshold (e.g., 50), the final score is set to 300 (i.e., `spam`). If the score is less than or equal to the threshold, the final score is set to 10 (i.e., `non spam`).

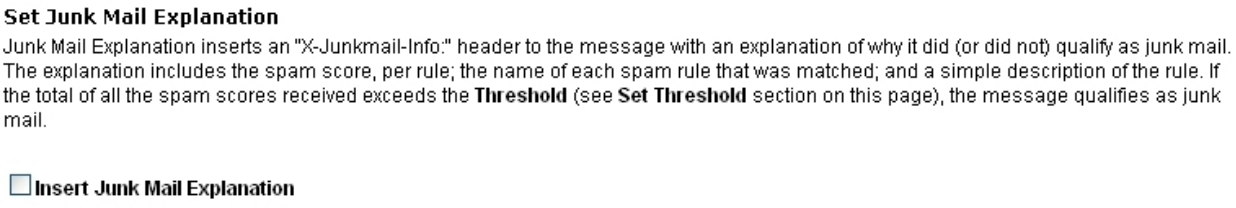
- For the **Final Score** setting, select the **Minimum**, **Maximum**, or **Last**. If **Maximum** is selected, the maximum of the two scores from each engine is used as the final spam score. If **Minimum** is selected, the minimum of the two scores from each engine is used. If **Last** is select, the score from Principal Edition or Premium Edition is used. By default, **Maximum** is selected.

6. Under the **Set Antispam Warning Flag** section, select the **Add Warning Flag** checkbox if you want to insert warning text into the **Subject** line of mail qualifying as spam. If you want to customize the warning flag, type your custom text into the **Flag text** text field. The default text is `*Spam?*`.



This option is useful for delivery to POP users who might lack a junk mail folder. However, spam mail for POP users must be configured to go to their Inbox.

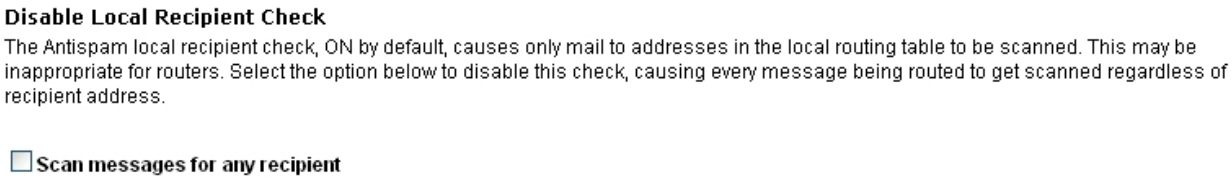
7. Under the **Set Junk Mail Explanation** section, make sure that the **Insert Junk Mail Explanation** checkbox is selected if you want to insert a special header, `X-Junkmail-Info` (Principal Edition Antispam) or `X-Junkmail-Premium-Raw` (Premium Edition Antispam), into the message header with information on the results of the antispam scan. The **Insert Junk Mail Explanation** checkbox only displays for Principal Edition Antispam or Premium Edition Antispam. This can be useful for debugging purposes.



8. Under the **Set Junk Mail Reporting** section, make sure that the **Enable Junk Mail Reporting** checkbox is selected if you want the **Report this spam to system support** or **Report this false spam to system support** options 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. This checkbox is selected by default.

   If users elect to report the spam/false spam to Mirapoint, two system folders are created (`junkmail.junkmail` and `junkmail.notjunkmail`). Periodically, samples from the two folders are sent to Mirapoint to assist in scanning improvements.

9. Under the **Disable Local Recipient Check** section, make sure that the **Scan messages for any recipient** checkbox is selected if you want to enable antispam scanning on outbound mail as well as inbound mail.



10. Click **Apply**.

    Your configuration options are recorded by the appliance and acted on as specified. A header line `X-Junkmail-Info` (Principal Edition Antispam), `X-Junkmail-Premium-Raw` (Premium Edition Antispam), or `X-Junkmail-Signature-Raw` (Signature Edition RAPID Antispam), is added to all messages identified as spam. For more information, see About Message Envelopes and Headers on page 238.

Signature Edition, Principal Edition, and Premium Edition

The antispam scanner uses one or two (depending on licensing) engines to categorize mail as junk mail (spam). However, you have three different engines to choose from: Signature Edition RAPID Antispam, Principal Edition Antispam, and Premium Edition Antispam.

Signature Edition RAPID 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`. Any UCE (unsolicited commercial email) score between 50 and 60 by default, categorizes the mail as bulk (i.e., spam) and triggers the **Junk Mail Filter**. For more information, see About the Junk Mail Filter on page 132 and About Antispam Scanning and Threshold on page 133. Signature Edition updates are named **rpdengine** and must be applied manually.

Principal Edition Antispam and Premium Edition Antispam compare all incoming email messages to a set of rules. The more rules the message matches, the higher the junk mail UCE score it is assigned. Like Signature Edition, 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 Principal Edition are named **default**. The rule group updates for Premium Edition are named **premium**. Updates for both rule groups are automatically applied.

Signature Edition's predictive-based scanning is faster than the rules-based scanning performed by Principal Edition or Premium Edition.

All of the antispam engines score messages and insert a message header to indicate junk mail. These headers are inserted when a message is scored above the junk mail threshold:

- `X-Junkmail-Info` for Principal Edition Antispam
- `X-Junkmail-Premium-Raw` for Premium Edition Antispam
- `X-Junkmail-Signature-Raw` for Signature Edition RAPID Antispam

The `X-Junkmail` headers can be used as a search parameter in a domain-wide or per-user message filter. The junk mail threshold can be adjusted on the **Antispam Configuration** (**Home > Antispam > Configuration**) page for all antispam engines. For a list of Mirapoint `X-Junkmail` headers, see Configuring Antispam Scanning on page 127 and About Message Envelopes and Headers on page 238.

Using MultiScan Antispam

If you have two antispam engines licensed on your appliance, either Signature Edition RAPID Antispam with Principal Edition Antispam *or* with Premium Edition Antispam, you can configure your appliance to use both engines in conjunction.

You cannot license and run Principal Edition and Premium Edition on the same appliance. However, you can have these engines running on separate appliances within the same environment.

If both engines are licensed, a **MultiScan Antispam Mode** section displays on the **Antispam Configuration** page (**Home > Antispam > Configuration**). When calculating the UCE (spam) score, Signature Edition scanning is always performed on each message. Therefore, the options under the MultiScan Antispam Mode section only control which messages are re-scanned by Principal Edition or Premium Edition, and how the final spam score is calculated.

You can configure the antispam scanner to perform MultiScan scanning for:

- **All** messages - Signature Edition with Principal Edition or with Premium Edition engines are used to scan every message, with Signature Edition scanning being performed first.
- **Bulk Only** messages - Only messages that are scored as bulk (50-60) by Signature Edition will be re-scanned by Principal Edition. The final spam score for those messages will be 10 for `non spam` or 300 for `spam` (as determined by the Principal Edition or Premium Edition score and the junk mail threshold as set on the appliance).
- **Selective** messages - Only messages with scores in the range you select will be re-scanned by Principal Edition or Premium Edition. The range uses a lower score limit and an upper score limit that you can modify. The final spam score is calculated based upon the **Final Score** setting. The **Final Score** setting can be the minimum or the maximum of the two scores, or the last score can override the first score.

You can also configure these options using the CLI and `Uce` commands. For more information, see the *Mirapoint Administration Protocol Reference*.

For more information on how to configure antispam scanning, see Configuring Antispam Scanning on page 127. For more information about the junk mail threshold, see About Antispam Scanning and Threshold on next page.

About the Junk Mail Filter

End-users must go to **Options > Junk Mail Control > Junk Mail Filter** or **Options > Messages Filters** within WebMail Direct Standard Edition or **Options > Mail > Message Filters** within WebMail Corporate Edition, and explicitly enable the filter. By default, the appliance-created **Junk Mail Filter** defaults to **Off** because non-WebMail POP users are not able to see the **Junk Mail** folder.

The user's **Junk Mail Filter** condition must be set to **Normal** or **Exclusive** in order for their allowed senders, blocked senders, and allowed mailing lists options in WebMail to work properly. The **Junk Mail Filter**, when **On**, tells the antispam scanner what to do with mail categorized as junk mail. The default filter action, **Move to the Junk Mail folder**, allows users to check their junk mail for false-positives.

The **Junk Mail Filter** is only used when Junk Mail Manager (JMM) is *not* used to manage junk mail messages. Users must turn the **Junk Mail Filter** off to use JMM.

How Antispam Features Are Applied

Mirapoint's antispam features are applied in the following 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 RG100s)
10. Junk Mail Filter (not available for RG100s)

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 junk mail score.

After a message is processed through the antispam scanner, if it is tagged as junk mail, 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.

About Antispam Scanning and Threshold

The antispam scanner uses one of three engines (or techniques) to categorize mail as junk mail (spam): Principal Edition Antispam, Premium Edition Antispam, or Signature Edition RAPID Antispam. Which antispam scanning engine you use depends on what licenses you have applied. You can also use two engines in conjunction. For more information, see Using MultiScan Antispam on page 131.

Principal Edition and Premium Edition antispam scanning uses several carefully compiled rule files based on common known factors of junk mail. The more rule matches, the higher the UCE (unsolicited commercial email) score. By default, a score over 50 classifies the mail as junk mail, this is known as the junk mail threshold. You can adjust this threshold on the **Antispam Configuration** page (**Home > Antispam > Configuration**).

Signature Edition RAPID antispam scanning uses an entirely different technique for scanning Internet traffic and detecting patterns to create a database of email signatures against which incoming email is compared and scored. By default, a UCE score between 35 and 45 is marked `suspect` in the message header, and such mail is not classified as junk mail. A score between 50 and 60 is marked `bulk` in the message header and is classified as junk mail. A score of 300 is marked as `spam` and classified as junk mail. 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 cutoff 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. Careful study has determined that the default threshold, a UCE score of 50, is optimal for both engines. 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.

However, adjusting the threshold to below 50 causes more messages to trigger the **Junk Mail Filter** and more false-positive messages (i.e., messages wrongly identified as junk mail) will be delivered. Adjusting the threshold to above 50 causes fewer messages to trigger the **Junk Mail Filter** and more false-negative messages (i.e., spam messages missed by the scanner) will be delivered. For more information, see About the Junk Mail Filter on previous page.

Antispam reporting allows Mirapoint to fine-tune the techniques based on feedback received. For more information, see Viewing Security Reports on page 270.

Updating Antispam

Antispam updates are an important step in the configuration process as rule group updates optimize the utility. In addition to rule group updates, exception files for MailHurdle listing known good mailers are included in updates.

Additional information about antispam updates is provided in the following sections:

- Installing/Updating Rule Groups below
- Setting Up Automatic Antispam Rule Group Updates on next page

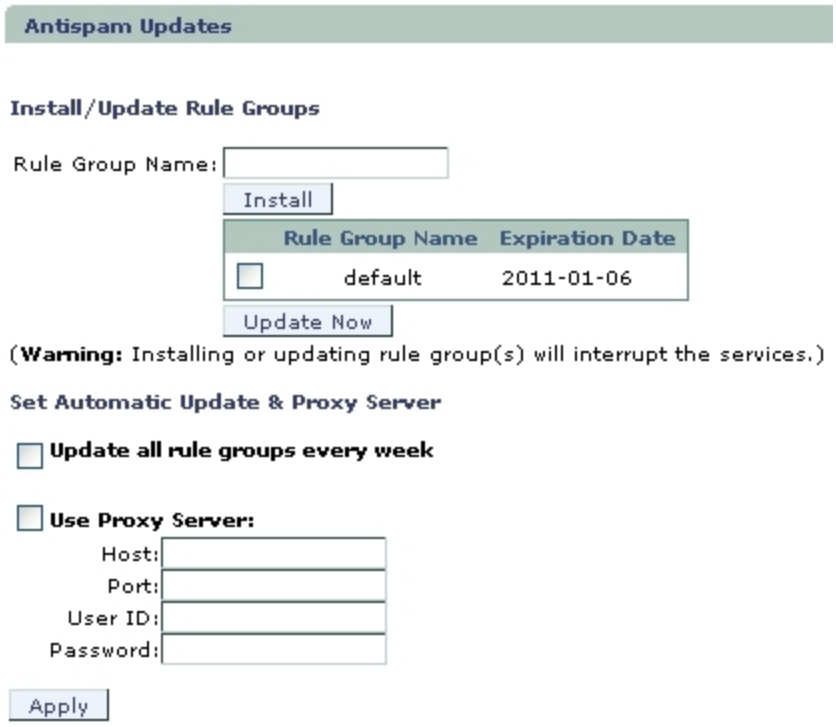
Installing/Updating Rule Groups

As spammers evolve new spamming techniques, new methods to battle them are added.

To install a rule group or exception file (i.e., known good mailers):

1. Go to **Home > Antispam > Updates**.

   The **Antispam Updates** page appears.



2. In the **Rule Group Name** text field, type in the rule group name you want to install.
3. Click **Install**.

Mirapoint occasionally adds named rule groups that you can access through the Mirapoint Technical Support website.

The new rule group is installed and displays in a table containing the following information:

- **Rule Group Name** - The name of the rule group.
- **Expiration Date** - The expiration date of the rule group.

To update a rule group:

1. Go to **Home > Antispam > Updates**.

   The **Antispam Updates** page appears.

2. In the table, select the rule group's checkbox.
   - **default** (Principal Edition Antispam)
   - **premium** (Premium Edition Antispam)
   - **rpdengine** (Signature Edition RAPID Antispam) or **rpdasia** (Signature Edition RAPID Antispam in Asia)
4. Click **Update Now**.

   Any available updates to that rule group are downloaded and updated with the latest junk mail rule group. The page redisplays with a message indicating that the update is complete.

Setting Up Automatic Antispam Rule Group Updates

You can set your antispam scanning utility to updates its rule groups and/or MailHurdle exception files (i.e., known good mailers) automatically every week.

To set up automatic antispam rule group updates:

1. Go to **Home > Antispam > Updates**.

   The **Antispam Updates** page appears.

2. Select the **Update all rule groups every week** checkbox.
3. If you use a proxy when accessing the Internet, select the **Use Proxy Server** checkbox.
4. In the appropriate text fields, type the **Host** name, **Port** number, **User ID**, and **Password** required by your proxy for access to the Internet.
5. Click **Apply**.

The utility retrieves an updated file with additional spam rules and, MailHurdle known good mailers, for it to use when scanning messages.

Managing Allowed Senders

Use the **Set Allowed Senders** page (**Home > Antispam > Allowed Senders**) to ensure that mail from certain senders is always sent to recipients and never tagged as junk mail. Domain and user filters can override the allowed senders list (also known as a *safelist*). You can also use the command-line interface (CLI) to set up logging of domain mail from allowed and blocked senders. For more information, see the *Mirapoint Administration Protocol Reference* or type `Help About Log` in the CLI.

The **Set Allowed Senders** page only displays if you have antispam licensed and configured for your appliance.

The allowed senders list does not do dot-to-underscore mapping so it might be necessary for you to create both a dot (.) and an underscore (_) entry for the same sender in order to be sure 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`. For more information on using wildcards with filters, see Using Patterns and Wildcard Characters on page 191.

A WebMail user's **Junk Mail Filter** condition must be **Normal** or **Exclusive** in order for the user-level allowed senders list in WebMail to work properly. This does *not* apply to Junk Mail Manager (JMM) or non-WebMail, users. For more information, see About the Junk Mail Filter on page 132 .

To create an allowed senders list:

1. Go to the **Home > Antispam > Allowed Senders**.

   The **Set Allowed Senders** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are creating.

If you want to set an allowed senders list for a particular domain, select the domain. Otherwise, the allowed senders list will apply to all traffic through the primary domain. If you selected a domain (other than the primary) before going to this page, if you log in as a Domain Administrator, or if this is for a Junk Mail Domain, these options do not display.

Select one of the following options:

- **Primary**: Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
- **Any**: Filter any messages routed to or through the appliance on which the filter is created.
- **Local**: Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
- **Non-local**: Only filter messages addressed to users not on the appliance on which the filter is created.

The filter looks only at the mail addressed to the selected domain. For more information, see About the Destination Domain on page 174.

3. In the **E-mail Address or Domain** text field, type the email address or domain name you want to safelist. If you enter a domain name, the at sign (@) is automatically prefixed.
4. Click **Add**.

The email address or domain name appears in the allowed senders list and the list's status is updated to reflect the new entries. Mail sent from senders on your allowed senders list is forwarded to the specified recipients with a header, `X-Junkmail-Whitelist: YES (by domain whitelist at hostname)`. For more information, see About the X-Junkmail: Whitelist Header on the facing page.

5. Under the **Prioritize Allowed Senders** area, select the **Immediately pass mail through if the sender is on the Allowed Senders list** checkbox to prevent mail from your allowed senders from getting processed by MailHurdle. If you leave the checkbox unselected, mail from senders on your allowed senders list will be processed by MailHurdle. There will be an initial delay the fist time for each sender. However, if the mail fails to pass MailHurdle, it will never be delivered.

If you selected the checkbox, click **Set**.

The sender is derived from the **From** header of the message.

To delete an allowed sender:

1. Go to **Home > Antispam > Allowed Senders**.

The **Set Allowed Senders** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are removing.

If you want to set an allowed senders list for a particular domain, select the domain. Otherwise, the allowed senders list will apply to all traffic through the primary domain. If you selected a domain (other than the primary) before going to this page, if you log in as a Domain Administrator, or if this is for a Junk Mail Domain, these options do not display.

Select one of the following options:

- **Primary**: Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
- **Any**: Filter any messages routed to or through the appliance on which the filter is created.
- **Local**: Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
- **Non-local**: Only filter messages addressed to users not on the appliance on which the filter is created.

3. In the allowed senders list, select the checkbox for the sender you want to remove.
4. Click **Remove**.

   A confirmation window appears.

5. Make sure the checkbox is still selected and click **Remove**.

About the X-Junkmail: Whitelist Header

The header for domain-allowed senders mail and user-allowed senders mail is slightly different. A domain-level allowed senders list generates the `X-Junkmail: Whitelist (by domain whitelist at` *`hostname`*`)` header. A user-level allowed senders list generates the `X-Junkmail: Whitelist (by` *`username`* `at` *`hostname`*`)` header. Neither header is visible unless the recipients view all of the headers. Recipients can view all headers in WebMail by clicking **Open** when viewing a message.

Managing Blocked Senders

Use the **Set Blocked Senders** page (**Home > Antispam > Blocked Senders**) to ensure that mail from certain senders is always sent to recipients tagged as `junkmail`. Administrators can use the command-line interface (CLI) to set up logging of domain mail from allowed and blocked senders. For more information, see the *Mirapoint Administration Protocol Reference* or type `Help About Log` in the CLI.

The **Set Blocked Senders** page only displays if you have antispam licensed and configured for your appliance.

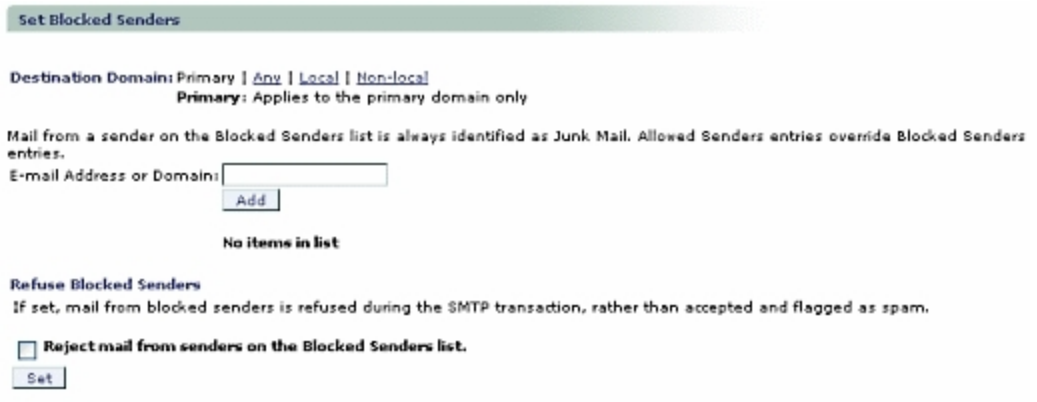
The blocked senders list does not do dot-to-underscore mapping so it may be necessary for you to create both a dot (.) and an underscore (_) entry for the same sender in order to be sure that the sender is blocked. For example, to make sure that `user.ab@example.com` is always blocked, use `user.ab@example.com` and `user_ab@example.com`. For more information on using wildcards with filters, see Using Patterns and Wildcard Characters on page 191.

A WebMail user's **Junk Mail Filter** condition must be **Normal** or **Exclusive** in order for the user-level allowed senders list in WebMail to work properly. This does *not* apply to Junk Mail Manager (JMM) or non-WebMail, users. For more information, see About the Junk Mail Filter on page 132 .

To create a blocked senders list:

1. Go to **Home > Antispam > Blocked Senders**.

   The **Set Blocked Senders** page appears.



2. In the **Destination Domain** area specify the scope for the filter you are creating.

   If you want to set a blocked senders list for a particular domain, select the domain. Otherwise, the blocked senders list will apply to all traffic through the primary domain. If you selected a domain (other than the primary) before going to this page, if you log in as a Domain Administrator, or if this is for a Junk Mail Domain, these options do not display.

   Select one of the following options:

   - **Primary**: Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
   - **Any**: Filter any messages routed to or through the appliance on which the filter is created.
   - **Local**: Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
   - **Non-local**: Only filter messages addressed to users not on the appliance on which the filter is created.

   The filter looks only at the mail addressed to the selected domain. For more information, see About the Destination Domain on page 174.

3. In the **E-mail Address or Domain** text field, type the email address or domain name you want to block. If you enter a domain name, the at sign (@) is automatically prefixed.
4. Click **Add**.

The email address or domain name appears in the blocked senders list and the list's status is updated to reflect the new entries. Mail sent from senders on your blocked senders list is forwarded to the specified recipients with a header, `X-Junkmail: Blacklisted`, added and is acted on by the **Junk Mail Filter** if the recipients have turned it on. For more information, see About the X-Junkmail: Blacklist Header on next page and About the Junk Mail Filter on page 132.

If the sender is on the user's personal allowed senders list, the header remains but the mail is delivered anyway.

5. Under the **Prioritize Blocked Senders** area, select the **Immediately classify the message as junkmail if the sender is on the Blocked Senders List** checkbox to reject mail from your Blocked Senders list. If this option is selected, mail from senders on your Block Senders list is rejected with a 550 error code (i.e., the mail was rejected for policy reasons) at the SMTP level. In addition, this mail is not processed by MailHurdle.

   If this option is not selected, mail from senders on your Blocked Senders list is flagged with an `X-Junkmail: Blacklisted` header, but is not receive an antispam score. However, it is processed by MailHurdle. If the mail passes MailHurdle, it is then subject to the selected **Junk Mail** filter action.

   If you selected the checkbox, click **Set**.

The sender is derived from the **From** header of the message.

To delete a blocked sender:

1. Go to **Home > Antispam > Blocked Senders**.

   The **Set Blocked Senders** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are removing.

If you want to set a blocked senders list for a particular domain, select the domain. Otherwise, the blocked senders list will apply to all traffic through the primary domain. If you selected a domain (other than the primary) before going to this page, if you log in as a Domain Administrator, or if this is for a Junk Mail Domain, these options do not display.

   Select one of the following options:

   - **Primary**: Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
   - **Any**: Filter any messages routed to or through the appliance on which the filter is created.
   - **Local**: Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
   - **Non-local**: Only filter messages addressed to users not on the appliance on which the filter is created.

3. In the blocked senders list, select the checkbox for the sender you want to remove.
4. Click **Remove**.

   A confirmation window appears.

5. Make sure the checkbox is still selected and click **Remove**.

About the X-Junkmail: Blacklist Header

The header for domain-blocked senders mail and user-blocked senders mail is slightly different. A domain-level blocked senders list generates the `X-Junkmail: Blacklisted` header. A user-level blocked senders list generates the `X-Junkmail: Blacklisted (by username at hostname)` header. Neither header is visible unless the recipients view all of the headers. Recipients can view all headers in WebMail by clicking **Open** when viewing a message.

Managing Allowed Mailing Lists

Use the **Set Allowed Mailing Lists** page (**Home > Antispam > Allowed Mailing Lists**) to ensure that mail addressed to certain recipients never receives the configured **Junk Mail Filter** action. This is primarily used to safeguard mailing lists that you are on, to avoid mail coming in to you being accidentally categorized as spam. Setting allowed mailing lists can also be used for mailing lists to which you want to send mail without antispam filtering delays. This feature is also known as the *recipient whitelist* or *whitelistto*.

Using 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, the Allowed Mailing Lists list must reside on the same appliance that handles MailHurdle. If the list resides on an appliance that receives the mail after MailHurdle processing, it will not prevent MailHurdle delays.

The **Set Allowed Mailing Lists** page only displays if you have antispam licensed and configured for your appliance.

In order for outbound antispam scanning to occur you must have the **Scan messages for any recipient** option selected on the **Antispam Configuration** page (**Home > Antispam > Configuration**). Administrators can use the command-line interface (CLI) to set up logging of domain mail from allowed, blocked, and allowed mailing list senders. For more information, see the *Mirapoint Administration Protocol Reference* or type `Help About Log` in the CLI.

The allowed mailing list does not do dot-to-underscore mapping so it might be necessary for you to create both a dot (.) and an underscore (_) entry for the same recipient in order to be sure 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`. For more information on using wildcards with filters, see Using Patterns and Wildcard Characters on page 191.

A user's **Junk Mail Filter** condition must be **Normal** or **Exclusive** in order for the user-level allowed senders list in WebMail to work. This does *not* apply to Junk Mail Manager (JMM) or non-WebMail users. For more information, see About the Junk Mail Filter on page 132 .

To create an allowed mailing list:

1. Go to **Home > Antispam > Allowed Mailing Lists**.

   The **Set Allowed Mailing Lists** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are creating.

   If you want to set an allowed mailing list for a particular domain, select the domain. Otherwise, the allowed mailing list will apply to all traffic through the primary domain. If you selected a domain (other than the primary) before going to this page, if you log in as a Domain Administrator, or if this is for a Junk Mail Domain, these options do not display.

   Select one of the following options:

   - **Primary**: Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
   - **Any**: Filter any messages routed to or through the appliance on which the filter is created.
   - **Local**: Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
   - **Non-local**: Only filter messages addressed to users not on the appliance on which the filter is created.

   The filter looks only at the mail addressed to the selected domain. For more information, see About the Destination Domain on page 174.

3. In the **Mailing List Address or Domain** text field, type the mailing list address or domain name you want to allow. If you enter a domain name, the at sign (@) is automatically prefixed.
4. Click **Add**.

The mailing list address or domain name appears in the allowed mailing list and the list's status is updated to reflect the new entries.

Mail sent to recipients on your allowed mailing list is forwarded to the specified recipients with a header, `X-Junkmail-Recipient-Whitelist: YES (by domain whitelist at hostname)`, added. This mail is not scanned by the antispam scanning utility. The header is added whether the exempting was at the primary level or at the delegated domain level. For more information, see About the X-Junkmail: WhitelistTo Header on the facing page.

5. Under the **Prioritize Allowed Mailing Lists** area, select the **Immediately pass mail through if the recipient is on the Allowed Mailing Lists** checkbox to prevent mail to your allowed mailing list recipients from getting processed by MailHurdle. If you leave the checkbox unselected, mail to recipients on your allowed mailing lists list will be processed by MailHurdle. Typically, the mail will arrive, but there might be an initial delay the first time for each sender. However, if for some reason the mail fails to pass MailHurdle, it will never be delivered.

   If you selected the checkbox, click **Set**.

The sender is derived from the **To** header of the message.

To remove an allowed mailing list:

1. Go to **Home > Antispam > Allowed Mailing Lists**.

   The **Set Allowed Mailing List** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are removing.

If you want to set an allowed mailing list for a particular domain, select the domain. Otherwise, the allowed mailing list will apply to all traffic through the primary domain. If you selected a domain (other than the primary) before going to this page, if you log in as a Domain Administrator, or if this is for a Junk Mail Domain, these options do not display.

   Select one of the following options:

   - **Primary**: Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
   - **Any**: Filter any messages routed to or through the appliance on which the filter is created.
   - **Local**: Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
   - **Non-local**: Only filter messages addressed to users not on the appliance on which the filter is created.

3. In the allowed mailing lists list, select the checkbox for the mailing list address you want to remove.
4. Click **Remove**.

   A confirmation window appears.

5. Make sure the checkbox is still selected and click **Remove**.

About the X-Junkmail: WhitelistTo Header

The header for domain-allowed mailing list emails and user-allowed mailing list emails is slightly different. A domain-level allowed mailing list generates this header: `X-Junkmail-Recipient-Whitelist (by domain whitelist at hostname)`. A user-level allowed mailing list generates this header: `X-Junkmail-Recipient-Whitelist (by username at hostname)`. Neither header is visible unless the recipients view all of the headers. Recipients can view all headers in WebMail by clicking **Open** when viewing a message.

Managing the Relay List

The **Set Relay List** page (**Home > Antispam > Relay List**) 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 effect on messages accepted for delivery to local mailboxes. Relay lists are useful to prevent your systems from being highjacked to send junk mail. Unless a relay address is explicitly added, the appliance does not relay messages from other networks or domains.

The appliance does *not* require an antispam license in order to use this feature.

To add a host to a relay list:

1. Go to **Home > Antispam > Relay List**.

   The **Set Relay List** page appears.

2. In the **IP Network or DNS Domain** text field, type an IP address or domain name. You can use a partial IP address, a full IP address, or a domain name.

To accept mail relay from a specific network, type 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, appliances relay mail from the mail domain you just set, but many administrators add the mail domain to the relay list anyway.

3. Click **Add**.

The new relay network displays in a list. Mail sent from those networks is relayed to its destination.

To delete a host from a relay list:

1. Go to **Home > Antispam > Relay List**.

   The **Set Relay List** page appears.

2. Select the checkbox for the sender you want to remove.
3. Click **Remove**.

Managing the Reject List

Use the **Set Reject List** page (**Home > Antispam > Reject List**) to specify networks from which your system will reject messages. Use this to help minimize the amount of unsolicited commercial email (UCE) that the appliance receives.

The appliance does *not* require an antispam license in order to use this feature.

To add a sender to the reject list:

1. Go to **Home > Antispam > Reject List**.

   The **Set Reject List** appears.

2. In the **IP Network or DNS Domain** text field, type an IP address or domain name. You can use a partial IP address, a full IP address, or a domain name.
3. Click **Add**.

The new reject network displays in a list. Mail sent from those networks is bounced back to the sender. This is equivalent to the `Uce Add` command in the command-line interface (CLI). For more information, see the *Mirapoint Administration Protocol Reference*.

To delete a sender from the reject list:

1. Go to **Home > Antispam > Reject List**.

   The **Set Reject List** appears.
2. Select the checkbox for the sender you want to remove.
3. Click **Remove**.

Managing RBL Host Lists

The **Set RBL Host List** page (**Home > Antispam > RBL Host List**) allows you to specify that all incoming messages be checked against the Real Time Blackhole List (RBL) Internet services you specify. 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 websites for these services and subscribe in order to use this option.

The appliance does *not* require an antispam license in order to use this feature.

Use the **Set RBL Check Action** section 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, and an appropriate `X-Junkmail` header is added based on that score and any safelist or blacklist 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. For information on the UCE score, see About Antispam Scanning and Threshold on page 133.

To add an RBL host to the host list:

1. Go to **Home > Antispam > RBL Host List**.

   The **Set RBL Host List** page appears.

2. If the RBL checking is not already enabled, click **Enable it**.
3. In the **RBL Host** text field, type the hostname for an RBL service.

   Currently, the main RBL service is hosted by Trend Micro's MAPS (Mail Abuse Prevention System LLC). Visit http://mail-abuse.com/ for subscription information.

4. Click **Add**.

   The new RBL host displays in a list. You can add up to 8 RBL hosts.

5. Under the **Set RBL Check Action** section, select one of the following options:

   - **Reject the message and send a "bounced" message to the sender**: The message is returned to the boycotted host with a 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 more information see Creating Advanced Content Filters on page 173.

6. Click **Apply**.

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.

To delete an RBL host from the host list:

1. Go to **Home > Antispam > RBL Host List**.

   The **Set RBL Host List** page appears.

2. Select the checkbox for the host you want to remove.
3. Click **Remove**.

Managing MailHurdle

Use the **About MailHurdle** page (**Home > Antispam > MailHurdle**) to configure the MailHurdle utility that provides an additional, highly effective, layer of antispam scanning. MailHurdle is an antispam method that caches three pieces of mail data called *triplets* and sends a standard SMTP error code that means, "you should retry this address later." Most spam mailers will not properly retry addresses that have received that error code, whereas legitimate mail agents will retry delivery.

The **About MailHurdle** page only displays if you have antispam licensed and configured for your appliance.

Allowed mailing lists are 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 filter must reside on the same appliance that runs MailHurdle. If the list resides on an appliance that receives the mail after MailHurdle processing, it will not prevent MailHurdle delays. For more information, see Managing Allowed Mailing Lists on page 141.

To prepare for deploying MailHurdle:

1. Using the **Remote Mail** logs (**Home > Logs/Reports > Mail > Remote**), create a list of known sites with which your users often correspond. Using the **Set Allowed Senders** page (**Home > Antispam > Allowed Senders**), put all such sites into the domain allowed senders list. Also select the **Immediately pass mail through if the sender is on the Allowed Senders list.** checkbox on that page.
2. Determine which users should have minimal delay imposed on their email, such as the company helpdesk. Using the **Set Allowed Mailing Lists** page (**Home > Antispam > Allowed Mailing Lists)**, place all such addresses into the recipient safelist. Also select the **Immediately pass mail through if the sender is on the Allowed Mailing Lists.** checkbox on that page.
3. Alert your end-user base as to when MailHurdle will be enabled. Inform users that if they are expecting important email during the transition phase, senders can send a short message first to the *prime* MailHurdle with the appropriate triplet. The priming email might take hours to arrive, but important emails should arrive quickly.
4. Instruct users to notify an administrator if an important email fails to arrive. It is possible the sending system is not SMTP conformant, and must be added to the domain safelist (see step 1). Mirapoint provides a list of non-conformant mailers, downloaded with the rule groups using the **Antispam Updates** page (**Home > Antispam > Updates**). This list is used by the **Allow Known Good Mailers** option on the **Advanced** page (**Home > Antispam > MailHurdle > Advanced**).

The **About MailHurdle** page provides the following links:

- Configuration - Configure MailHurdle servers, timeout periods, and server cache.
- Allowed Host - Specify hosts that are allowed to make queries to the MailHurdle server.
- Advanced - Specify filtering priorities, and fine-tune caching options.

Configuring MailHurdle

Use the **Configuration** page (**Home > Antispam > MailHurdle > Configuration**) to specify a server to perform the MailHurdle function, and set the default timeouts for the three phases of caching triplets. *Triplets* are the three pieces of mail data: Remote Server Peer (IP) Address, Sender (Envelope From) Address, and Recipient (Envelope To) Address, that MailHurdle caches while waiting for a retry after having `tempfailed` the message.

To configure MailHurdle:

1. Go to **Home > Antispam > MailHurdle > Configuration**.

   The **Configuration** page appears.

2. If MailHurdle is not enabled, click **Enable it**.
3. Specify the **MailHurdle server** and click **Add**. This is the appliance that will perform the MailHurdle caching. Default is the local host.
4. Set the following **Triplet Timeout** options.

These options do not display if MailHurdle is not enabled.

- **Initial Deny**: 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**). The default is 5 minutes.
- **Initial Active**: An **Initial-Active** triplet is one that may now change status; either to **Active** (a retry is accepted) or **Initial-Expired** (no retry is accepted) before the time period you specify ends. If a retry for an **Initial-Expired** triplet arrives, the triplet is returned to an **Initial-Deny** state. The default is 12 hours.
- **Active**: An **Active** triplet is one that has had a retry accepted by the system; during this time period all mail from that triplet is accepted. Each new accepted message resets the **Active** timeout counter; otherwise, the triplet is **Expired** after the time period you specify. If a retry for an **Expired** triplet arrives, the triplet is returned to an **Initial-Deny** state.The default is 36 days.

Triplet timeouts and lifetimes are not exact. The actual timeout will occur between the time specified and one time unit later. For instance, if you specify 5 minutes, timeout occurs 5-6 minutes after. If you specify 2 hours, timeout occurs 2-3 hours later. Timeframe specifications are limited to 59 seconds, 59 minutes, 23 hours, and 60 days. For more information regarding triplet timeouts and lifetimes, and the `Mtaverify` command, see the *Mirapoint Administration Protocol Reference*.

5. **Accept All Triplets Based on "Active" IP Address** (default is selected): After a triplet achieves the **Active** state, all mail from that IP Address is accepted regardless of the sender or recipient address. This can help prevent MailHurdle delays. If you choose to turn this feature off, you must do so on every MailHurdle server and client.
6. Click **Set**.

MailHurdle caches the received triplets as specified immediately. You might notice an initial slow-down in mail delivery, however, this should diminish with time.

MailHurdle and SMTP Authentication

MailHurdle from an authenticated SMTP connection, to a local user, is not enforced (treated as local-local). MailHurdle from a non-authenticated SMTP connection, to a local user, is enforced.

MailHurdle from an authenticated SMTP connection, to a remote user (relaying), is enforced, depending upon the value of the **Inbound Mail Only** option on the **Advanced** page (**Home > Antispam > MailHurdle > Advanced**). If this option is selected (the default), authentication is not enforced. If this option is de-selected, authentication is enforced.

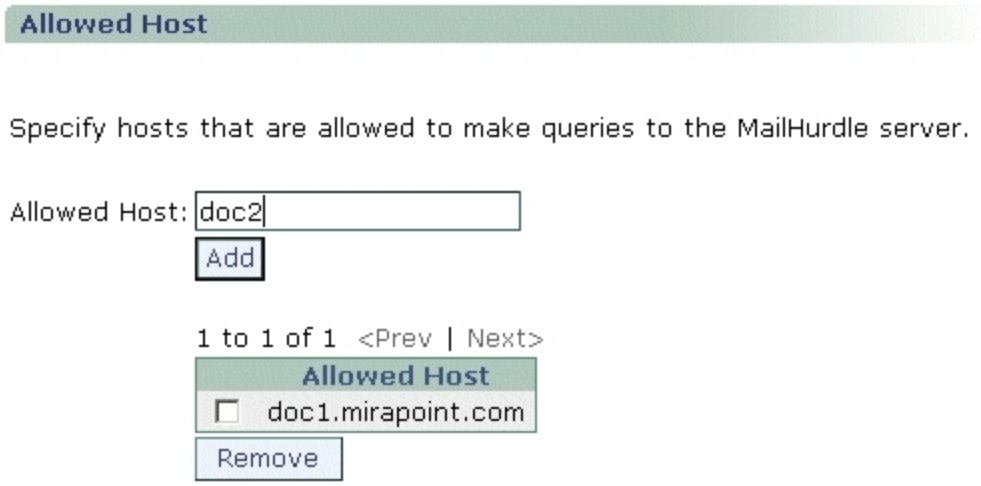
Setting Allowed Hosts

Use the **Allowed Host** page (**Home > Antispam > MailHurdle > Allowed Host**) to specify which machines can query the MailHurdle server.

To set an allowed host:

1. Go to **Home > Antispam > MailHurdle > Allowed Host**.

   The **Allowed Host** page appears.



2. In the **Allowed Host** text field, type the hostname of an appliance that needs to communicate with the MailHurdle server. The local host appliance is allowed by default.
3. Click **Add**.

A table displays the list of allowed hosts. To delete a host from the table, select the checkbox and click **Remove**.

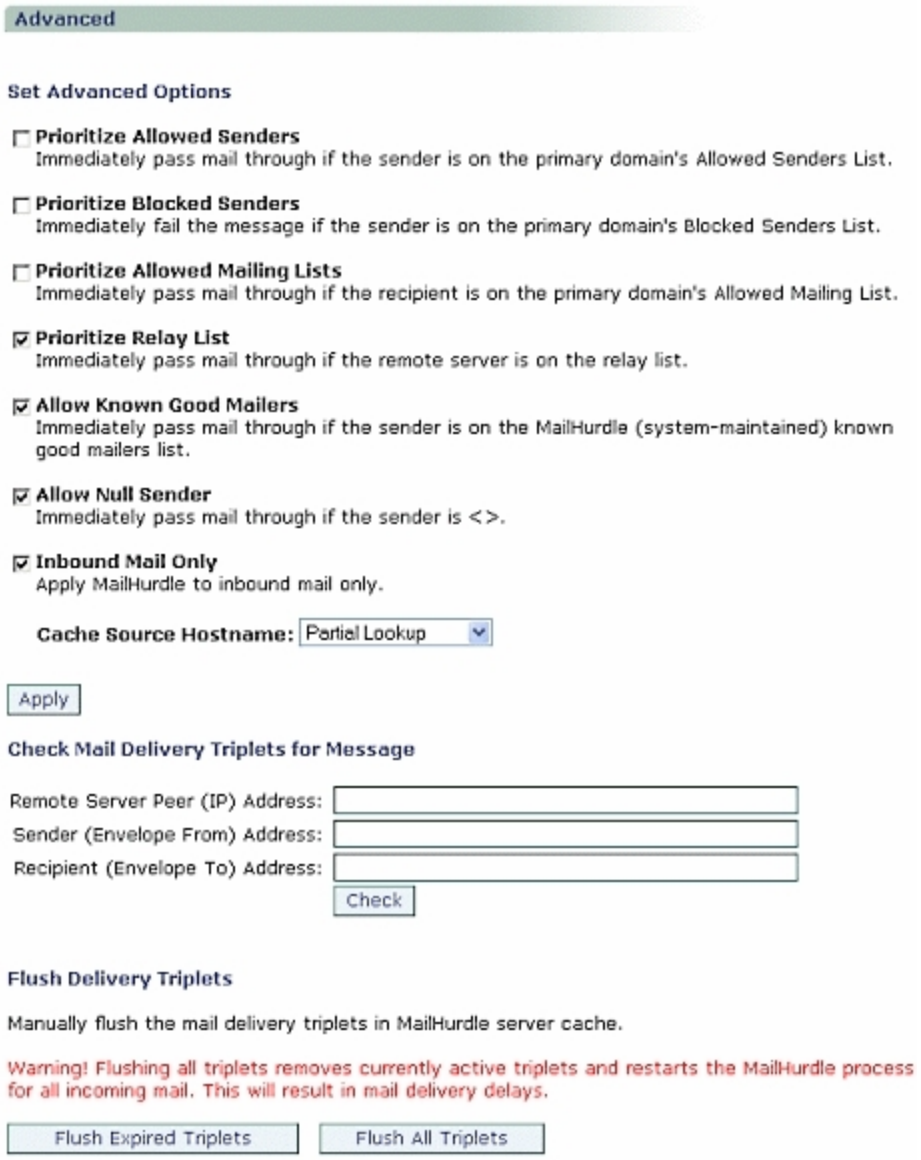
Setting Advanced MailHurdle Options

Use the **Advanced** page (**Home > Antispam > MailHurdle > Advanced**) to set prioritization and other options and also to search for triplets or manually flush the triplet cache.

To set advanced MailHurdle handling options:

1. Go to **Home > Antispam > MailHurdle > Advanced**.

   The **Advanced** page appears.



2. Select one or more of the following MailHurdle handling options:
   - **Prioritize Allowed Senders** - This option ensures that mail from a sender on your allowed senders list does not get delayed by MailHurdle. This option is deselected by default, however, Mirapoint recommends selecting this option.
   - **Prioritize Blocked Senders** - This applies your set blocked senders filter action immediately to mail from those senders without utilizing MailHurdle. Mirapoint recommends leaving this option deselected if any of your users plan to use POP.
   - **Prioritize Allowed Mailing Lists** - This option ensures that mail addressed to recipients on your allowed mailing lists list is delivered without MailHurdle delays. This option is deselected by default, however, Mirapoint recommends selecting this option.

   Mirapoint recommends leaving the following options in their default state:

- **Prioritize Relay List** - This option ensures that mail being routed through the system from servers on your relay list is not subject to MailHurdle delays. This option is selected by default.
- **Allow Known Good Mailers** - This option provides for the corner case of certain well-known senders who routinely fail to follow the SMTP rule of responding to the MailHurdle `try me later` message. This list is maintained by the antispam community at large and will be periodically updated. You can schedule automatic updates of this list using the **Antispam Updates** page. For more information, see Updating Antispam on page 134. This option is selected by default.
- **Allow Null Sender** - This option provides for the corner case where mail is sent with no information for the sender header. This option is selected by default. You can also use the following command-line interface (CLI) commands:

  `Mtaverify Set AllowNullFrom` *`value`*

  `Mtaverify Get AllowNullFrom`

- **Inbound Mail Only** - This option specifies that MailHurdle should only process inbound mail; outbound mail will not be delayed. This option is selected by default.

All domains that you want to receive MailHurdle action for inbound mail must be entered as domains on the appliance, otherwise, those domains will be ignored by MailHurdle if you select this option.

- **Cache Source Hostname** - Controls how incoming IP addresses are converted into hostnames. The appliance performs a reverse PTR lookup via DNS to find the hostname. By default, it takes the most significant parts of the fully-qualified domain name (FQDN) and stores them in the triplet database as the source hostname. This is useful if you want to avoid delaying mail from senders that send mail through multiple systems with different IP addresses.
  - **Original Hostname** - The hostname is stored as is
  - **Partial Lookup** - The most significant parts of the hostname are stored. This option is selected by default.
  - **Complete Lookup** - Multiple DNS lookups are performed in order to determine the number of significant parts in the hostname, then those parts are stored

The default number of significant parts is determined by the suffix (i.e., .com or .jp). Also, in the CLI this option is set using the `Mtaverify Set Reversemx` command. For more information, see the *Mirapoint Administration Protocol Reference*.

3. Click **Apply**.

Checking Mail Delivery Triplets for Message

After you enable MailHurdle, you can look for a specific message in the MailHurdle queue using the mail delivery triplets.

To check triplets for a specific message:

1. Go to **Home > Antispam > MailHurdle > Advanced**.

   The **Advanced** page appears.

2. Under the **Check Mail Delivery Triplets for Message** area, type the appropriate information in one or more of the following text fields:

   - **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.

3. Click **Check**.

The message or an error message displays.

Flushing Mail Delivery Triplets

After you enable MailHurdle, you can flush the MailHurdle triplets queue manually, if necessary.

To flush delivery triplets:

1. Go to **Home > Antispam > MailHurdle > Advanced**.

   The **Advanced** page appears.

2. Under the **Flush Delivery Triplets** area, click one of the following options:

   - **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 will begin again with new incoming mail; triplets that had been passed to an **Active** state will return to **Initial Deny** until passed again.

Managing Junk Mail Manager

Junk Mail Manager (JMM) is a RazorGate option to quarantine spam on a dedicated server where it cannot clog up users' primary mailboxes. Users receive daily email summarizing messages categorized as spam. Using the JMM summary, users can remotely read and/or approve important messages. True spam can be deleted, or left to expire, automatically.

Junk Mail Manager is a licensed feature.

The following topics are included:

- What is a Junk Mail Domain? on the facing page
- Configuring Junk Mail Manager on page 157
- Managing Junk Mail Domains on page 161
- Enabling LDAP Provisioning for Junk Mail Manager on page 169
- Bulk Creating Junk Mail User Accounts on page 169
- Sending a Junk Mail Summary Message on page 171

If you are enabling and configuring Junk Mail Manager (JMM) on your RazorGate appliance, make sure that you have enabled LDAP Provisioning for Junk Mail Manager on your Message Server. For more information, see the Message Server Online Help and the *Mirapoint MOS Configuration Guide*.

Mail security with MailHurdle and antispam scanning, junk mail quarantining, and message routing can all be done on one appliance, or separated onto three or more appliances. JMM can be on an appliance performing all three features, just antispam scanning and quarantining, or just quarantining. What functions the JMM host is performing is an important factor in determining where filters and lists should be configured. For example, your allowed mailing lists filter should always be configured on the appliance that handles MailHurdle. Likewise, safelists on a JMM appliance that only receives messages already categorized as junk mail, are not very effective.

JMM provides an interface, `http://hostname/spam`, for users to access and manage their quarantined junk mail. Once configuration is complete, users receive a welcome email message, that you can configure, that includes an option to opt-out of JMM. If they opt-out, all of their junk mail is delivered directly to them.

JMM also sends users a summary email of their quarantined junk mail with functions that allow them to act directly on the junk mail without logging in to the JMM interface itself. Most users will not log in to the JMM interface but will manage their junk mail through the summaries that are emailed to them at a specified time schedule.

Users that do not opt-out of JMM, can choose not receive the summary emails, however, this is highly discouraged as users must check their quarantined junk mail for false positives (i.e., email mis-categorized as junk mail), and their junk mail will continue to be quarantined with no notification to the user. For information on the JMM interface, see the Mirapoint Junk Mail Manager online help.

What is a Junk Mail Domain?

A *Junk Mail Domain* is an Internet domain with an MX record for which JMM stores and manages spam messages. It is always associated with a JMM host and a mail host. The JMM host is the fully-qualified host name of an appliance that stores and manages spam messages for one or more Junk Mail Domains. The Junk Mail Domain name should match your mail domain names on your Message Server, for example, Mail Domain `example.com` would be entered as Junk Mail Domain `example.com`.

What's the difference between a local Junk Mail Domain and a remote Junk Mail Domain?

A *local* Junk Mail Domain is one configured on the local appliance. A *remote* Junk Mail Domain is configured on a different appliance. You can administer local Junk Mail Domains on the **Administer Local Junk Mail Domains** page (**Junk Mail Manager > Junk Mail Domains**). You must go to the JMM host for a remote domain to administer it. On the **Junk Mail Manager Configuration** page (**Junk Mail Manager > Configuration**), you are asked to specify all remote Junk Mail Domains, and their JMM hosts, so that mail coming in locally can be routed correctly.

Why does the JMM configuration change with routing options?

Only the options necessary for the appliance's selected routing method display. If you are using LDAP routing, the LDAP attributes provide the account default settings, so they are not available on the **Junk Mail Manager Configuration** page. For more information, see Junk Mail Manager LDAP Records on page 159. If you are using the Local Routing Table, you cannot configure remote Junk Mail Domains, so those options are not available on the **Junk Mail Manager Configuration** page.

In what order are JMM filters and lists applied?

JMM only applies filters and lists to configured Junk Mail Domains, but it does apply those filters and lists for all mail going to those domains. If other antispam scanning is done upstream, then JMM antispam scanning overrides previous spam scores. Messages that once receive a quarantine filter action are no longer subject to further quarantine actions.

Configuring Junk Mail Manager

Use the **Junk Mail Manager Configuration** page (**Home > Junk Mail Manager > Configuration**) to enable/disable Junk Mail Manager (JMM) and enable/disable the summary emails. If you are using the Local Routing Table for routing, you can also set basic mail store defaults for the quarantining of junk mail here. If you are using LDAP for routing, you can set remote Junk Mail Domains (those not local to the appliance) here, however, you can only administer Junk Mail Domains local to the appliance on the Junk Mail Domains pages.

Before you begin configuring JMM, you should have the following information:

- Make sure you have licensed and configured your appliance for antispam scanning. For more information, see Signature Edition, Principal Edition, and Premium Edition on page 130.
- The names of all the mail domains, and their hosts, whose junk mail you want JMM to quarantine. Each mail domain must be entered to JMM as a Junk Mail Domain. For example, for the mail domain `example.com` you would use the Junk Mail Domain `example.com`.
- The names of all your JMM enabled hosts, if you have more than one.

For more information, see the *Mirapoint MOS Configuration Guide*.

To configure Junk Mail Manager:

1. Go to **Home > Junk Mail Manager > Configuration**.

   The **Junk Mail Manager Configuration** page appears.

2. If JMM is not already enabled, click **Enable it**.

If you are enabling JMM for the first time, use the **Setup Wizard** (**Home > System > Setup Wizard**) to enable the feature. Do *not* enable JMM on the **Junk Mail Manager Configuration** page initially. If you do, there are complications that are noted in Troubleshooting Junk Mail Manager in Existing Setups on page 159.

When JMM is enabled many system records are added or modified at this point.

If you are using the **Setup Wizard** to configure JMM, it will ask you to choose and set up a routing method. Different JMM records are written depending on your choice. Once your routing method is set up, the wizard allows you to add Junk Mail Domains and hosts.

3. Enable or disable **LDAP Autoprovisioning**. If you have LDAP routing configured, select this to autoprovision JMM users. When a spam message is received for a user that does not have a JMM account, and this option is enabled, a JMM account is automatically created for that user, based on their existing LDAP records, and the Welcome message is sent.
4. **Set Account Defaults** for Local Routing Table routing *or* **Remote Junk Mail Domain to Host Mapping** for LDAP routing:

For Local Routing Table routing:

- **Message Expiration Timeout** - Type an integer for the amount of time a message can be quarantined in a single user's JMM account. The default timeout is 14 days. Mirapoint recommends that this be set to no less than 10 days (e.g., a week plus two weekends).
- **Folder Quota** - Type an integer for the amount of megabytes (MB) that can accumulate in a single user's JMM account quarantine folder, or leave blank for no quota (recommended). Type `-1` to remove a quota.

For LDAP routing:

For each JMM Domain located on a different JMM Host, specify the following information:

- **Remote Junk Mail Domain** - The mail domain whose junk mail a different JMM Host (not this appliance) is to handle. These domains should be configured on the remote JMM first.
- **Junk Mail Manager Host** - The name of the JMM appliance for that remote Junk Mail Domain.
- **Mail Host** - This option only displays when Microsoft Active Directory routing is used. The appliance that receives the non-junk mail for that remote Junk Mail Domain.

The domain table shows all domains that you add. Domains autoprovisioned for the appliance at install do not display. Remote domains that you add here must be created on the remote JMM host.

You can specify domains within the Setup Wizard's **Junk Mail Manager Domain to Host Mapping** page or the **Administer Junk Mail Domains** page (**Home > Junk Mail Manager > Junk Mail Domains > Administration**).

5. Enable or disable the **Junk Mail Summary**. The summary notification emails are enabled by default. If you disable the summaries, your users will need to log in to Junk Mail Manager in order to manage their junk mail.
6. Create a **Junk Mail Summary Custom Schedule**.
   a. From the **Available Hours** list, select the hour you want to add to the schedule.
   b. Click **Add**.

   The selected hours appear in the **Custom Schedule** list. Summaries are generated and sent at the hours specified. The default summary generating/sending hour is 4 am.

   The custom schedule option also appears on the end-user's JMM summaries page so they can choose to get junk mail summaries more often than once a day.
7. (Optional) If your site uses a proxy server (e.g., if direct Internet access is blocked by a firewall), designate the proxy server through which summary message links can be reached. In the **Proxy Hostname** text field, type the proxy hostname and click **Set**.

   If you want to use the appliance's hostname, leave this text field blank.

How Junk Mail Manager Quarantine Works

JMM uses the **Quarantine** filter action in its system default **Junk Mail Filter**. In this **Junk Mail Filter**, the **Quarantine** action is set to send matching messages (i.e., those categorized by the antispam scanner as junk mail) to the **Junk Mail** folder (or JMM interface, `http://hostname/spam`) where users can manage them. For information, see How Content Filtering Quarantine Works on page 192 and How Antivirus Quarantine Works on page 107.

Troubleshooting Junk Mail Manager in Existing Setups

If this is the first time you are enabling JMM and you enable the feature on the **Junk Mail Manager Configuration** page as opposed to the **Setup Wizard: Set Junk Mail Manager** page, LDAP might get confused.

To reset an appliance and restart the JMM setup without having to re-install, complete the following steps:

1. Go to **Home > Junk Mail Manager > Configuration**.

   The **Junk Mail Manager Configuration** page appears.

2. Click **Disable it**.

   This can also be done on the **Setup Wizard: Set Junk Mail Manager** page (**Home > System > Setup Wizard**).

3. Go to **Home > System > Routing**.
4. Delete your LDAP server on the routing page.
5. On the **Junk Mail Manager Configuration** page, the **Setup Wizard: Set Junk Mail Manager** page, or using the command-line interface (CLI), complete the following steps:

   a. Delete any local LDAP databases.
   b. Delete LDAP ACCESS.
   c. Delete LDAP MAILHOST.
   d. Delete LDAP QUARANTINEHOST.
   e. Make sure the Junk Mail Domain is not in MAILDOM.
   f. Delete the Junk Mail Domains.

6. On the **Setup Wizard: Set Junk Mail Manager** page, enable and configure JMM again.

Junk Mail Manager LDAP Records

These are the LDAP records that are required for Junk Mail Manager to work correctly. If you do not use Mirapoint schema, you must enter equivalent records into your LDAP.

These are the mandatory records:

- mailhost
- miquarantinehost
- micosdn: cn=Junkmail_Manager_default_cos
- miservice: msgexpiration
- miservice: quota
- miservice: antispam
- miservice: junkmailmanager
- mimailquota
- mimailexpirepolicy: QTNBOX.* 14 I
- midefaultjunkmailfilter::
  I0BNaXJhcG9pbnQtRmlsdGVyLTEuMA0KZmlsdGVyICJTeXN0ZW0g
  SnVuayBNYWlsIFJ1bGUiIFF1YXJhbnRpbmUgIlFUTkJPWC5KdW5rIE1haWwiIGFsbG
  9mIHN0b3ANCjpVQ0UgaXMgIm5vcm1hbCINCg==

In the CLI, the filter would look like this:

```
#@Mirapoint-Filter-1.0
filter "System Junk Mail Rule" Quarantine "QTNBOX.Junk Mail" allof stop
:UCE is "normal")
```

The following is an example:

```
dn: o=mira_route_top
objectclass: Organization
o: mira_route_top

dn: ou=domains,o=mira_route_top
objectclass: OrganizationalUnit
ou: domains

dn: miDomainName=primary,ou=domains,o=mira_route_top
objectclass: miDomain
midomainname: primary

dn: miDomainName=demo.com, ou=domains, o=mira_route_top
objectclass: miDomain
midomainname: demo.com

dn: mail=@demo.com, miDomainName=demo.com, ou=domains, o=mira_route_top
cn: domain entry
objectclass: mirapointUser
objectclass: mirapointMailUser
mail: @demo.com
mailhost: exammple0.mirapoint.com
miquarantinehost: example.mirapoint.com
micosdn: cn=Junkmail_Manager_default_cos, miDomainName=primary, ou=cos,
o=mira_route_top
```

```
dn: ou=cos,o=mira_route_top
objectclass: OrganizationalUnit
ou: cos

dn: miDomainName=primary,ou=cos,o=mira_route_top
objectclass: miDomain
midomainname: primary

dn: cn=Junkmail_Manager_default_cos,miDomainName=primary,ou=cos,o=mira_route_
top
miservice: msgexpiration
miservice: quota
miservice: antispam
miservice: junkmailmanager
objectclass: miClassOfService
cn: Junkmail_Manager_default_cos
mimailquota: 0
mimailexpirepolicy: QTNBOX.* 14 I
midefaultjunkmailfilter:: IOBNaXJhcG9pbnQtRmlsdGVyLTEuMAOKZmlsdGVyICJTeXNOZ
WOgSnVuayBNYWlsIFJ1bGUiIFF1YXJhbnRpbmUgIlFUTkJPWC5KdW5rIE1haWwiIGFsbG9mIHNO
b3ANCjpVQOUgaXMgIm5vcm1hbCINCg==
```

Managing Junk Mail Domains

Use the **Administer Local Junk Mail Domains** page (**Home > Junk Mail Manager > Junk Mail Domains**) to tell Junk Mail Manager (JMM) what domains have accounts for which JMM is to quarantine junk mail, in other words, any mail domain. Also, select Junk Mail Domains for administration, including antispam scanning options.

The **Administer Local Junk Mail Domains** page provides the following links:

- Administration - Add, find, select, or delete Junk Mail Domains. You must select a domain in order to administer it.
- Accounts - Add, find, or delete junk mail user accounts. You must select a domain in order to add accounts to it.
- Welcome Message - Customize the Welcome Message for new junk mail user accounts.
- Over-Quota Message - Customize the Over-Quota Message for junk mail user accounts that have exceeded their quota.
- Allowed Senders - Create or edit Junk Mail Domain allowed senders (senders whose mail will never be classified as junk mail).
- Blocked Senders - Create or edit Junk Mail Domain blocked senders (senders whose mail will always be classified as junk mail).
- Allowed Mailing Lists - Create or edit Junk Mail Domain allowed mailing lists (recipients whose mail will never be classified as junk mail).
- Message Filters - Create or edit Junk Mail Domain message filters.

Adding and Deleting Junk Mail Domains

Use the **Administer Local Junk Mail Domains** page (**Junk Mail Manager > Junk Mail Domains > Administration**) to tell JMM which mail domains it needs to quarantine junk mail for.

To add a Junk Mail Domain:

1. Go to **Home > Junk Mail Manager > Junk Mail Domains > Administration**.

   The **Administer Local Junk Mail Domains** page appears.

2. In the **Junk Mail Domain Name** text field, type the domain name of the mail domain.
3. (Optional) In the **Domain Disk Quota** text field, type the disk quota for the Junk Mail Domain in kilobytes (KB). If left blank, then no quota is applied.
4. (Optional) In the **Maximum Users** text field, type the maximum number of users that can access this Junk Mail Domain. If left blank, then a default of 20 users is applied.
5. Click **Add Domain**.

   Repeat these steps to add the domain names of all the mail domains in your deployment. You can edit the information for any existing Junk Mail Domain by selecting it from the domain list, and clicking the **Edit** icon ( ).

   After domains are added, this page allows you to select a Junk Mail Domain for administration. For more information, see Selecting a Junk Mail Domain on next page.

To delete a Junk Mail Domain:

1. Go to **Home > Junk Mail Manager > Junk Mail Domains > Administration**.

   The **Administer Local Junk Mail Domains** page appears. Click **Prev** and **Next** to page through the list of names, as needed. You can also use **Find** to locate existing Junk Mail Domains. For more information, see Finding Junk Mail Domains below.

2. Select the name in the domain list.
3. Click the **Delete** icon ( ).

   A confirmation page appears.

4. Click **OK**.

Finding Junk Mail Domains

On the **Administer Local Junk Mail Domains** page (**Home > Junk Mail Manager > Junk Mail Domains** or **Junk Mail Manager > Junk Mail Domains > Administration**) a list of existing Junk Mail Domain names appears in the table in the order in which they were created. The total number of domains appears as an alphanumeric number above and to the left of the table. When the domain list becomes too long to display on one page, you can page through the list by selecting **Prev** and **Next** accordingly.

To find a Junk Mail Domain:

1. Go to **Home > Junk Mail Manager > Junk Mail Domains** or **Home > Junk Mail Manager > Junk Mail Domains > Administration**.

   The **Administer Local Junk Mail Domains** page appears.

2. In the **Junk Mail Domains Name** text field, type the entire domain name or use the wildcard asterisk (*) to match any sequence of zero or more characters. For example, `fo*` finds domain `foo.com`, `foods.com`, `folly.com`, and so forth.

You can type the asterisk (*) wildcard alone in the text field to display all of the domain names on the appliance.

3. Click **Find**.

   The specified name appears in the domain list.

Selecting a Junk Mail Domain

When you select a domain, the **Domain *domain name*** indicator in the bottom left corner of the all of the Junk Mail Domains-related pages changes to the current selected Junk Mail Domain and all other domain specifications you make using the Junk Mail Domains-related pages act only on that domain.

For example, if you create a user, `george@example.com`, while the Junk Mail Domain `qtn.example.com` is current, you create a Quarantine folder that will receive the junk mail (as determined by the appliance's antispam scanner) for `george@example.com` and put that mail into George's `qtn.example.com` folder. George will open JMM (`qtn.example.com/spam`) to act on his junk mail.

To select a Junk Mail Domain to administer:

1. Go to **Home > Junk Mail Manager > Junk Mail Domains** or **Home > Junk Mail Manager > Junk Mail Domains > Administration**.

   The **Administer Local Junk Mail Domains** page appears.

2. Select the name in the domain list
3. Click **Select Domain**.

   You can also use **Find** to locate existing Junk Mail Domains. For more information, see Finding Junk Mail Domains on previous page.

Managing Junk Mail User Accounts

Use the **Add Junk Mail Account** page (**Home > Junk Mail Manager > Junk Mail Domains > Accounts**) to add or modify JMM accounts, or to find, rename, or delete an account. Make sure you select the proper Junk Mail Domain before administering JMM accounts. For more information, see Selecting a Junk Mail Domain above.

About Junk Mail User Accounts

A JMM account consists of a login name and password, and a main folder-quarantine.username. The user's login name is used as the address for their quarantine folder. By default, JMM user folders reside in a system folder called `quarantine`.

When a user logs in to JMM (`http://hostname/spam`), they see only their quarantine account folder. If they log into WebMail Corporate Edition/WebMail Direct they will see the default **Junk Mail** folder. Users can perform the following junk mail management tasks using JMM:

- Change their JMM account password
- Set message filters and some JMM options

Finding Junk Mail User Accounts

To find a junk mail user account:

1. Go to **Home Junk Mail Manager > Junk Mail Domains > Accounts**.

   The **Add Junk Mail Account** page appears.

2. In the **Account Name** text field, type the name of user account. For more information on wildcards, see Using Patterns and Wildcard Characters on page 191.
3. Click **Find**.

   The table displays the find results. Ten names display at a time.

Adding or Deleting Junk Mail User Accounts

Use the **Add Junk Mail Account** page to add, find, or modify JMM users, including setting folder quotas, and assigning a notification message when appropriate.

Make sure you set up your mail accounts on the mail hosts before creating JMM accounts as the welcome message is sent the instant each JMM account is created.

To add a junk mail user account:

1. Make sure you selected the proper Junk Mail Domain. For more information, see Selecting a Junk Mail Domain on previous page.
2. Go to **Home > Junk Mail Manager > Junk Mail Domains > Accounts**.

   The **Add Junk Mail Account** page appears.

3. In the **Account Name** text field, type the name for the user account. This name becomes the name of that user's folder under the `qtn` system directory, the first part of their JMM quarantine email address, and their login name.

If this account is for a DL, you type the DL name here. For more information, see Adding Junk Mail User Accounts to Distribution Lists on the facing page.

4. In the **Full Name** text field, type the complete name of the user. This name is displayed in messages alongside the user name.
5. (Optional) If you are using LDAP routing, you can use the LDAP username and password combination for the user's JMM account. To Use the LDAP password, select the **Use LDAP Password** checkbox.
6. In the **Password** text field, type a password for the user. A password is a secret text string (numbers and letters) that is case sensitive and up to 80 characters long.
7. In the **Confirm Password** text field, re-type the password.
8. In the **JMM Folder Quota** text field, type in kilobytes (KB) the quota amount for the folder. This is the quota for that user's Quarantine folder. All of their subfolders are included in the total set quota. You can completely remove a quota from a folder by typing `-1`.

   The **DL Notification Address** text field is only used of this account is for a DL. For more information, see Adding Junk Mail User Accounts to Distribution Lists on the facing page.
9. Click **Add Account**. Repeat steps 3 through 9 as necessary to add more users.

   The appliance creates an account in JMM for that user and incoming mail for that user that is categorized as junk mail is sent to this account.

To delete a junk mail user account:

1. Make sure you selected the proper Junk Mail Domain. For more information, see Selecting a Junk Mail Domain on page 163.
2. Go to **Home > Junk Mail Manager > Junk Mail Domains > Accounts**.

   The **Add Junk Mail Account** page appears.
3. Click **Prev** and **Next** to page through the list of names, as needed. You can also use **Find**. For more information, see Finding Junk Mail User Accounts on previous page.
4. Click the **Delete** icon (✕) next to the account name.

   A confirmation page appears.
5. Click **OK**.

Use the **Edit Junk Mail Account** page to change a JMM user password, folder quota, or distribution list owner notification.

To edit a junk mail user account:

1. Make sure you selected the proper Junk Mail Domain. For more information, see Selecting a Junk Mail Domain on page 163.
2. Go to **Home > Junk Mail Manager > Junk Mail Domains > Accounts**.

   The **Add Junk Mail Account** page appears.

3. Click **Prev** and **Next** to page through the list of names, as needed. You can also use **Find**. For more information, see Finding Junk Mail User Accounts on page 164.
4. Clicking the **Edit** icon ( ) next to the account name.

   The **Edit Junk Mail Account** page appears.
5. Make the necessary modifications to the account.

You can completely remove a quota from a JMM folder by entering -1.

6. Click **OK**.

Adding Junk Mail User Accounts to Distribution Lists

JMM can also manage the junk mail for a distribution list (DL). In this case, a DL is treated as an account. The expansion of the DL to member's email addresses happens after JMM processing.

To add a DL to a junk mail account:

1. Go to **Home > Junk Mail Manager > Junk Mail Domains > Accounts**.

   The **Add Junk Mail Account** page appears.
2. In the **Account Name** text field, type the name of the DL. For more information, see Adding and Deleting Junk Mail Domains on page 162.
3. In the **DL Notification Address** text field, type an email address for the DL owner. You can add multiple DL owners using the **Edit Junk Mail Account** page.
4. Click **Add Account**.

The welcome message, with login information, goes to all the DL owners as well as the junk mail summaries. If a DL owner clicks **Deliver**, the message is sent to all members of the DL. If a DL owner clicks **Approve**, the message is sent to all members of the DL and the sender is added to the DL account's allowed senders list. All of the DL owners can log in and manage the account.

Customizing the Welcome Message

You use the **Set Welcome Message** (**Junk Mail Domains > Junk Mail Domains > Welcome Message**) to customize the message that is delivered when a user's JMM account has been created. You can also select the character set used to encode the message. For example, if you select ISO-2022-JP and Japanese characters are used, the message is encoded in the ISO-2022-JP character set.

The welcome message you customize here is associated with the domain that you selected in the on the **Administer Local Junk Mail Domains** page (**Junk Mail Manager > Junk Mail Domains > Administration**).

To customize a Junk Mail Domain's welcome message:

1. Make sure you selected the proper Junk Mail Domain. For more information, see Selecting a Junk Mail Domain on page 163.
2. Go to **Home > Junk Mail Manager > Junk Mail Domains > Welcome Message**.

   The **Set Welcome Message** page appears.
3. If the welcome message is **disabled**, click **Enable it**.

   The welcome message must be **enabled** before customizing it.
4. Customize the text in the **From**, **Subject**, and **Message** text fields as desired.
5. (Optional) Select a character set for the message from the **Charset** drop-down menu. The default is UTF-8.
6. Click Apply.

The customized welcome message, along with the character set you specified (if any), is sent to users when their JMM account is created. To revert to the default welcome message, click **Restore Default**.

If the domain is assigned to a named brand, clicking **Restore Default** causes that named brand's welcome message to be sent to users when their accounts are created.

Customizing the Over-Quota Message

Use the **Set Over-Quota Message** page (**Junk Mail Manager > Junk Mail Domains > Over-Quota Message**) to customize the warning message that is delivered when a user's folder has gone over its allocated size limit. You can also specify the character set used to encode the message. For example, if you select ISO-2022-JP and Japanese characters are used, the message is encoded in the ISO-2022-JP character set.

The over-quota message you customize here is associated with the domain that you selected in the on the **Administer Local Junk Mail Domains** page (**Junk Mail Manager > Junk Mail Domains > Administration**).

To customize a Junk Mail Domain's over-quota message:

1. Make sure you selected the proper Junk Mail Domain. For more information, see Selecting a Junk Mail Domain on page 163.
2. Go to **Junk Mail Manager > Junk Mail Domains > Over-Quota Message**.

   The **Set Over-Quota Message** page appears.
3. Customize the text in the **From**, **Subject**, and **Message** text fields as desired.
4. (Optional) Select a character set for the message from the **Charset** drop-down menu. The default is UTF-8.
5. Click **Apply**.

The over-quota message, along with the character set you specified (if any), is sent to users when their folder quota is reached. To revert to the default over-quota message, click **Restore Default**.

Managing Allowed Senders for Junk Mail Domains

Once you have added a new, or selected an existing, Junk Mail Domain, use JMM's **Set Allowed Senders** page (**Junk Mail Manager > Junk Mail Domains > Allowed Senders**) to ensure that mail from certain senders is always sent to recipients and never classified as junk mail.

This page works in an identical manner to the antispam scanner's **Set Allowed Senders** page (**Antispam > Allowed Senders**). For more information, see Creating Advanced Content Filters on page 173.

Managing Blocked Senders for Junk Mail Domains

Once you have added a new, or selected an existing, Junk Mail Domain, use JMM's **Set Blocked Senders** page (**Junk Mail Manager > Junk Mail Domains > Blocked Senders**) to specify certain addresses that should never have mail received at that Junk Mail Domain.

This page works in an identical manner to the antispam scanner's **Set Blocked Senders** page (**Antispam > Blocked Senders**). For more information, see Blocked Senders.

Managing Allowed Mailing Lists for Junk Mail Domains

Once you have added a new, or selected an existing, Junk Mail Domain, use JMM's **Set Allowed Mailing Lists** page (**Junk Mail Manager > Junk Mail Domains > Allowed Mailing Lists**) to ensure that mail from certain senders is always sent to recipients and never classified as junk mail.

This page works in an identical manner to the antispam scanner's **Set Allowed Mailing Lists** page (**Antispam > Allowed Mailing Lists**). For more information, see Allowed Mailing Lists.

Managing Message Filters for Junk Mail Domains

Once you have added a new, or selected an existing, Junk Mail Domain, use JMM's **Message Filters** page (**Junk Mail Manager > Junk Mail Domains > Message Filters**) to create custom filters and manage your existing filters.

This page works in a similar manner to the **Advanced Content Filters** page (**Content Filtering > Advanced**). For more information, see Advanced. The difference between the two pages is that for JMM's **Message Filters** page you do not have the option of directing the filter towards a Destination Domain because the filter you create on that page applies only to the Junk Mail Domain that you have selected or logged in to as a Domain Administrator. In order to create a system-wide filter, use the **Advanced Content Filters** page.

Enabling LDAP Provisioning for Junk Mail Manager

Enabling LDAP provisioning for Junk Mail Manager (JMM) on your Message Server lets you write to your LDAP database JMM domain and user information. To do this, you must enable LDAP provisioning, ensure that your Message Server and JMM host point to the same LDAP server, and use the same attributes (with the exception of `user:quota` on the JMM host). When you create domains and/or users on your LDAP-enabled Administration Suite pages on the Message Server, the necessary LDAP records for corresponding Junk Mail domains and users are automatically created.

You must enable LDAP GUI before you can enable LDAP GUI-JMM for JMM. However, you must enable LDAP GUI on your Message Server, not on your JMM host (e.g., a RazorGate). Once LDAP GUI and LDAP GUI-JMM are enabled, domains and users that you create on your Message Server are automatically added to your a LDAP server as JMM domains and users. For more information, see the *Mirapoint Message Server Administrator's Guide*.

Bulk Creating Junk Mail User Accounts

The **Bulk Create Accounts** page (**Home > Junk Mail Manager > Bulk Create Accounts**) lets you import a text file containing information about your existing user accounts. The format of the file is a newline separated text file containing the fully-qualified email address of each account. Additionally, for each account, you can include the user's full name and password. If you do not include the full name, the appliance uses the fully-qualified email address to derive a name. If you do not include the password, the appliance creates a random password for the account and includes that password in the welcome message. For information on JMM welcome messages, see Customizing the Welcome Message on page 166.

You must create your Junk Mail Domains *before* bulk creating Junk Mail Manager (JMM) accounts. For more information, see Managing Junk Mail Domains on page 161. Be sure to set up your mail accounts on the mail hosts before creating any JMM accounts as the welcome message is sent the instant each account is created. Mirapoint also recommends using LDAP provisioning for JMM accounts. For more information, see the *Mirapoint MOS Configuration Guide*.

To bulk create junk mail user accounts:

1. Go to **Home > Junk Mail Manager > Bulk Create Accounts**.

   The **Bulk Create Accounts** page appears.

2. In the **Filename** text field, type the directory path to the file that contains the user account data, in the format described in Formatting the Input File on the facing page, or click **Browse** to find the file.
3. Click **Create Accounts**.

   A message displays indicating the completion or any problems.

The appliance parses your input file and creates accounts based on the user name, domain name, full name and password scanned from each line. If the domain does not exist, the appliance stops the process and displays an error on the page. If the user or folder already exists, the appliance skips to the next line. If the password field is "" (an empty string) or `PLAINTEXT:LOCAL`, the appliance generates a password for the user that is included in their welcome message. For the non-local password, the appliance displays in their welcome message a note that their password is "`Their regular password`".

Formatting the Input File

The format of the input file for bulk creating accounts must be:

`fully_qualified_email_address "fullname" "password"`

Where:

- `fully_qualified_email_address` is the hostname plus the domain name. For example, `user@example.com`
- `fullname` is the user's first and last names, enclosed in quotes (") to allow for spaces
- `password` is the user's password. If left empty ("") the appliance generates a random password

  The `password` argument can be used to specify whether the authentication for these accounts is via non-local or local passwords. If authentication is via a non-local password, the password argument should contain one of the valid authentication schemes, for example, `PLAINTEXT:LDAP`. For more information on valid authentication schemes, see the *Mirapoint Administration Protocol Reference*.

Here are some annotated examples of the lines you can specify in the input file:

```
joe@example.com
```

In this example, there is no password or full name included, so JMM generates a random password for this user.

```
joe@example.com "" ""
```

In this example, there is an empty string ("") instead of a full name, and an `AUTH` type and password, so JMM generates a random password for this user with no full name.

```
joe@example.com "Joe Smith" "joepassword"
```

In this example, JMM uses the specified full name and password for this user.

```
joe@example.com "" "joepassword"
```

In this example, JMM uses the specified password for this user, but the account has no full name.

```
joe@example.com "Joe Smith" ""
```

In this example, JMM uses the specified full name and generates a random password for this user.

```
joe@example.com "Joe Smith" "PLAINTEXT:LDAP"
```

In this example, JMM uses the specified full name and the password `AUTH` type and database for this user.

Other than the enclosed quotes, double quotes are disallowed in the fields, even if you use an escape character. That is, an entry such as:

```
user1@dom1.com "A \"Test\" account" ""
```

Would create an account with a full name of `A \`.

Sending a Junk Mail Summary Message

Use the **Send Junk Mail Summary** page (**Home > Junk Mail Manager > Send Summary**) to send an ad hoc junk mail summary message to a single user or multiple users. Typically JMM summary messages are sent to users automatically based on a schedule. For more information, see Configuring Junk Mail Manager on page 157.

To send an ad hoc junk mail summary message to users:

1. Go to **Home > Junk Mail Manager > Send Summary**.

   The **Send Junk Mail Summary** page appears.

2. In the **E-mail Addresses** text field, type in the email addresses, separated by commas (,).
3. Click **Send**.

A JMM summary message is generated and sent to the specified addresses.

Chapter 4: Managing Content Filters

This chapter describes how to set up content filters at the domain level and user level.

A content policy is a set of rules for what content is allowed to whom. You set content policies on a domain-level basis and implement them through content filters (or message filters). A *content filter* is a method of identifying a message and specifying an action for that message. Content filters provide the ability to finely control your mail flow. Administrators can set up domain-level and user-level (or personal) filters. Additionally, administrators can set up content policies on an appliance-wide basis for all, local, or non-local email.

Content filters can trigger, as configured, at any stage of the mail stream. Domain-level filters and lists are always applied before user-level filters and lists. Antispam scanning is done before content filtering by default. For more information, see Managing Antispam Scanning on page 125.

The following topics are included:

- Creating Content Policies below
- Creating Advanced Content Filters on next page
- Managing Wire Taps on page 193
- Managing Blocked Addresses Filters on page 195
- Managing Blocked Messages Filters on page 197
- Managing Blocked Attachments Filters on page 199
- Managing Redirected Attachments Filters on page 202
- Managing Corporate Word List Filters on page 204
- Managing Objectionable Word List Filters on page 206

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.

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 intellectual property (IP) and trade secrets—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 more information, see Creating a Mail Signature on page 68.
- 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.

For examples of domain-level filters you can create to enforce various content policies, see Content Policy Enforcement Filter Examples on page 185.

Creating Advanced Content Filters

Use the **Advanced Content Filters** page (**Home > Content Filtering > Advanced**) to create content filters and manage the other filters.

The rules and conditions specified in a domain-level content filter are applied to all incoming messages to that domain. In order to modify or administer a domain, you must select it. When you do this, the **Domain *domain name*** indicator in the bottom-left corner of the all of the **Domains**-related pages change to the current selected domain and the **Destination Domain** options do not display.

Additional information about the advanced content filters is provided in the following sections:

- Content Filtering Options below
- Reordering a List of Filters on page 187
- Using the Filter List on page 188
- Using Patterns and Wildcard Characters on page 191
- How Content Filtering Quarantine Works on page 192

Content Filtering Options

Content filters provide the ability to finely control your mail flow. You can set up domain-level content filters users or user-level (or personal) content filters. The **Destination Domain** options allow you to specify certain pools of recipient addresses to which the filter will apply. For more information, see Creating a Message Filter on page 177.

Each domain or folder (i.e., user account) can have multiple filters, which are evaluated in the order created for each incoming message. You can change the order on the **Advanced Content Filters** page. For more information, see About Filter Priorities and Ordering below and Reordering a List of Filters on page 187.

About the Destination Domain

Unless you log in as a delegated Domain Administrator, or specifically select a domain to administer, or are administering a Junk Mail Manager (JMM) domain, the option to choose a **Destination Domain** displays at the top of various Administration Suite pages. The **Destination Domain** option allows you to specify a pool of recipient addresses for the filter.

Figure 14 Destination Domain Option

The **Destination Domain** options are:

- **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
- **Any** - Filter any messages routed to or through the appliance on which the filter is created.
- **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
- **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

The order in which these filters are applied is as follows:

- The **Any** filter is always applied before any other destination domain filters. Usually, the **Primary** domain filter is applied next.
- If the message is for local (i.e., inbound), then the **Local** and **Primary** domain filters are applied, in that order, after the **Any** domain filters.
- If the message is non-local (i.e., outbound), then only **Non-local** domain filters are executed, after the **Any** domain filters.

About Filter Priorities and Ordering

Filters you create are assigned one of three priorities:

- Priority 100 - Filter is applied before antivirus and antispam scanning. This priority is set on the **Add/Edit Advanced Content Filter** page by selecting the **Filter this message before performing Antivirus and Antispam scanning** filter action.
- Priority 450 - Filter is applied before quarantine. This priority is set on the **Add/Edit Advanced Content Filter** page by selecting the **Send to Quarantine folder** filter action.
- Priority 500 - Filter is a domain filter. This priority is set creating the filter within that domain on the **Message Filters** page.

Filters are applied using the following priority order by default:

1. 100 (High Priority) filters **Any** Destination Domain
2. 100 (High Priority) filters **Primary** Destination Domain
3. 100 (High Priority) filters **Local/Non-local** Destination Domain
4. 100 (High Priority) delegated domain filters
5. antivirus scanning
6. antispam scanning
7. 450 filters **Any** Destination Domain
8. 450 filters **Primary** Destination Domain
9. 450 filters **Local/Non-local** Destination Domain
10. 450 filters delegated domain filters
11. 500 filters **Any** Destination Domain
12. 500 filters **Primary** Destination Domain
13. 500 filters **Local/Non-local** Destination Domain
14. 500 filters delegated domain filters

If you select the filter action, **Filter this message before performing Antivirus and Antispam scanning**, that filter is a priority 100 filter. If you do *not* select this 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 **Add/Edit Advanced Content Filter** 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.

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:

1. antivirus scanning
2. antispam scanning
3. domain signatures
4. domain filters (including primary domain)
5. end-user filters

The **Advanced Content Filters** page indicates the order in which configured filters are applied. You can re-order the list to change the processing order. For more information, see and Reordering a List of Filters on page 187.

About MIME and Filtering Attachments

MIME stands for Multipurpose Internet Mail Extension, a standard for multi-part, multimedia, email messages. The old Internet mail standards treated the body of a message as a single, indivisible unit. As its name suggests, MIME extends these standards to 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), 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, except the message body, are considered attachments and filtered if the **Attachment MIME Type** parameter is specified.

When a message is filtered, the various encodings are converted to UTF-8 and then the filter is applied.

A normal message with no attachments 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 have the 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. This can be done by clicking **Open** when viewing a message in WebMail Direct Standard Edition or right-clicking on a message and selecting **View Source** within the **Message Pane** when viewing a message in WebMail Corporate Edition.

Figure 15 Example Message Source

```
Return-Path: <k@mirapoint.com>
Received: (from mirapoint.com )
        by mirapoint.com (MOS 3.8.0.16)
        with HTTPS/1.1 id AAH02744 (AUTH kyoko);
        Tue, 18 Apr 2006 17:35:49 -0700 (PDT)
From: Kyoko <k@mirapoint.com>
Subject: Policy Server
To: LaSandra <lb@mirapoint.com>
X-Mailer: Mirapoint Webmail Direct 3.8.0.16
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20060418173549.AAH02744@mirapoint.com>
Date: Tue, 18 Apr 2006 17:35:49 -0700 (PDT)
X-Junkmail-Whitelist: YES (by domain whitelist at mirapoint.com)
X-Mirapoint-RAPID-Raw: score=unknown(0),
        refid=str=0001.0A090206.44458481.0038,ss=1,fgs=0,
        ip=0.0.0.0,
        so=2006-04-13 08:43:17,
        dmn=5.1.5/2006-04-17
X-Mirapoint-Loop-Id: e1efbb75a1eadd421ad5930a5b0a7893

Hi LaSandra and Matt,

A quick question for you.
```

Common Virus Attachment Names

The following is a list of file extensions that often have viruses in them. A *file extension* refers to the characters 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, however, this is just a list of the common types.

```
.Trojan
.scr
.vbs
.pif
.hta
.reg
.bat
```

Microsoft publishes a list of attachments that they recommend you block. You can find the list at the following URLs:

- http://office.microsoft.com/en-us/assistance/HA011402971033.aspx (for Outlook 2003)
- http://technet.microsoft.com/en-us/library/cc179163.aspx (for Outlook 2007)

Creating a Message Filter

To create a message filter:

1. Go to **Home > Content Filtering > Advanced**.

   The **Advanced Content Filters** page appears.

2. 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 Domain, these options do not display.

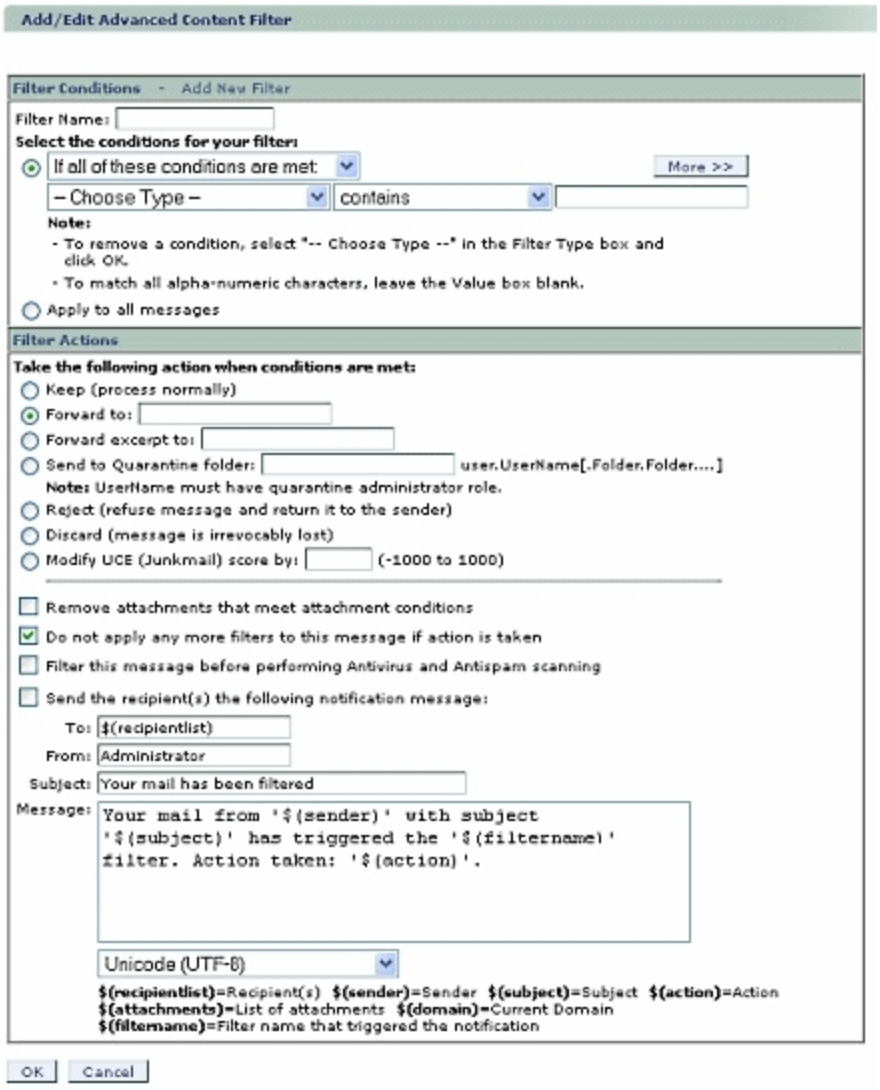
Select one of the following domain filters:

- **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
- **Any** - Filter any messages routed to or through the appliance on which the filter is created.
- **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
- **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

The filter looks only at the mail addressed to the selected user group. For more information, see About the Destination Domain on page 174.

3. Click **Add Filter**.

   The **Add/Edit Advanced Content Filter** page appears.



4. In the **Filter Name** text field, type the name of the filter. Do not use quotation marks (") in the name.

   The name displays in the filter list for that filter.

5. In the **Filter Conditions - Add New Filter** area specify a **Filter Name** and target condition from the drop-down menu. Select one of the following:

- **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 to Step 6.

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 to Step 9.

6. Select a filter type from the drop-down menu. This is the part of the message that the filter will scan. The filter type you select determines the value you must specify (i.e, text, special characters, or integers). The filter types are:
   - **From** - The sender line.
   - **To/CC** - The recipient's lines (does not include blind carbon copy (BCC) recipients. You cannot filter on the BCC field).
   - **Subject** - The subject line.
   - **Body** - The message body; text and text attachments including Plain text, HTML text, and Rich Text. This is the same as choosing **bodydecoded** (the decoded form of all MIME parts of the message) in the command-line interface (CLI). If you are looking for an 8-bit string, this option may be best. This option may 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.

For example, because whitespace is removed, a **Body** filter type 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 selected **Open** in WebMail Direct Standard Edition or **View Source** in WebMail Corporate Edition for that message. This is the same as choosing **Body** (the raw RFC 822 text) in the CLI. If you are looking for a word (ASCII text) in a message, this option may be best.
   - **Body (binary)** - Use this to find the binary value of an alphanumeric string in the message. For example, to use this option to find the Yen character (i.e., hex A5), you would enter `\xA5`.

Use backslashes (\) to separate characters. Backslashes (\) not followed by `x` are ignored and `A-F` is case-insensitive. This is the same as choosing **bodydecodedbinary** (unrolls all the MIME parts and allows binary searches) in the CLI.

If you are looking for a virus signature pattern such as `(\x64\xA2\x66\x66\x02)`, this option might be best.

- **To (message envelope)** - A specific recipient's address; this enables filtering on a particular user even on mail coming to them via a distribution list or blind copy. Useful especially for domain filters.
- **From (message envelope)** - A specific sender's address; this is similar to **Return-path** but helps ensure that the responsible party for the mail is filtered. For example, this option can be useful in filtering on mailing list copies; the mailing list manager would be the **From (message envelope)** address.
- **Return-path** - The return-path address; not useful with domain filters as the return path may be re-written, use **From (message envelope)** instead.
- **X-Junkmail** - The `X-Junkmail` header that is added to messages that the Junk Mail filter categorizes as spam.
- **X-Junkmail-Whitelist** - The `X-Junkmail-Whitelist` header that is added to messages that come from senders on a safelist (Allowed Senders/Allowed Mailing Lists).
- **X-Mirapoint-Virus** - The `X-Mirapoint-Virus` header that is added to messages that are found to contain viruses. This may be useful as a filter for virus deleted messages. For more information, see Filtering Out VIRUSDELETED Messages on page 184.
- **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; users should be warned to never open attachments from unknown sources.
- **X-DSN-Junkmail**, **X-DSN-Junkmail-Status**, and **X-DSN-Mirapoint-Virus** - Delivery Status Notification (DSN) 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 the **Destination Domain** is set to **Any** or **Non-local**.
- **Attachment MIME Type** - The attachment media type. Choices include the top level MIME types: text, multipart, message, application, image, audio, video, and model; use the **matches** rather than the **contains** content condition and search for something specific (for example, `application/vbs`). For more information, see How Content Filtering Quarantine Works on page 192.
- **Attachment file name** - The attachment name. You can use the asterisk wildcard; for example, `*.vbs`.
- **UCE (Junkmail) score** - An integer to be added to the message's UCE score. For more information, see About Antispam Scanning and Threshold on page 133.
- **Message size (bytes)** - The value must be an integer.

7. Select a content condition for the filter type from the drop-down menu. The content conditions are:

- **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 this option to filter on mail with empty To/CC lines.
- **matches** - The object must match the text you enter. Wildcards may be useful; 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. Using wildcards is useful.
- **regex-matches** - The object must match the regular expression you enter; use with regular expressions only. Can be used to adjust the UCE score; for details see Using Regex Filters to Modify UCE Scoring on page 184.
- **does not regex-match** - The object must not match the regular expression you enter; use with regular expressions only. Can be used to adjust the UCE score. For more information, see Using Regex Filters to Modify UCE Scoring on page 184.
- **is less than** - The object value must be less than the integer you enter. Using wildcards is useful.
- **is more than** - The object value must be more than the integer you enter. Using wildcards is useful.

8. In the text field, type a value for the filter type, using text or integers as appropriate. You can use the following wildcard characters:

   - **Asterisk (*)** - Matches any sequence of zero or more characters. For 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. For example, to find all messages from `Maria` or `Marie`, use these filter conditions: **From: matches** `"Mari?"`

   The conditions for the filter are set as specified. Click **More>>** if you want to add additional filter types and content conditions.

9. In the **Filter Actions** area specify a response by selecting one of the following options:

   - **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, For more information, see Keep (process normally) Filter Examples on page 183.
   - **Forward to** - Type in any valid email address or mailhost. The format for a mailhost is `@`*`hostname`*, where *`hostname`* is the mailhost prefaced by an ampersand (e.g., `@mycompany.com`). Matching messages are forwarded as specified. This option is selected by default. For more information, see Forward to vs. Send to Quarantine Folder on page 183.

The **Forward to** action sends the message directly to the specified email address or hostname but does not save a copy on the appliance.

- **Forward excerpt to** - Type in any email address. The first several lines of matching messages are forwarded as specified. Use this option in conjunction with wireless devices.
- **Send to Quarantine folder** - Type in the fully-qualified folder name for any user that has the **Quarantine Administrator** role; for example, `user.UserName.FolderName` (folder names are optional. If not specified, the Inbox is used). If nothing is specified in the text field, `user.QuarantineAdmin` is used by default. Mail meeting the filter conditions is sent to this folder. A Quarantine Administrator can then decide to restore the message to the mail queue, or reject it. For more information, see Forward to vs. Send to Quarantine Folder on next page and How Content Filtering Quarantine Works on page 192.

For domain specific filters, this folder name (whether fully qualified or `user.QuarantineAdmin`) must match a user in that delegated domain that has the **Quarantine Administrator** role.

- **Reject (refuse message and return it to the sender)** - Matching messages are bounced back to the sender. The recipient receives a message that the action was taken.
- **Discard (message is irrevocably lost)** - Matching messages are deleted. The recipient does not receive a message that the action was taken.
- **Modify UCE (Junkmail) score** - Type in 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** within WebMail. 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** filter actions and places the new filter rule above the **Junk Mail Filter** rule in order of precedence. For more information, see About the Junk Mail Filter on page 132.

If JavaScript is disabled, it might be necessary to apply these adjustments manually.

Additionally, you can specify:

- **Remove attachments that meet attachment conditions** - 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. This is option selected by default.
- **Filter this message before performing Antivirus and Antispam scanning** - The message will be passed to antivirus and antispam scanning after it has been filtered by the preceding filters.

  By default, filters that you create on the **Advanced Content Filters** page, with a filter action other than **Send to Quarantine folder**, are processed after antivirus and antispam scanning and are priority 500 filters; this is also true for delegated domain-level content filters. However, if you select the **Filter this message before performing Antivirus and Antispam scanning** option, the filter will be a priority 100 filter. If you do *not* select this option, but do select the **Send to Quarantine folder** option, the filter will be a priority 450 filter. For more information, see About Filter Priorities and Ordering on page 174.

- **Send the recipient(s) the following notification message** - The message recipient will receive the default message or you can change the To, From, Subject, Message text, and/or encoding. Variables that you can use are given below the encoding drop-down menu. By default the character set used in the notification message is **Unicode (UTF-8)**.

10. Click **OK**.

    The appliance accepts the settings and a description of the filter appears within a table on the **Advanced Content Filters** page. Incoming messages and attachments are filtered and acted on as directed.

Keep (process normally) Filter Examples

The **Keep (process normally)** filter action 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 is *not* selected
  - Filter Two would have the same conditions as Filter One, and these actions:

    Keep (process normally) is selected

    Do not apply any more filters to this message if action is taken is 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.

This filter action, like all filter actions except **Discard** and **Quarantine**, apply only to that filter priority level. Filters at a different priority level might still act on the message. For more information, see About Filter Priorities and Ordering on page 174.

Forward to vs. Send to Quarantine Folder

There are two important differences in between the **Forward to** and **Send to Quarantine Folder** filter action options:

- The address you can enter.

For the **Forward to** filter action, if you know the user is local to the appliance, you can just enter the username, for example, `UserName@example.com`. For the **Send to Quarantine Folder** filter action, you must enter the fully-qualified folder address of a user local to the appliance, for example, `user.`*`UserName`*`.`*`FolderName`*. You must preface the address with `user.`*`UserName`*, but *`FolderName`* is optional. If you omit the folder name the message will go to the username's Inbox. Regardless of the filter action used, the address must have the **Quarantine Administrator** role in order to use the **Deliver** option within WebMail. For more information, see About the Quarantine Administrator User on page 55.

- The way the actions treat the message.

  The **Forward to** filter action simply delivers the message to the forwarding address. The **Send to Quarantine folder** filter option uses special coding to wrap the message so that if it is released back to the mail queue (via the **Deliver** option in WebMail) it is delivered to the recipients without indication that it was in quarantine.

Using Regex Filters to Modify UCE Scoring

The **regex-matches** filter option matches against the regular expression (Regex) you enter as the filter condition value. A regular expression is a way of representing data using symbols. You must enter a regular expression if you choose this filter content condition. For a fundamental explanation of regular expressions, see http://www.dc.turkuamk.fi/docs/gnu/rx/rx_3.html.

You can use **regex-matches** in a filter to modify the UCE (junk mail) score that the antispam scanner assigns to messages. The following filter provides an example:

Filter Name: `regex-matches example`
If all of these conditions are met:
From
regex-matches
`example.*com`
Modify UCE (junkmail) score by: `50`

In a received message header, if the strings `example` and `com` occur separated by any number of characters the UCE (junk mail) score is increased by `50`.

Filtering Out VIRUSDELETED Messages

There are many spamming viruses (for example, W32/Sobig-F) that send themselves to addresses stored on an infected computer. Mirapoint's antivirus scanner removes, cleans, or ignores the virus-infected attachment (depending on your antivirus configuration, see Managing Antivirus Scanning on page 105), and then 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**.

The appliance must have an antivirus license.

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) select **Discard** for the **Filter Action**, and use the following for the **Filter Conditions**:

X-Mirapoint-Virus contains `Sobig-F`

Alternatively, to filter on all flavors of the Sobig virus, the **Filter Conditions** could be:

X-Mirapoint-Virus matches `*Sobig*`

As new viruses appear, they can be added to the filter using **More>>** in the **Filter Conditions** area.

Content Policy Enforcement Filter Examples

You should set policy content limitations using domain-level content filters. Most content policy filters are on outgoing email, so you should set the **Destination Domain** to **Non-local** for each policy enforcement filter you create. If you set the **Destination Domain** to **Any**, then all incoming and outgoing mail is filtered.

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, create a corporate word list or objectionable word list filter. Words that might be used in a corporate word list filter include:

- Proprietary
- Confidential
- Internal

For more information, see Managing Corporate Word List Filters on page 204 and Managing Objectionable Word List Filters on page 206.

Filtering on Mail Sent to Competitors

This filter scans the **To (message envelope)**, that includes BCC (blind carbon copy) recipients, and quarantines messages that are sent to competitors.

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

Or,

To (message envelope)
matches
`competitor B`
Send to Quarantine folder: `user.QA.socsecnums`

In this example, two filter conditions (one for `competitor A` and the other for `competitor B`) are created, but you can create as many as conditions needed.

Filtering All Mail Outgoing From an Address

Create a wire tap content filter where the **Destination Domain** is **Non-Local**, so all mail outgoing from the specified address is sent to the specified **Forward to** address where it can be examined. For more information, see Managing Wire Taps on page 193.

Filtering Outgoing Mail with Too Many Recipients

To filter out (i.e., bounce) all outgoing mail messages with more than 50 recipients, use the **Maximum Recipients per message** option on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**). The default maximum number of recipients is 50000. For more information, see Managing the SMTP Service on page 42.

Filtering Over-sized Messages

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

Destination Domain = Non-local
Filter Name: `BounceMessageTooLarge`
If all of these conditions are met:
Message size (bytes)
is more than
`134217728`
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 the $(filtername) filter.`

The advantage of restricting the message size with a content filter is that you can send a custom notification message. However, you can also restrict the message size using the **Maximum Message Size** option on the SMTP service's **Main Configuration** page (**Home > System > Services > SMTP > Main Configuration**). The default maximum message size is 31457280 bytes (or 30 megabytes). For more information, see Managing the SMTP Service on page 42.

Reordering a List of Filters

Before and during message acceptance, SMTP authentication, relay and blocked domains, and Realtime Blackhole Lists (RBLs) are processed. After message acceptance, the default order of operations among content filters is as follows:

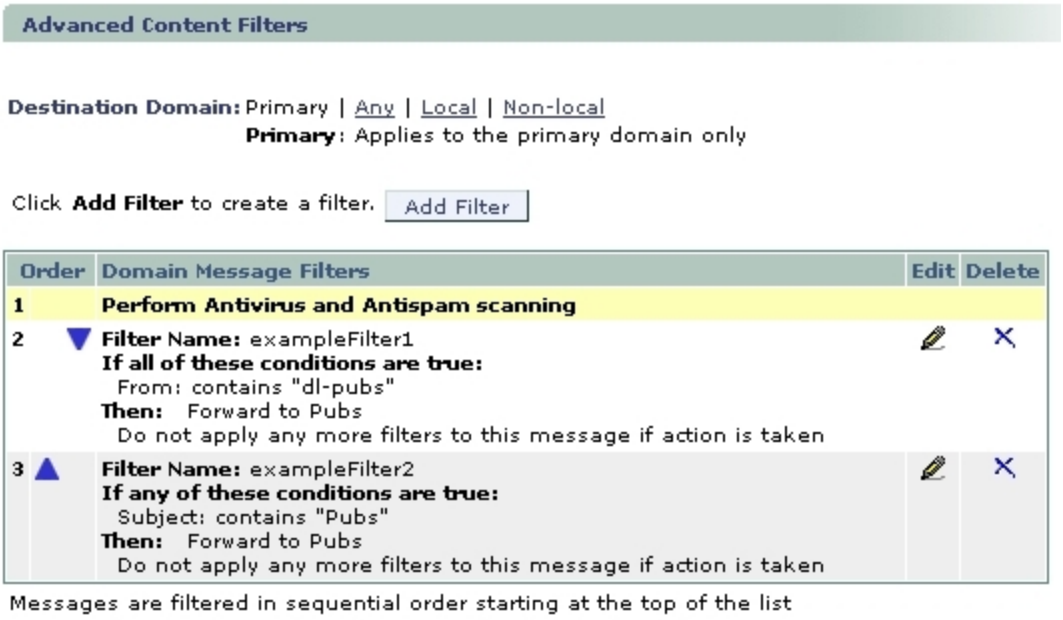
1. antivirus
2. antispam
3. domain signatures
4. domain filters (including primary domain)
5. end-user filters

Each incoming message is filtered in the order the filters appear in the **Advanced Content Filters** 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). For information on how the destination domain for a filter effects the order in which it is executed, see About the Destination Domain on page 174 and About Filter Priorities and Ordering on page 174.

To reorder a list of content filters:

1. Go to **Home > Content Filtering > Advanced**.

   The **Advanced Content Filters** page appears.



2. In the table, 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, click on the **down-arrow** (▼) in the **Order** column.
   - Click the **Edit** icon (✎) for a filter. On the **Add/Edit Advanced Content Filter** page, move a filter either above or below the **Perform Antivirus and Antispam scanning here** point, by selecting or deselecting the **Filter this message before performing Antivirus and Antispam scanning** filter action checkbox.

Using the Filter List

All of the content 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.

Managing a filter list is similar for all content filters. Filter lists are processed as follows:

- A word list is imported for the current domain. Each line forms a pattern, which is UTF-8 normalized, as defined by the Unicode specification. Uppercase letters are converted to lowercase.

Mirapoint appliances convert supported character set encodings into UTF-8. Therefore, depending on the original encoding, there is a possibility that the conversion might cause issues with filtering.

- 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 (i.e., portion of an email message) is also UTF-8 normalized, unless it is a header address or a 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 (i.e., line), word lists 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 lowercase.
- The pattern and filter attribute are compared word by word, moving forward one word at a time, words being separated by a delimiter. If all the words match and we run out of words in the pattern, the comparison returns **MATCH**, and searching terminates.

Strings of delimiters are treated as a single delimiter. Any delimiter matches any other delimiter.

- 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 in the word list, if any.

Word lists 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" will trigger on:

```
"a big

match"
```

The intention is that all the following match the end/start pattern, for example:

```
Fragment end... start another!
Fragment end? Start another.
Fragment end!! Start another.
“Fragment end.” “Start another.”
```

In the following example, pattern `a@b.com` matches any of the following patterns, but not `a1@b.com` nor `abba@b.com` addresses:

```
a@b.com
"a"@b.com
<a@b.com>
<"a"@b.com>
```

However, the pattern `a1@b.com` would match input `a1????b.com` because all delimiters match each other, and multiple delimiters are compressed to a single delimiter.

To create, edit, or delete a filter list for any content filter (wire taps, blocked addresses, blocked messages, etc.):

1. To add an initial filter list, either import an existing list, or in the **Add/Edit List** area, add the appropriate information into one of the following text field options:
   - **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. Word list filters match on whole words, not parts of words. So, phrases may 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 175.
2. Click **Add** and repeat step 1 as needed.

You cannot separate word list entries with spaces or semi-colons (;), each entry must be on a separate line. Therefore, you must make your entries one at a time.

In the **Edit List** area, a filter list displays the trigger text you added.

3. To change the filter list, do one of the following:
   - Type a 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 edit a filter list entry. You must delete the entry you want to change, then add it back.

If you enter new text and click **Add**, that new filter trigger displays in the filter list. If you select an address, word, or attachment (respectively) and click **Remove**. On the **Confirm Delete** page that appears, click **Remove**.

4. To import a filter list, enter the filename and path of the list (a text file), or browse to it and click **Import**.

   The selected list is loaded to the page and displays in the **Edit List** area. The imported word list replaces any existing word list that you may have previously imported or manually created. To save your existing word list, export it and incorporate it into your new word list. For more information, see Integrating a New Word List below.

5. To export a filter list, click **Export**.

   A **File Download** dialog box opens allowing you to open the list file or save it as a text file.

Integrating a New Word List

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

Using Patterns and Wildcard Characters

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 (?) - Matches any single character. For compatibility with the IMAP4 protocol, the 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 dot (.).
- Percent sign (%) - Matches zero or more characters, not including folder hierarchy separators. This wildcard is provided for compatibility with the IMAP4 protocol. However, it is interpreted as a wildcard *only* in folder names.

For example, using the search pattern `ann?` would find the following usernames:

```
anna anne
```

Using the search pattern `jo*` would find the following usernames and folder names:

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

How Content Filtering Quarantine Works

The **Send to Quarantine folder** filter action is available for all the content filtering filters and **Advanced** content filters. You can use any WebMail user account that has the role of **Quarantine Administrator** to receive messages via the **Send to Quarantine folder** filter action. For more information, see About the Quarantine Administrator User on page 55. For more information about message filters, see Creating a Message Filter on page 177.

You can still create a `QuarantineAdmin` user and use that address (i.e., `user.QuarantineAdmin`) as the quarantine address. If you type in `user.QuarantineAdmin`, the appliance auto-creates the **QuarantineAdmin** folder (local to the appliance) when the first mail that receives that filter action arrives. If you type in the address of a Quarantine Administrator user account other than `user.QuarantineAdmin`, the appliance does not auto-create the folder.

If you enter a different folder name, it is not auto-created. If you do not enter any folder name, `user.QuarantineAdmin` is used. The folder name you enter, or the default folder, `user.QuarantineAdmin`, is domain specific if the filter you create is for a delegated domain. Make sure that you have the `QuarantineAdmin` user or another user with the **Quarantine Administrator** role, in the delegated domain.

When you select the **Send to Quarantine folder** filter action and specify an address, mail meeting the filter conditions is sent to that address. The Quarantine Administrator can view the quarantined messages in WebMail, and decide to reject the messages or allow them to be delivered normally.

The **Send to Quarantine folder** filter action generates a new message from `Administrator@`*`hostname`* that contains the original message, and sends it to the specified quarantine address. If the message is released back to the mail queue through the **Deliver** button, only the original message is delivered. The message has one MIME part; in this there are three sub-parts:

- A text/plain part describing what this message is
- A message/vnd.mirapoint.rfc2821envelope (MIME type message/vnd.mirapoint.rfc2821envelope)
- The message body

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 list (DL) or sent from a mailing list is filtered. Mirapoint also recommends making sure that this filter (that includes the **Sent to Quarantine folder** filter action) is the last filter applied, because if the message is re-inserted into the mail queue, no further filtering is performed. For information on antivirus quarantine, see How Antivirus Quarantine Works on page 107.

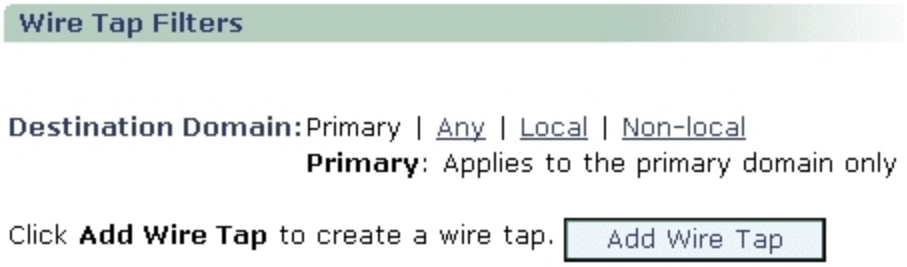
Managing Wire Taps

Use the **Wire Taps Filters** page (**Home > Content Filtering > Wire Taps**) to specify addresses for which all mail going through the content filtering enabled appliance will have a copy sent to the specified forwarding address. Use this feature to monitor all mail incoming to or outgoing from a certain address.

To create a wire tap filter:

1. Go to **Home Content Filtering > Wire Taps**.

   The **Wire Taps Filters** page appears.



2. In the **Destination Domain** area specify the scope for the filter you are creating.

   If you selected a domain before going to this page or if you log in as a Domain Administrator, these options do not display.

   Select one of the following options:

   - **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
   - **Any** - Filter any messages routed to or through the appliance on which the filter is created.
   - **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
   - **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

   The filter looks only at the mail addressed to the selected domain. For more information, see About the Destination Domain on page 174.

3. Click **Add Wire Tap**.

The **Add/Edit Wire Tap Filter** page appears.

4. In the **Address to Wire Tap** text field, type an email address. An empty **Address to Wire Tap** text field causes all mail for that **Destination Domain** to get wire tapped.
5. In the **Forward to** text field, type an email address. Mail sent to or coming from the specified **Address to Wire Tap** address, has a copy sent also to the specified **Forward to** address.
6. Click **OK**.

   The **Wire Tap Filters** page reloads and the wire tap filter table displays the wire tapped address and the forward to address. You can delete the wire tap filter by clicking the **Delete** icon (✕) in the filter table.

Using the CLI you can create a more specific wire tap filter to wire tap mail based on advanced filter criteria. For more information, type `Help About Filter` in the CLI.

To edit a wire tap filter:

1. Go to the **Home > Content Filtering > Wire Taps**.

   The **Wire Tap Filters** page appears.

2. To change the filter action, click the **Edit** icon (✎) in the filter table.

   The **Add/Edit Wire Tap Filter** page appears.

3. Make the necessary changes and click **OK**.

Example Wire Tap Address Entries

You can use the **Add/Edit Wire Tap Filter** page to create your own list. For example:

`allan@example.com` - Specifically adds the user `allan` from `example.com` to your wire tap list. Any incoming mail from `allan@example.com` is forwarded as specified.

`@spamcity.com` - Adds any address at `spamcity.com` to your wire tap list. Any incoming mail from any user in the `spamcity.com` domain is forwarded as specified.

You cannot 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. Also, wildcards are not accepted. For more information, see Using Patterns and Wildcard Characters on page 191.

Managing Blocked Addresses Filters

Use the **Blocked Addresses Filter** page (**Home > Content Filtering > Blocked Addresses**) to specify certain addresses or domains from which incoming mail should trigger the selected blocked addresses filter action. You can create your blocked addresses list before or after adding your filter. For more information, see Using the Filter List on page 188.

To create a blocked addresses filter:

1. Go to the **Home > Content Filtering > Blocked Addresses**.

   The **Block Addresses Filter** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are creating.

If you selected a domain before going to this page or if you log in as a Domain Administrator, these options do not display.

   Select one of the following options:

   - **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
   - **Any** - Filter any messages routed to or through the appliance on which the filter is created.
   - **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
   - **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

   The filter looks only at the mail addressed to the selected domain. For more information, see About the Destination Domain on page 174.

3. Click **Add Filter**.

   The **Add/Edit Blocked Addresses Filter** page displays.

4. In the **Filter Actions** area specify a response by selecting one of the following options:

- **Forward to** - Type in any valid email address or mailhost. The format for a mailhost is `@hostname`, where *hostname* is the mailhost prefaced by an ampersand (e.g., `@mycompany.com`). Matching messages are forwarded as specified. For more information, see Forward to vs. Send to Quarantine Folder on page 183.

The **Forward to** action sends the message directly to the specified email address or hostname but does not save a copy on the appliance.

- **Send to Quarantine folder** - Type in the fully-qualified folder name for any user that has the **Quarantine Administrator** role; for example, `user.UserName.FolderName` (folder names are optional. If not specified, the Inbox is used). If nothing is specified in the text field, `user.QuarantineAdmin` is used by default. Mail meeting the filter conditions is sent to this folder. A Quarantine Administrator can then decide to restore the message to the mail queue, or reject it. For more information, see Forward to vs. Send to Quarantine Folder on page 183 and How Content Filtering Quarantine Works on page 192.

For domain specific filters, this folder name (whether fully-qualified or `user.QuarantineAdmin`) must match a user in that delegated domain that has the **Quarantine Administrator** role.

- **Reject (refuse message and return it to the sender)** - Matching messages are bounced back to the sender. The recipient receives a message that the action was taken. This option is selected by default.
- **Discard (message is irrevocably lost)** - Matching messages are deleted. The recipient does not receive a message that the action was taken.

5. (Optional) Select the **Send the recipient(s) the following notification message** checkbox. The message recipient will receive the default message or you can change the To, From, Subject, Message text, and/or encoding. Variables that you can use are given below the encoding drop-down menu. By default, the character set used in the notification message is specific to your login's locale (e.g., **Unicode (UTF-8)** for English, **ISO-2022-JP** for Japanese, etc.).
6. Click **OK**.

   The **Blocked Addresses Filter** page reloads and the blocked addresses filter table displays the selected filter action that will act on your filter list. You can delete the blocked addresses filter by clicking the **Delete** icon (✕) in the filter table.

7. To complete your blocked addresses filter, you must create a blocked addresses list. For more information, see Using the Filter List on page 188 and Example Blocked Address List Entries on next page.

To edit a blocked addresses filter:

1. Go to the **Home > Content Filtering > Blocked Addresses**.

   The **Block Addresses Filter** page appears.

2. To change the filter action, click the **Edit** icon (✎) in the filter table.

   The **Add/Edit Blocked Addresses Filter** page appears.

3. Make the necessary changes and click **OK**.

Example Blocked Address List Entries

You can use the **Add/Edit List** area of the **Blocked Addresses Filter** page to create your own list. For example:

`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; any incoming mail from any user at the `spamcity.com` domain (e.g., `allan@spamcity.com`, `john@spamcity.com`, etc.) is acted on as specified by the blocked address filter action.

Managing Blocked Messages Filters

Use the **Blocked Messages Filter** page (**Home > Content Filtering > Blocked Messages**) to specify certain words or phrases that should trigger the selected blocked messages filter action. You can create your blocked messages list before or after adding your filter. For more information, see Using the Filter List on page 188.

To create a blocked messages filter:

1. Go to the **Home > Content Filtering > Blocked Messages**.

   The **Block Messages Filter** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are creating.

If you selected a domain before going to this page or if you log in as a Domain Administrator, these options do not display.

Select one of the following options:

- **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
- **Any** - Filter any messages routed to or through the appliance on which the filter is created.
- **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
- **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

The filter looks only at the mail addressed to the selected user group. For more information, see About the Destination Domain on page 174.

3. Click **Add Filter**.

   The **Add/Edit Blocked Messages Filter** page displays.

4. In the **Filter Actions** area specify a response by selecting one of the following options:

   - **Forward to** - Type in any valid email address or mailhost. The format for a mailhost is `@hostname`, where `hostname` is the mailhost prefaced by an ampersand (e.g., `@mycompany.com`). Matching messages are forwarded as specified. For more information, see Forward to vs. Send to Quarantine Folder on page 183.

> The **Forward to** action sends the message directly to the specified email address or hostname but does not save a copy on the appliance.

   - **Send to Quarantine folder** - Type in the fully-qualified folder name for any user that has the **Quarantine Administrator** role; for example, `user.UserName.FolderName` (folder names are optional. If not specified, the Inbox is used). If nothing is specified in the text field, `user.QuarantineAdmin` is used by default. Mail meeting the filter conditions is sent to this folder. A Quarantine Administrator can then decide to restore the message to the mail queue, or reject it. For more information, see Forward to vs. Send to Quarantine Folder on page 183 and How Content Filtering Quarantine Works on page 192.

> For domain specific filters, this folder name (whether fully-qualified or `user.QuarantineAdmin`) must match a user in that delegated domain that has the **Quarantine Administrator** role.

   - **Reject (refuse message and return it to the sender)** - Matching messages are bounced back to the sender. The recipient receives a message that the action was taken. This option is selected by default.
   - **Discard (message is irrevocably lost)** - Matching messages are deleted. The recipient does not receive a message that the action was taken.

5. (Optional) Select the **Send the recipient(s) the following notification message** checkbox. The message recipient will receive the default message or you can change the To, From, Subject, Message text, and/or encoding. Variables that you can use are given below the encoding drop-down menu. By default, the character set used in the notification message is specific to your login's locale (e.g., **Unicode (UTF-8)** for English, **ISO-2022-JP** for Japanese, etc.).
6. Click **OK**.

   The **Blocked Messages Filter** page reloads and the blocked messages filter table displays the selected filter action that will act on your filter list. You can delete the blocked messages filter by clicking the **Delete** icon (✕) in the filter table.

7. To complete your blocked messages filter, you must create a blocked messages list. For more information, see Using the Filter List on page 188 and Example Blocked Messages List Entry below.

To edit a blocked messages filter:

1. Go to the **Home > Content Filtering > Blocked Messages**.

   The **Block Messages Filter** page appears.

2. To change the filter action, click the **Edit** icon (✎) in the filter table.

   The **Add/Edit Blocked Messages Filter** page appears.

3. Make the necessary changes and click **OK**.

Example Blocked Messages List Entry

You can use the **Add/Edit List** area of the **Blocked Messages Filter** page to create your own list. For example:

`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. Also, wildcards are not accepted. For more information, see Using Patterns and Wildcard Characters on page 191.

Managing Blocked Attachments Filters

Use the **Blocked Attachments Filter** page (**Home > Content Filtering > Blocked Attachments**) to specify that mail containing certain attachment names or types should trigger the selected blocked attachments filter action. You can create your blocked attachments list before or after adding your filter. For more information, see Using the Filter List on page 188 and About MIME and Filtering Attachments on page 175.

To create a blocked attachments filter:

1. Go to the **Home > Content Filtering > Blocked Attachments**.

   The **Block Attachments Filter** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are creating.

If you selected a domain before going to this page or if you log in as a Domain Administrator, these options do not display.

Select one of the following options:

- **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
- **Any** - Filter any messages routed to or through the appliance on which the filter is created.
- **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
- **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

The filter looks only at the mail addressed to the selected user group. For more information, see About the Destination Domain on page 174.

3. Click **Add Filter**.

   The **Add/Edit Blocked Attachments Filter** page displays.

4. In the **Filter Actions** area specify a response by selecting one of the following options:

   - **Forward to** - Type in any valid email address or mailhost. The format for a mailhost is `@hostname`, where `hostname` is the mailhost prefaced by an ampersand (e.g., `@mycompany.com`). Matching messages are forwarded as specified. For more information, see Forward to vs. Send to Quarantine Folder on page 183.

The **Forward to** action sends the message directly to the specified email address or hostname but does not save a copy on the appliance.

   - **Send to Quarantine folder** - Type in the fully-qualified folder name for any user that has the **Quarantine Administrator** role; for example, `user.UserName.FolderName` (folder names are optional. If not specified, the Inbox is used). If nothing is specified in the text field, `user.QuarantineAdmin` is used by default. Mail meeting the filter conditions is sent to this folder. A Quarantine Administrator can then decide to restore the message to the mail queue, or reject it. For more information, see Forward to vs. Send to Quarantine Folder on page 183 and How Content Filtering Quarantine Works on page 192.

For domain specific filters, this folder name (whether fully-qualified or `user.QuarantineAdmin`) must match a user in that delegated domain that has the **Quarantine Administrator** role.

   - **Reject (refuse message and return it to the sender)** - Matching messages are bounced back to the sender. The recipient receives a message that the action was taken. This option is selected by default.
   - **Discard (message is irrevocably lost)** - Matching messages are deleted. The recipient does not receive a message that the action was taken.

5. (Optional) Select the **Send the recipient(s) the following notification message** checkbox. The message recipient will receive the default message or you can change the To, From, Subject, Message text, and/or encoding. Variables that you can use are given below the encoding drop-down menu. By default, the character set used in the notification message is specific to your login's locale (e.g., **Unicode (UTF-8)** for English, **ISO-2022-JP** for Japanese, etc.).
6. Click **OK**.

   The **Blocked Attachments Filter** page reloads and the blocked attachments filter table displays the selected filter action that will act on your filter list. You can delete the blocked attachments filter by clicking the **Delete** icon (✕) in the filter table.

7. To complete your blocked attachments filter, you must create a blocked attachments list. For more information, see Using the Filter List on page 188, Example Blocked Attachments List Entries below, and About MIME and Filtering Attachments on page 175.

To edit a blocked attachments filter:

1. Go to the **Home > Content Filtering > Blocked Attachments**.

   The **Block Attachments Filter** page appears.

2. To change the filter action, click the **Edit** icon (✎) in the filter table.

   The **Add/Edit Blocked Attachments Filter** page appears.

3. Make the necessary changes and click **OK**.

Example Blocked Attachments List Entries

You can use the **Add/Edit List** area of the **Blocked Attachments Filter** page to create your own list. For example:

`iloveyou.vbs` - Specifically adds the attachment filename `iloveyou.vbs` to your blocked attachments filter list. Any incoming mail attachment with the name `iloveyou.vbs` is acted on as specified by the blocked attachments filter action.

`.vbs` - Specifically adds the file extension `.vbs` to your blocked attachments filter list. Any incoming mail attachment with the extension `.vbs` is acted on as specified by the blocked attachments filter action.

If you enter `vbs` without the dot (.), the filter scans the entire attachment name for the letters v, b, and s, not just the extension.

`application/x-msdos-program` - Specifically adds the executable MS DOS MIME type to your blocked attachments filter list. Any incoming mail attachment with the file extension `.com`, `.exe`, or `.bat`, is acted on as specified by the blocked attachments filter action.

`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. Therefore, you must make your entries one at a time. Also, wildcards are not accepted. For more information, see Using Patterns and Wildcard Characters on page 191.

Managing Redirected Attachments Filters

Use the **Redirected Attachments Filter** page (**Home > Content Filtering > Redirected Attachments**) to specify that mail containing certain attachment names or types should trigger the selected redirected attachments filter action. You can create your redirected attachments list before or after adding your filter. For more information, see Using the Filter List on page 188 and About MIME and Filtering Attachments on page 175.

To create a redirected attachments filter:

1. Go to **Home > Content Filtering > Redirected Attachments**.

   The **Redirected Attachments Filter** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are creating.

   If you selected a domain before going to this page or if you log in as a Domain Administrator, these options do not display.

   Select one of the following options:

   - **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
   - **Any** - Filter any messages routed to or through the appliance on which the filter is created.
   - **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
   - **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

   The filter looks only at the mail addressed to the selected user group. For more information, see About the Destination Domain on page 174.

3. Click **Add Filter**.

   The **Add/Edit Redirected Attachments Filter** page displays.

4. In the **Filter Actions** area specify a response by selecting one of the following options:

   - **Forward to** - Type in any valid email address or mailhost. The format for a mailhost is `@hostname`, where `hostname` is the mailhost prefaced by an ampersand (e.g., `@mycompany.com`). Matching messages are forwarded as specified. For more information, see Forward to vs. Send to Quarantine Folder on page 183.

The **Forward to** action sends the message directly to the specified email address or hostname but does not save a copy on the appliance.

- **Send to Quarantine folder** - Type in the fully-qualified folder name for any user that has the **Quarantine Administrator** role; for example, `user.UserName.FolderName` (folder names are optional. If not specified, the Inbox is used). If nothing is specified in the text field, `user.QuarantineAdmin` is used by default. Mail meeting the filter conditions is sent to this folder. A Quarantine Administrator can then decide to restore the message to the mail queue, or reject it. For more information, see Forward to vs. Send to Quarantine Folder on page 183 and How Content Filtering Quarantine Works on page 192.

For domain specific filters, this folder name (whether fully-qualified or `user.QuarantineAdmin`) must match a user in that delegated domain that has the **Quarantine Administrator** role.

- **Reject (refuse message and return it to the sender)** - Matching messages are bounced back to the sender. The recipient receives a message that the action was taken. This option is selected by default.
- **Discard (message is irrevocably lost)** - Matching messages are deleted. The recipient does not receive a message that the action was taken.

5. (Optional) Select the **Send the recipient(s) the following notification message** checkbox. The message recipient will receive the default message or you can change the To, From, Subject, Message text, and/or encoding. Variables that you can use are given below the encoding drop-down menu. By default, the character set used in the notification message is specific to your login's locale (e.g., **Unicode (UTF-8)** for English, **ISO-2022-JP** for Japanese, etc.).
6. Click **OK**.

   The **Redirected Attachments Filter** page reloads and the redirected attachments filter table displays the selected filter action that will act on your filter list. You can delete the redirected attachments filter by clicking the **Delete** icon (✕) in the filter table.

7. To complete your redirected attachments filter, you must create a redirected attachments list. For more information, see Using the Filter List on page 188, Example Redirected Attachments List Entries on the facing page, and About MIME and Filtering Attachments on page 175.

To edit a redirected attachments filter:

1. Go to the **Home > Content Filtering > Redirected Attachments**.

   The **Redirected Attachments Filter** page appears.

2. To change the filter action, click the **Edit** icon (✎) in the filter table.

   The **Add/Edit Redirected Attachments Filter** page appears.

3. Make the necessary changes and click **OK**.

Example Redirected Attachments List Entries

You can use the **Add/Edit List** area of the **Redirected Attachments Filter** page to create your own list. For example:

`application/x-msdos-program`: Specifically adds the executable MS DOS MIME type to your attachments filter list; any incoming mail attachment with the suffix com, exe, or bat, is acted on as specified by the attachments filter action.

`vbs`: Specifically adds the file extension `.vbs` to your attachments filter list; any incoming mail attachment with the suffix `.vbs` is acted on as specified by the attachments filter action.

You cannot separate entries with spaces or semi-colons (;), each entry must be on a separate line. Therefore, you must make your entries one at a time. Also, wildcards are not accepted. For more information, see Using Patterns and Wildcard Characters on page 191.

Managing Corporate Word List Filters

Use the **Corporate Word List Filter** page (**Home > Content Filtering > Corporate Word List**) to specify certain words or phrases that should trigger the selected corporate word list filter action. You can create your corporate word list before or after adding your filter. For more information, see Using the Filter List on page 188.

To create a corporate word list filter:

1. Go to the **Home > Content Filtering > Corporate Word List**.

   The **Corporate Word List Filter** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are creating.

If you selected a domain before going to this page or if you log in as a Domain Administrator, these options do not display.

Select one of the following options:

- **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
- **Any** - Filter any messages routed to or through the appliance on which the filter is created.
- **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
- **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

The filter looks only at the mail addressed to the selected user group. For more information, see About the Destination Domain on page 174.

3. Click **Add Filter**.

   The **Add/Edit Corporate Word List Filter** page displays.

4. In the **Filter Actions** area specify a response by selecting one of the following options:

   - **Forward to** - Type in any valid email address or mailhost. The format for a mailhost is `@hostname`, where `hostname` is the mailhost prefaced by an ampersand (e.g., `@mycompany.com`). Matching messages are forwarded as specified. For more information, see Forward to vs. Send to Quarantine Folder on page 183.

> The **Forward to** action sends the message directly to the specified email address or hostname but does not save a copy on the appliance.

   - **Send to Quarantine folder** - Type in the fully-qualified folder name for any user that has the **Quarantine Administrator** role; for example, `user.UserName.FolderName` (folder names are optional. If not specified, the Inbox is used). If nothing is specified in the text field, `user.QuarantineAdmin` is used by default. Mail meeting the filter conditions is sent to this folder. A Quarantine Administrator can then decide to restore the message to the mail queue, or reject it. For more information, see Forward to vs. Send to Quarantine Folder on page 183 and How Content Filtering Quarantine Works on page 192.

> For domain specific filters, this folder name (whether fully-qualified or `user.QuarantineAdmin`) must match a user in that delegated domain that has the **Quarantine Administrator** role.

   - **Reject (refuse message and return it to the sender)** - Matching messages are bounced back to the sender. The recipient receives a message that the action was taken. This option is selected by default.
   - **Discard (message is irrevocably lost)** - Matching messages are deleted. The recipient does not receive a message that the action was taken.

5. (Optional) Select the **Send the recipient(s) the following notification message** checkbox. The message recipient will receive the default message or you can change the To, From, Subject, Message text, and/or encoding. Variables that you can use are given below the encoding drop-down menu. By default, the character set used in the notification message is specific to your login's locale (e.g., **Unicode (UTF-8)** for English, **ISO-2022-JP** for Japanese, etc.).
6. Click **OK**.

   The **Corporate Word List Filter** page reloads and the corporate word list filter table displays the selected filter action that will act on your filter list. You can delete the corporate word list filter by clicking the **Delete** icon (✕) in the filter table.

7. To complete your corporate word list filter, you must create a corporate word list. For more information, see Using the Filter List on page 188 and Example Corporate Word List Entries below.

To edit a corporate word list filter:

1. Go to the **Home > Content Filtering > Corporate Word List**.

   The **Corporate Word List Filter** page appears.

2. To change the filter action, click the **Edit** icon (✎) in the filter table.

   The **Add/Edit Corporate Word List Filter** page appears.

3. Make the necessary changes and click **OK**.

Example Corporate Word List Entries

You can use the **Add/Edit List** area of the **Corporate Word List Filter** page to create your own list. For example:

`confidential`: Specifically adds the word `confidential` to your corporate word filter list; any incoming mail containing that word is acted on as specified by the list's filter action.

`phooey`: Specifically adds the word `phooey` to your corporate word filter list; any incoming mail containing that word is acted on as specified by the list's 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. Also, wildcards are not accepted. For more information, see Using Patterns and Wildcard Characters on page 191.

Managing Objectionable Word List Filters

Use the **Objectionable Word List Filter** page (**Home > Content Filtering > Objectionable Word List**) 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. You can create your Objectionable Word list before or after adding your filter. For more information, see Using the Filter List on page 188.

To create an objectionable word list filter:

1. Go to **Home > Content Filtering > Objectionable Word List**.

   The **Objectionable Word List Filter** page appears.

2. In the **Destination Domain** area specify the scope for the filter you are creating.

If you selected a domain before going to this page or if you log in as a Domain Administrator, these options do not display.

Select one of the following options:

- **Primary** - Only filter messages addressed to users on the primary domain of the appliance on which the filter is created.
- **Any** - Filter any messages routed to or through the appliance on which the filter is created.
- **Local** - Only filter messages addressed to users (all domains) on the appliance on which the filter is created.
- **Non-local** - Only filter messages addressed to users not on the appliance on which the filter is created.

The filter looks only at the mail addressed to the selected user group. For more information, see About the Destination Domain on page 174.

3. Click **Add Filter**.

   The **Add/Edit Objectionable Word List Filter** page displays.

4. In the **Filter Actions** area specify a response by selecting one of the following options:

   - **Forward to** - Type in any valid email address or mailhost. The format for a mailhost is `@hostname`, where *hostname* is the mailhost prefaced by an ampersand (e.g., `@mycompany.com`). Matching messages are forwarded as specified. For more information, see Forward to vs. Send to Quarantine Folder on page 183.

The **Forward to** action sends the message directly to the specified email address or hostname but does not save a copy on the appliance.

   - **Send to Quarantine folder** - Type in the fully-qualified folder name for any user that has the **Quarantine Administrator** role; for example, `user.UserName.FolderName` (folder names are optional. If not specified, the Inbox is used). If nothing is specified in the text field, `user.QuarantineAdmin` is used by default. Mail meeting the filter conditions is sent to this folder. A Quarantine Administrator can then decide to restore the message to the mail queue, or reject it. For more information, see Forward to vs. Send to Quarantine Folder on page 183 and How Content Filtering Quarantine Works on page 192.

For domain specific filters, this folder name (whether fully-qualified or `user.QuarantineAdmin`) must match a user in that delegated domain that has the **Quarantine Administrator** role.

- **Reject (refuse message and return it to the sender)** - Matching messages are bounced back to the sender. The recipient receives a message that the action was taken. This option is selected by default.
- **Discard (message is irrevocably lost)** - Matching messages are deleted. The recipient does not receive a message that the action was taken.

5. (Optional) Select the **Send the recipient(s) the following notification message** checkbox. The message recipient will receive the default message or you can change the To, From, Subject, Message text, and/or encoding. Variables that you can use are given below the encoding drop-down menu. By default, the character set used in the notification message is specific to your login's locale (e.g., **Unicode (UTF-8)** for English, **ISO-2022-JP** for Japanese, etc.).
6. Click **OK**.

   The **Objectionable Word List Filter** page reloads and the objectionable word list filter table displays the selected filter action that will act on your filter list. You can delete the objectionable word list filter by clicking the **Delete** icon (✕) in the filter table.

7. To complete your objectionable word list filter, you must create a objectionable word list. For more information, see Using the Filter List on page 188 and Example Objectionable Word List Entries below.

To edit a objectionable word list filter:

1. Go to the **Home > Content Filtering > Objectionable Word List**.

   The **Objectionable Word List Filter** page appears.

2. To change the filter action, click the **Edit** icon (✎) in the filter table.

   The **Add/Edit Objectionable Word List Filter** page appears.

3. Make the necessary changes and click **OK**.

Example Objectionable Word List Entries

You can use the **Add/Edit List** area of the **Objectionable Word List Filter** page to create your own list. For example:

`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. Also, wildcards are not accepted. For more information, see Using Patterns and Wildcard Characters on page 191.

Chapter 5: Monitoring the Appliance

This chapter describes how to monitor system performance, check hardware status, and track down problems. Mirapoint appliances provide several monitoring options, including internal distribution lists where logs and reports are sent, sorting and searching the message queue, and sending alerts. The appliance also allows you to use external systems to perform monitoring functions.

The following topics are included:

- Internal Distribution Lists for Monitoring below
- Monitoring System and Data Storage Status on page 211
- Monitoring External Systems via SNMP on page 233
- Viewing the Message Queue on page 234
- Using Appliance Logs, Reports, and Graphs on page 246

Internal Distribution Lists for Monitoring

Default distribution lists (DLs) (shown in Table 16 on page 210) 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 are not used by the appliance (i.e., 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 appliance. 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. For more information on reserved DL names, see Reserved Distribution List Names on page 64.

Table 16 Default Mirapoint Distribution Lists

DL Name	Description
system-alerts	Used to notify recipients about conditions that might require human intervention. For more information, see Managing Alerts on page 219. 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 247. This list includes the Administrator user 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 247. This list includes the Administrator user by default and is reserved for Mirapoint use.
postmaster	Required reserved postmaster address (see RFC 2821 and RFC 2822). This list includes Administrator by default. Delegated domain default DL.
abuse	Standard abuse alias. Used to receive information about abuse issues. This list includes the Administrator user by default and can be deleted.
mailer-daemon	Standard mailer-daemon alias. This list includes postmaster by default and can be deleted. (Even if deleted, the mailer-daemon is used as the From address for bounced mail.) Delegated domain default DL.
operator	Standard operator alias. This list includes the Administrator user by default and can be deleted.
schedule-output	This list includes the Administrator user by default.
virus-alerts	This list includes the Administrator user by default.
nobody	Standard nobody alias. This list is empty by default and can be deleted.

Monitoring System and Data Storage Status

The monitoring-related Administration Suite pages (**Home > Monitoring**) allow you to check system status and data storage, as well as view alerts. It is advisable to monitor the health of appliance hardware, especially if you receive email notifications or anecdotal reports of problems. You can separately check the hardware status of the main chassis, RAID controller, and separate disk enclosures.

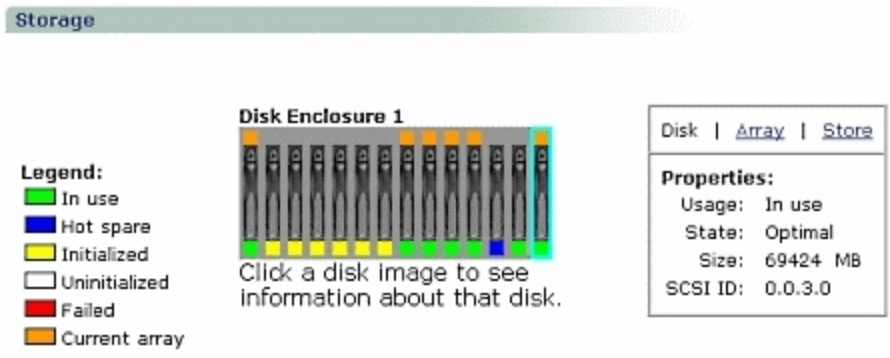
The contents of the **Monitoring** pages differ depending on your hardware and licensing.

Viewing Storage Information and Managing Arrays

Use the **Storage** page (**Home > Monitoring > Storage**) to view the current status of, and manage, your RAID (redundant array of independent disks) system or view the properties of your IDE storage and manage the disk cache. The display changes per your appliance configuration. Additionally, you can 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; add or delete spares and arrays, and configure arrays. The **Storage** page provides different options depending on your hardware and licensing.

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

Figure 17 Storage Page



- The **Legend** provides an explanation for the colors used in the **Disk Enclosure** graphics.
- The **Disk Enclosure** graphic displays individual hard drive identification when you put your cursor over an individual drive's image, and information on the selected drive in the **Properties** data box when you click on a drive's image. When you click on a drive, it becomes outlined in outlined in aqua.
- The **Properties** data box shows storage information. You can choose between the following views:

- **Disk** - View data on installed RAID disks. Add a spare, if available. For more information, see Viewing Disk Data below.
- **Array** - View data on system storage arrays. Add an array, if available. Delete an array or spare. For more information, see Viewing Array Data on the facing page.
- **Store** - View data on system storage space. For RazorGate (RG) 100s, the **Properties** data box only displays the **Store** view. For more information, see Viewing Storage Space Data on page 215.

Additional information about storage information and arrays is provided in the following sections:

- Setting the Disk Write Cache below
- Viewing Disk Data below
- Adding and Deleting a Spare on the facing page
- Viewing Array Data on the facing page
- Adding and Deleting an Array on page 214
- Viewing Storage Space Data on page 215
- Silencing the Alarm and Scanning on page 216
- Storage Page Colors on page 216

Setting the Disk Write Cache

The **Set Disk Write Cache** setting allows you to turn off the IDE disk write cache. By default, the disk write cache is set to **Cache On**, providing the fastest performance and is industry-standard. If you change the disk write cache setting, you must reboot your appliance.

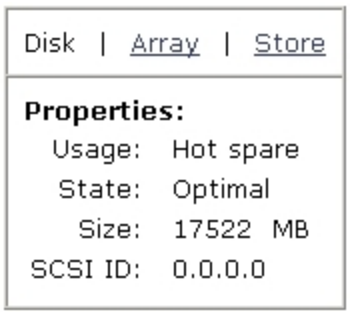
This option does not display for RG300s unless you have an IDE disk instead of the more typical RAID.

Viewing Disk Data

Each **Disk Enclosure** graphic shows the general status of each disk the enclosure contains. A **Properties** data box provides information on the disks shown. By default, the properties of the last initialized disk is displayed. Click on any displayed disk to see its properties.

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

Figure 18 Storage Page > Disk - Properties



The terms used in the **Properties** data box for **Disk** are as follows:

- **Usage** - In use, Hot spare, Not in use, or No disk
- **State** - Optimal, Initializing, Rebuilding, or Failed
- **Size** - Size in megabytes (MB)
- **SCSI ID** - Information on the location of the disk (in relation to the other disks in the enclosure)

Adding and Deleting a Spare

You should 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. To find the location of the hot-spare disk bay or bays on your appliance, see the hardware manual for your model. If there is no unused disk in any hot-spare disk bay, the **Add Spare** option does not appear.

To add a spare:

1. Install your new hot spare disk as described in the hardware manual for your appliance model.

   The new disk is available or an error message displays.

2. Go to **Home > Monitoring > Storage**.

   The **Storage** page appears.

3. Make sure you are in the **Disk** view, click **Add Spare**.

A message displays indicating success or failure at adding the spare.

Delete a spare only when you want to replace it with a higher-capacity disk.

To remove a spare:

1. Go to **Home > Monitoring > Storage**.

   The **Storage** page appears.

2. Make sure you are in the **Array** view and select the spare you want to remove.
3. Click **Delete**.

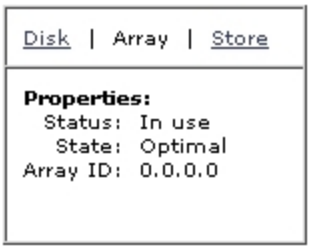
   A confirmation message appears.

4. Click **Delete**.

Viewing Array Data

To view the disk array status, on the **Storage** page in **Array** view, click on a disk. The disk becomes outlined in aqua. The **Properties** data box changes to display array properties.

Table 19 Storage Page > Array - Properties



The terms used in the **Properties** data box for **Array** are as follows:

- **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 Deleting an Array

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 model. If the disks are installed incorrectly the Add Array option does not appear. You can add an array to your appliance only if a sufficient number of unused disks are available (independent of configuration), otherwise, the Add Array option 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:

1. Install your new unused disks as described in the hardware manual for your model.

You might need to click the **Scan** in the **Store** view in order for the appliance to recognize the new disk(s).

2. Go to **Home > Monitoring > Storage**.

   The **Storage** page appears.

3. Make sure you are in the **Disk** view and click **Add Array**.

   A progress bar displays and a message indicating success or failure at adding the array although the add process continues and will typically last several hours. You can do other administration tasks or close the browser while the initialization process progresses.

4. On the **Storage** page, in the **Array** view, select the new array.
5. Click **Configure**.

A progress bar and confirmation message appear. Configuring the array will cause the appliance to stop all email services for five to fifteen minutes or more.

6. To proceed, click **Configure**.

The page re-displays with the **Properties** data box showing the status of the configuration and the appliance adds the array to the mail store. Adding the appliance 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**.

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 configured into the mail store) can be deleted.

To delete an array:

1. Go to **Home > Monitoring > Storage**.

   The **Storage** page appears.

2. Make sure you are in the **Array** view and select the array you want to delete.
3. Click **Delete**.

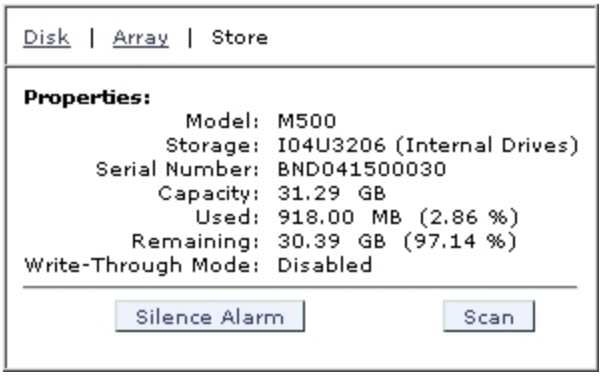
   A confirmation message appears.

4. Click **Delete**.

Viewing Storage Space Data

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 and click **Store**.

Figure 20 Storage Page > Store - Properties



The terms used in the **Properties** data box for **Store** are as follows:

- **Model** - The hardware model type.
- **Storage** - The identification number for the internal disks.
- **Serial Number** - The identification number for the array.
- **Capacity** - How many GBs (gigabytes) of space the disk enclosure supplies.
- **Used** - How many GBs/MBs (megabytes) of space the disk enclosure is currently using.
- **Remaining** - How many GBs/MBs of space the disk enclosure has available.
- **Write-Through Mode** - Displays the status of the disk write cache setting (i.e., enabled or disabled). For more information, see Setting the Disk Write Cache on page 212.

Silencing the Alarm and Scanning

Use the **Silence Alarm** option to turn off the audible alarm triggered by a failure in the RAID system (such as a disk failure).

Use the **Scan** option to scan the RAID system for changes in the hardware configuration, such as the insertion of new disks. It is best to use the **Scan** option only after installing new disks. Using this option frequently can degrade performance.

Storage Page Colors

Table 21 Store Page Colors Legend

Color	Description
	In Use
	Host Spare
	Initialized
	Uninitialized
	Failed
	Current array. On the **Disk** or **Array** views, the **Properties** data box changes to reflect the current selection.

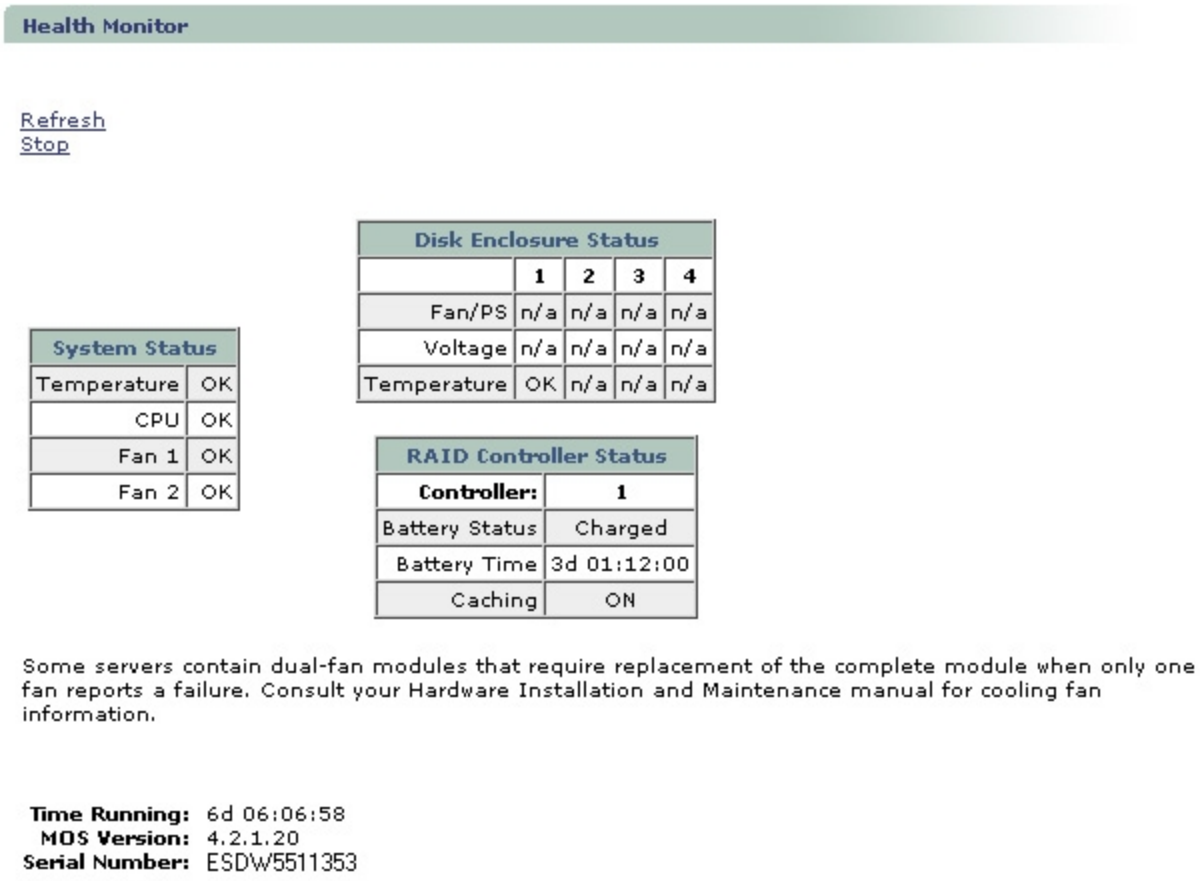
Using Health Monitoring

The information shown on the **Health Monitor** page (**Home > Monitoring > Health Monitor**) depends on the configuration of your hardware platform. If no information is given for an item, it means the monitoring system is unable to determine the item's status. For RG100 hardware models, typically, this page provides no useful information except for Viewing Time Running Status on page 219.

The **System Status** table represents the computer chassis, while the **Disk Enclosure Status** table on the right represents the disk enclosure. Reported statistics vary per appliance. The **RAID Controller Status** table shows battery status and cache status for the RAID controller. The MOS release number and time since the appliance was last restarted appear in the lower left. Problem conditions appear in red.

Additional information is available on more system statistics than those shown above. To see all available values, use the `Stat Get *` command from the command-line interface (CLI).

Figure 22 Health Monitor Page



Additional information about health monitoring is provided in the following sections

- Starting and Stopping Health Monitoring below
- Viewing System Status on next page
- Viewing Disk Enclosure Status on next page
- Viewing RAID Controller Status on next page
- Viewing Time Running Status on page 219
- Viewing the MOS Version and Serial Number on page 219

Starting and Stopping Health Monitoring

If you want to stop health monitoring, click **Stop**. The link changes to **Start** so you can restart the monitor. The **Health Monitor** page refreshes itself every thirty seconds, so stopping it is generally not necessary. If you have currently active alerts, a message displays indicating so and a link displays that opens the **Alerts** page. For more information, see Managing Alerts on page 219.

Viewing System Status

Only applicable statistics for your appliance is displayed. For appliances with a valid failover license, statistics are shown for both the primary system's active hardware and the standby system.

Table 23 System Status Items

Item	Description
Temperature	System chassis temperature is nominal (OK) or outside the acceptable range (Bad).
CPU n	Indicates that the n-th CPU is operating correctly (OK) or has failed (Bad). Only physical CPUs are displayed, not logical CPUs.
CPU n Temperature	Indicates that the CPU temperature is nominal (OK) or outside the acceptable range (Bad). Which CPU is indicated by the n notation, if there is only one CPU, there is no notation.
CPU Fan	Indicates that the CPU fan is operating correctly (OK) or has failed (Bad).
Fan n	Indicates that the n-th cooling fan is operating correctly (OK) or has failed (Bad).
Voltage	Indicates that the power supply voltage is nominal (OK). Bad is an indication of several potential problems; for example, loss of AC power, failed or missing power supply modules, fan failure in a power supply module, or an out-of-tolerance DC voltage on the motherboard.

Viewing Disk Enclosure Status

Each numbered column indicates a separate disk enclosure (also called a *shelf*). Newer systems have only one shelf, but much higher density.

Table 24 Disk Enclosure Status Items

Item	Description (for each fan)
Fan/PS	Indicates that the Fan/Power Supply is operating correctly (OK) or has failed (Bad). You must determine whether the Fan or the Power supply has the problem.
Voltage	Indicates that the power supply voltage is nominal (OK) or outside the acceptable range (Bad).
Temperature	Indicates that the disk shelf internal temperature is nominal (OK) or outside the acceptable range (Bad).

Viewing RAID Controller Status

This status does not display on some older hardware. Only an external disk shelf equipped system can have a failover, and that appliance will have two battery statuses.

Table 25 RAID Controller Status Items

Item	Description
Battery Status	The status of the battery. Possible values are:

Item	Description
	• Startup: The system just started and is determining its status. • Charged: The battery is fully charged. • Charging: The battery is charging because it became discharged while the system was off, or during a battery initialization cycle. • Bad: The battery is bad and should be replaced; generates system alert. • None: Battery is missing or the cable connecting it to the system is loose; generates system alert. • Unknown: The battery is in an unknown state; generates system alert. Contact Customer Service, this state is not normal. • Discharging: The battery is discharging; this can be caused by a battery initialization cycle. • Initialize Charging: The initial charging in an initialization cycle. • Initialize Discharging: The initial discharging in an initialization cycle. • Initialize Recharging: A recharge during an initialization cycle; rare. • n/a: Your box should have 2 RAID controllers and the 2nd controller is missing.
Battery Time	A time displayed exactly like the Viewing Time Running Status below.
Cache	ON or OFF

Viewing Time Running Status

- # days - Indicates the number of days the system has been running since the last reboot.
- Hours, minutes, seconds - Indicates the number of hours, minutes, and seconds (`hh:mm:ss`) the system has been running since the last reboot.

Viewing the MOS Version and Serial Number

MOS Version - Indicates the version number of the Messaging Operating System (MOS) release on the appliance.

Serial Number - Indicates the serial number of the appliance.

Managing Alerts

Use the **Alerts** page (**Home > Monitoring > Alerts**) to view active alerts on the appliance. Clicking on a column header link sorts the table by that factor. The **Refresh** link manually updates the page, and the **Start** or **Stop** links to enable or disable the automatic update of the page.

The **System Information** report (**Home > Logs / Reports > System**) displays **System Alert** messages not related to the persistent conditions shown on this page. To get a more complete picture of appliance activity, view the **System Information** report in addition to this page. For more information, see Viewing the System Information Report on page 274.

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. The table also includes the following features:

- Click on a column header to sort the table by that factor.
- The **Time Outstanding** indicates how long the alert has been active.

Figure 26 Alerts Page

The following tables provide a listing of RAID, SYSTEM, and UPS-related alerts you might encounter as well as all of the official statistics from the `Stat Get *` command-line interface (CLI) command. For more information, see the *Mirapoint Administration Protocol Reference* which provides additional information on these alerts and the `Stat` command.

- Managing Alerts on previous page
- System Alerts/Statistics on page 224
- UPS Alerts/Statistics on page 232

In the following tables, *n* represents a number (i.e., 0,1, and so on). For example, RAID.CAB*n*FAN would display as RAID.CAB0FAN, RAID.CAB1FAN, and so on.

RAID Alerts/Statistics

RAID Alert/Statistic	Description/Probable Cause	Recommended Action
RAID.BATTERYSTATUS	RAID controller battery is bad, missing, or in an unknown state	If this alert appears, check battery connections and connector pins. Replace the battery if old. Contact Mirapoint Technical Support for replacement.
RAID.BATTERY1STATUS RAID.BATTERY2STATUS	On certain hardware models, this alert indicates the battery condition of the first (or second) RAID controller. For more information on the various battery statuses, see the *Mirapoint Administration Protocol Reference*.	If this alert appears, check battery connections and connector pins. Replace the battery if old. Contact Mirapoint Technical Support for replacement.
RAID.BATTERYTIME	Indicates charge time left in the designated RAID controller battery	If this alert appears and the time left is only 10 or 15 minutes, the batteries are reaching their end of life, so you should consider changing them.
RAID.CAB*n*FAN	A disk enclosure fan or power supply has failed	If this alert appears, replace the fan or power supply as described in the *Mirapoint Hardware Manual* for your appliance model.
RAID.CAB*n*MONFAIL	Health monitoring module has a communications problem	If this alert appears, physically inspect the disk shelf to determine which LSM has failed and replace it.
RAID.CAB*n*TEMP	The temperature in a disk enclosure is too high	If this alert appears, try reducing the ambient temperature.
RAID.CAB*n*VOLT	The voltage in a disk enclosure is outside the nominal range	If this alert appears, contact Mirapoint Technical Support immediately.
RAID.CACHEON	RAID controller battery is being initialized or needs to be replaced	If this alert appears, the RAID controller cache is in write-through mode and writing directly to disk, so I/O performance will be slow until battery is fully initialized or replaced.

RAID Alert/Statistic	Description/Probable Cause	Recommended Action
RAID.CACHE1-ON RAID.CACHE2-ON	State of the first (or second) battery-backed RAID controller cache	If this alert appears, the RAID controller cache is in write-through mode and writing directly to disk, so I/O performance will be slow until battery is fully initialized or replaced.
RAID.CMDREAD	Number of read commands issued to the RAID within the last second. A RAID read command failed.	If this alert appears, contact Mirapoint Technical Support.
RAID.CMDTOT	Number of commands of all types issued to the RAID within the last second	If this alert appears, contact Mirapoint Technical Support.
RAID.CMDWRITE	Number of write commands issued to the RAID within the last second. A RAID write command failed.	If this alert appears, contact Mirapoint Technical Support.
RAID.CONTROLLER	RAID controller experienced a timeout or interrupt failure	If this alert appears infrequently, then it can be safely ignored. If this happens 10-15 times a day, the RAID controller needs to be replaced.
RAID.FAILED	A RAID disk has failed	If this alert appears, replace the failed disk.
RAID.HBAnTEMP	The host bus adapter (HBA) card in the appliance chassis is too hot	If this alert appears, check chassis fans and try reducing the ambient temperature.
RAID.HBAnVOLT	Voltage to the host bus adapter (HBA) card in the appliance chassis is out of its nominal range	If this alert appears, contact Mirapoint Technical Support immediately.
RAID.KBREAD	Number of kilobytes read from RAID within the last second	If this alert appears, contact Mirapoint Technical Support.
RAID.KBWRITE	The number of kilobytes written to RAID within the last second	If this alert appears, contact Mirapoint Technical Support.
RAID.LATREAD	The average read latency in milliseconds	If this alert appears, contact Mirapoint Technical Support.
RAID.LATWRITE	The average write latency in milliseconds.	If this alert appears, contact Mirapoint Technical Support.
RAID.MAILSTORE	Mail store partition, the space used for storing	If this alert appears, delete unwanted messages and user accounts or add RAID disks if possible.

RAID Alert/Statistic	Description/Probable Cause	Recommended Action
	accounts and mailboxes, is nearly full	
RAID.MAILSTOREF	Mail store contains too many files	If this alert appears, delete unwanted messages and user accounts or add RAID disks if possible. Contact Mirapoint Technical Support immediately.
RAID.MAILSTOREFULL	Mail store space is full	If this alert appears, delete unwanted messages and user accounts, or add RAID disks if possible. Contact Mirapoint Technical Support immediately.
RAID.SYSSTORE	Percentage of total space currently being used in the system disk partition. The system disk partition (i.e., the space containing system files, temporary files, and MOS) is nearly full. During normal operation, this may go up and down.	If the result of the `Stat Get Raid.Sysstore` CLI command is more than 95% and stays there or continues to grow toward 100%, contact Mirapoint Technical Support.
RAID.SYSSTOREF	System storage contains too many files	If this alert appears, delete unwanted messages and user accounts or add RAID disks if possible. Contact Mirapoint Technical Support immediately.
RAID.SYSSTOREFULL	System storage partition is full	If this alert appears only at midnight and soon clears, the appliance is rolling the logs. Under any other circumstance, contact your Mirapoint Technical Support immediately.
RAID.WARNING	A disk drive is not certified or not recognized as certified	A disk drive uses a version of firmware that has not been qualified by Mirapoint. If the disk was supplied by Mirapoint, this alert can be ignored. There was a mismatch between the list of valid drives that were actually qualified by manufacturing. A `F3_CertifiedDisks` patch is available on the Mirapoint Support website to correct this problem.

System Alerts/Statistics

System Alert/Statistic	Description/Probable Cause	Recommended Action
SYSTEM.ADMINC	Too many administrator connections.	If this alert appears and you really want to allow this many administrator connections, the threshold for this alert can be adjusted using the `Mon Setthresh SYSTEM.ADMINC` command.
SYSTEM.AGREETCHATTER	Number of SMTP drops caused by `Bannerdelay` is too high	If this alert appears, check your `Bannerdelay`settings in the CLI using `Smtp Get Bannerdelay` and `Smtp Get BannerdelayTime`.
SYSTEM.AMKDELIVERED	Amount of email message data delivered to local mailboxes is too high	If this alert appears, check the mail logs to see which users are receiving a large volume of email. Devise filters or implement antispam scanning to reduce their email volume.
SYSTEM.AMKIN	Amount of email message data coming into the appliance is too high	If this alert appears, check the mail logs to see which sites are sending so much email. Possibly put them on the blocked address list using the `Uce Add` CLI command or the **Blocked Addresses Filter** page (**Home > Content Filtering > Blocked Addresses**).
SYSTEM.AMKOUT	Amount of email message data originating from the appliance is too high	If this alert appears, check the mail logs to see which users are sending so much email.
SYSTEM.AMMSGATTACH	Number of messages received with attachments since appliance inception or counter overflow. This presents a high-order view of mail attachments. Any MIME-style message part boundary counts	If this alert appears, check the mail logs to see which sites are sending so much email with attachments.
SYSTEM.AMMSGDELIVERED	Number of email messages delivered to local mailboxes is too high	If this alert appears, check the mail logs to see which users are receiving a large amount of email. Also, devise filters or implement antispam scanning to reduce their amount of email.
SYSTEM.AMMSGIN	Number of email messages coming into the appliance is too high	If this alert appears, check the mail logs to see which sites are sending so much email. Also, consider putting them on the blocked address list using the `Uce Add` CLI command or the **Blocked Addresses Filter** page (**Home > Content Filtering > Blocked Addresses**).

System Alert/Statistic	Description/Probable Cause	Recommended Action
SYSTEM.AMMSGOUT	Number of email messages originating from the appliance is too high	If this alert appears, check the mail logs to see which users are sending so much email.
SYSTEM.AMMSGRECP	Number of message recipients since appliance inception or counter overflow	Use the `Stat Get SYSTEM.AMMSGRECP` CLI command to monitor incoming mail usage. Also, check the mail logs.
SYSTEM.AMMSGSPAM	Count of messages that the antispam subsystem(s) have classified as junk mail. This count increments when a message is marked as spam, under any threshold, and the counter persists across reboot	Use the `Stat Get SYSTEM.AMMSGSPAM` CLI command to monitor antispam scanning. Also, check the mail logs.
SYSTEM.AMMSGVIRUS	Number of email viruses found since appliance inception or counter overflow	Use the `Stat Get SYSTEM.AMMSGVIRUS` CLI command to monitor antivirus scanning. Also, check the mail logs.
SYSTEM.APKTCOLL	Too many network packet collisions since the appliance was booted	If this alert appears, the network is saturated or is reaching the saturation point. Analyze traffic and possibly subnet or repartition the network.
SYSTEM.APKTIN	Too many ingoing network packets since the appliance was booted	If this alert appears, it might indicate a heavily loaded server.
SYSTEM.APKTINERR	Total number of inbound network errors since system inception or counter overflow	If this alert appears, check to make sure that the server is not heavily loaded.
SYSTEM.APKTOUT	Too many outgoing network packets since the appliance was booted	If this alert appears, it might indicate a heavily loaded server.
SYSTEM.APKTOUTERR	Total number of outbound network errors since system inception or counter overflow	If this alert appears, check to make sure that the server is not heavily loaded.

System Alert/Statistic	Description/Probable Cause	Recommended Action
SYSTEM.ASMTPCIN	Number of inbound SMTP connections	Use the `Stat Get SYSTEM.ASMTPCIN` CLI command to monitor SMTP connection usage.
SYSTEM.ASMTPCOUT	Number of outbound SMTP connections.	Use the `Stat Get SYSTEM.ASMTPCOUT` CLI command to monitor SMTP connection usage.
SYSTEM.AVENGINE	Antivirus engine's pattern files are out of date	If this alert appears, run the antivirus `Update` CLI command, or use the **Antivirus Updates** page (**Home > Antivirus >** ***Antivirus Engine (e.g., Sophos)*** **> Updates**), to update the pattern files. Ordinarily these pattern files are automatically updated every hour. Investigate why this did not occur.
SYSTEM.CHASTEMP	The appliance chassis is too hot or the appliance temperature is too cold	If this alert appears, check the fans and try reducing the ambient room temperature if the appliance is too hot. If the appliance temperature is too cold, increase the ambient room temperature. Also check the `Stat Get STANDBY.CHASTEMP` CLI command.
SYSTEM.CONTEXT	Too much context switching	If this alert appears, contact Mirapoint Technical Support.
SYSTEM.CPUSTATUS1 SYSTEM.CPUSTATUS2	CPU module 1 (or 2) is missing or failed	If this alert appears, check and possibly replace CPU module 1 (or 2) in multiprocessor units.
SYSTEM.CPUTEMP	The processor's temperature	If this alert appears, the processor might have exceeded the recommended maximum. Check and possibly replace the CPU.
SYSTEM.CP1UTEMP SYSTEM.CPU2TEMP	The temperature of multiple processor 1 (or 2)	If this alert appears, the processor might have exceeded the recommended maximum. Check and possibly replace the CPU.
SYSTEM.DISK*n*	A disk is missing or has failed	If this alert appears, check and possibly replace the disk. DISK0 represents the disk in slot 0, and so on.
SYSTEM.DNS*n*RESP	Domain Name System (DNS) response time is poor	If this alert appears, consider switching to a more responsive DNS server. Use the `Dns Add` CLI command, or the **Set Interface** page (**Home > System > Network > Interface**), to add a secondary or tertiary DNS server to the list. Check the server if it is down or not responding. Otherwise the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.
SYSTEM.FANC	The main or numbered CPU fan is not functioning properly	If this alert appears, replace the CPU fan or contact Mirapoint Technical Support immediately to have the fan replaced.
SYSTEM.FANMB*n*	A motherboard fan has	If this alert appears, inspect the fans and replace any that

System Alert/Statistic	Description/Probable Cause	Recommended Action
	failed	are not working. If the fans are all working fine, contact Mirapoint Technical Support. Similar alerts can be issued for the standby appliance.
SYSTEM.HWMONFAIL	The health monitoring subsystem has failed	If this alert appears, contact Mirapoint Technical Support to have the problem diagnosed and fixed.
SYSTEM.IDLECPU	The percentage of cycles that the processor is idle was exceeded, indicating that there is too little CPU capacity left	If this alert appears, consider upgrading to a newer or faster appliance.
SYSTEM.IMAPC	There are too many IMAP connections	This alert threshold can be configured with the `Mon Setthresh` CLI command. If this problem persists, consider purchasing another Mirapoint appliance to handle the increased load.
SYSTEM.IMAPL	The IMAP service is not running	If this alert appears, try to restart the service with the `Service Start Imap` CLI command, or the **IMAP** page (**Home > System > Services > IMAP**). If the IMAP service fails to start, contact Mirapoint Technical Support.
SYSTEM.IMAPLOGINS	The IMAP service has exceeded its user-limit license	If this alert appears, the number of unique IMAP logins per day has exceeded the license limit. Contact a Mirapoint Sales Representative to upgrade your IMAP user license to a higher allowed number.
SYSTEM.KERB5*n*RESP	Kerberos 5 server(s) response time is poor	If this alert appears, consider switching to a more responsive Kerberos server. Check the server if it is down or not responding. Otherwise the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.
SYSTEM.LDAP*n*RESP	LDAP server(s) response time is poor	If this alert appears, check the server if it is down or not responding. Consider switching to a more responsive LDAP server. Use the `LDAP Add` CLI command, or the **Choose Routing Method** page (**Home > System > Routing > Routing Method**), to add a secondary or tertiary LDAP server to the list. Otherwise the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.
SYSTEM.LMRRESP	Local Mail Router (LMR) response time is poor	If this alert appears, consider upgrading to a more responsive LMR server. Check the server if it is down or not responding. Otherwise the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.

System Alert/Statistic	Description/Probable Cause	Recommended Action
SYSTEM.LMRSTATUS	The Local Mail Router (LMR) is not accepting mail	If this alert appears, identify the LMR using the `Smtp Get Lmr` CLI command. Check the status and configuration of the appliance.
SYSTEM.LOAD	Work rate is too high, as measured by the average number of processes in the run queue over the last 60 seconds	This alert is sent if the appliance load is 50 or more. If this is unusual for your appliance and lasts longer than 30 minutes, contact Mirapoint Technical Support.
SYSTEM.MAILQUEUE	Mail queue is too big. Too many messages in the SMTP delivery queue	If this alert appears, examine the mail queue using the `Mailq List` CLI command, or the message queue-related administration pages (**Home > Queue**), using patterns to limit the listing. You might want to delete extraneous or user-missing messages using the `Mailq Reject` CLI command.
SYSTEM.MEMORY	The status of system main memory	If this alert appears and a memory error is indicated, check the memory. You might need to contact Mirapoint Technical Support.
SYSTEM.MKIN	Total volume of incoming messages per second is high	If this alert appears, check the incoming mail queue with the `Mailq List` CLI command, or the message queue-related administration pages (**Home > Queue**). It is possible that a spammer is sending many large messages to your site. If many large messages originate from a single site, you might want to block that address using the `Uce Add` CLI command, or the **Blocked Addresses Filter** page (**Home > Content Filtering > Blocked Addresses**).
SYSTEM.MKOUT	Total volume of outgoing messages per second is high	If this alert appears, check the outgoing mail queue with the `Mailq List` command, or the **Queue** page. If many large messages originate from one sender, that user might be sending too many large attachments. It is also possible that users are just busy sending big messages.
SYSTEM.MMSGIN	Number of incoming messages is high	If this alert appears, check the incoming mail queue with the `Mailq List` command, or the **Queue** page. It is possible that your appliance is experiencing a mail storm or denial-of-service (DoS) attack. If most messages originate from a single site, you might want to block that address using the `Uce Add` CLI command, or the **Blocked Addresses Filter** page (**Home > Content Filtering > Blocked Addresses**).
SYSTEM.MMSGOUT	Number of outgoing messages is high	If this alert appears, check the outgoing mail queue with the `Mailq List` CLI command, or the message queue-related administration pages (**Home > Queue**). If many messages originate from one sender, one of your

System Alert/Statistic	Description/Probable Cause	Recommended Action
		customers might be sending spam. It is also possible that users are just busy sending messages.
SYSTEM.NETMEDIA	Appliance has switched from 100-Base-TX to 10-Base-T networking	If the Mirapoint appliance was configured to do auto-negotiation with the network switch to allow the MAC hardware to automatically select its speed, an alert is issued when the negotiated speed changes from 100BaseT to 10BaseT or vice versa.
SYSTEM.NPROCS	Too many processes running on the appliance	If this alert appears, contact Mirapoint Technical Support.
SYSTEM.NTP*n*RESP	Network Time Protocol (NTP) server(s) response time poor	If this alert appears, check the server to see if it is down or not responding. Consider switching to a more responsive NTP server. Otherwise the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.
SYSTEM.OMRRESP	Outbound Message Router (OMR) appliance response time	If this alert appears, consider upgrading to a more responsive Mirapoint OMR appliance. Check the appliance if it is down or not responding. Otherwise the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.
SYSTEM.PGIN	System paging (back into memory) is too high	If this alert appears, contact Mirapoint Technical Support.
SYSTEM.PGOUT	System paging (out onto disk) is too high	If this alert appears, contact Mirapoint Technical Support.
SYSTEM.PKTCOLL	Too many network packet collisions per second. The network is saturated or is reaching the saturation point	Use the `Stat Get SYSTEM.PKTCOLL` CLI command to monitor network traffic to see if there is anything that can be done to reduce load.
SYSTEM.PKTIN	Too many incoming network packets per second. Incoming network traffic has saturated the network	Use the `Stat Get SYSTEM.PKTIN` CLI command to monitor network traffic to see if there is anything that can be done to reduce load.
SYSTEM.PKTINERR	Average number of inbound network errors per second during the last monitoring interval	Use the `Stat Get SYSTEM.PKTINERR` CLI command to monitor network traffic to see how you can balance the load.
SYSTEM.PKTOUT	Too many outgoing network packets per second	If this alert appears, outgoing network traffic has saturated the network. Monitor traffic to see if there is anything that can be done to reduce load.
SYSTEM.PKTOUTERR	Average number of outbound network errors	Using the `Stat Get SYSTEM.PKTOUTERR` CLI Command to monitor network traffic in order to determine how you can

System Alert/Statistic	Description/Probable Cause	Recommended Action
	per second during the last monitoring interval	balance the load.
SYSTEM.POPC	There are too many POP connections	The threshold for this alert can be configured using the `Mon` CLI command. If this problem persists, consider purchasing another Mirapoint appliance to handle the increased load.
SYSTEM.POPL	The POP service is not running	If this alert appears, try to restart the service with the `Service Start Pop` CLI command, or the **POP** page (**Home > System > Services > POP**). If the POP service fails to start, contact Mirapoint Technical Support.
SYSTEM.POPLOGINS	The POP service has exceeded its user-limit license	If this alert appears, the number of unique POP logins per day has exceeded the license limit. Contact a Mirapoint Sales Representative to upgrade your POP user license to a higher allowed number.
SYSTEM.POWER	A appliance power supply has failed, or the power supply sensor cable connecting the appliance's LCD panel is reversed	If this alert appears, physically inspect the power supplies on the appliance head unit and the connections. Replace the failed power supply if necessary. If the power supplies are working fine, but this alert continues, contact Mirapoint Technical Support.
SYSTEM.RADIUS*n*RESP	RADIUS authentication server(s) response time is poor	If this alert appears, check the RADIUS server to see if it is down or not responding. Consider switching to a more responsive RAIDUS server. Otherwise, the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.
SYSTEM.RBL*n*RESP	Realtime blackhole list (RBL) server(s) response time is poor	If this alert appears, you might want to temporarily suspend RBL services with the `Smtp Set Rbl Off` CLI command, or the **Set RBL Host List** page (**Home > Antispam > RBL Host List**), until response improves. Check the server if it is down or not responding. Otherwise the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.
SYSTEM.ROUTERRESP	Network gateway (IP router) response time is poor	If this alert appears, consider switching to a more responsive network gateway. Check the server if it is down or not responding. Otherwise the threshold for this alert can be adjusted with the `Mon Setthresh` CLI command.
SYSTEM.SMTPC	There are too many simultaneous inbound SMTP connections	If this alert appears, monitor incoming messages to see if anything can be done to reduce load. It is possible your appliance is undergoing a sudden mail storm. This alert threshold can be changed with the `Mon Setthresh` CLI command. If this problem persists, consider

System Alert/Statistic	Description/Probable Cause	Recommended Action
		purchasing another Mirapoint appliance to handle the increased load.
SYSTEM.SMTPL	The SMTP service is not running (i.e., listening)	If this alert appears, the SMTP service (listener) on the Mirapoint appliance could be intentionally stopped for various reasons, and if so, SMTP listener service will be resumed automatically once a condition clears. If this alert does not clear itself, restart SMTP service using the `Service Start Smtp` CLI command, or the SMTP page (**Home > System > Services > SMTP**). This alert also indicates the condition or reason why the alert message appeared.
SYSTEM.SSLC	Current number of SSL connections	Using the `Stat Get SYSTEM.SSLC` CLI Command is useful for monitoring network traffic.
SYSTEM.SWAPIN	Appliance swapping from disk into memory is too great	If this alert appears, contact Mirapoint Technical Support.
SYSTEM.SWAPOUT	Appliance swapping from memory onto disk is too great	If this alert appears, contact Mirapoint Technical Support.
SYSTEM.SYSCPU	Appliance CPU usage is too high	If this alert appears, contact Mirapoint Technical Support.
SYSTEM.TOUCH	The front-panel keypad (touchpad) and/or LCD panel have failed	If this alert appears, contact Mirapoint Technical Support for help and possibly a component replacement.
SYSTEM.USERCPU	User mode CPU usage is too high	If this alert appears, contact Mirapoint Technical Support.
SYSTEM.VOLTAGE	The appliance chassis voltage is out of the nominal range	If this alert clears itself within a few minutes, it could be due to a transient power fluctuation. If it continues to appear, contact Mirapoint Technical Support immediately.
SYSTEM.WEBMAILLOGINS	WebMail service exceeded the user-limit license	If this alert appears, the number of unique WebMail logins per day has exceeded the license limit. Contact a Mirapoint Sales Representative to upgrade your WebMail user license to a higher allowed number.

UPS Alerts/Statistics

UPS Alert/Statistic	Description/Probable Cause	Recommended Action
UPS.CABHOT	The UPS is too hot	If this alert appears, try reducing the cabinet temperature and the ambient temperature.
UPS.CAPACITY	The battery capacity is nearing its end	If this alert appears and the appliance has not been shut down recently, the battery probably needs maintenance. Contact Mirapoint Technical Support immediately.
UPS.COMFAIL	The appliance cannot communicate with the UPS, or the UPS has sent garbled data that the Mirapoint appliance cannot understand	If this alert appears, check the UPS serial cable connections. If the condition lasts more than 10 minutes or happens frequently, contact Mirapoint Technical Support.
UPS.CPUHOT	The processor in the UPS is too hot	If this alert appears, try reducing the cabinet temperature and the ambient temperature.
UPS.CURRENT	Appliance is running on battery backup	If this alert appears, the appliance is running on battery backup because of a power loss. Work to restore power from the grid or backup generator.
UPS.LOAD	The load on the UPS is too great	If this alert appears, make sure only the main appliance and at most three disk enclosures are plugged into the UPS, it is not intended to handle additional load.
UPS.NOLOAD	The appliance is running, the UPS is running, and the cable is connected, but nothing is drawing power from the UPS	If this alert appears, check that the UPS serial cable is connected to the Mirapoint appliance.
UPS.RUNNING	Appliance is running on battery backup. This value is being deprecated	If this alert appears, the UPS lost AC power supply and is running the Mirapoint appliance on battery backup. Depending on the MOS version, the alert message may or may not give the remaining time. The UPS is used by the Mirapoint appliance to ensure a clean shutdown. After the AC power has been restored, the appliance will automatically power up when the UPS battery capacity reaches 65%.
UPS.SHUTDOWN	The appliance lost power and the UPS is starting to shut down the appliance. This value is being deprecated	If this alert appears, try to restore power from the grid or backup generator.
UPS.TIME	Approximate time in	If this alert indicates that the time is only 10 or 15 minutes, the batteries

UPS Alert/Statistic	Description/Probable Cause	Recommended Action
	minutes that the UPS could sustain the appliance on battery backup power	are reaching their end of life, you should consider replacing them.

Monitoring External Systems via SNMP

You can use the SNMP service Administration Suite pages (**Home > System > Services > SNMP**) to enable, disable, start, or stop this monitoring service, as well as configure SNMP monitoring options, hosts, and traps.

To configure SNMP monitoring on an appliance:

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

   The **Main Configuration** page appears.

2. Access MIB definition files by clicking one of the following **MIB Definition Modules** links:

   - **Master MIB**: The MIB definition file for every MIB object supported by the appliance.
   - **Enterprise MIB**: The MIB definition file for proprietary MIB objects supported by the appliance, a subset of the Master MIB.
   - **Traps MIB**: The MIB definition file for trap MIB objects supported by the appliance, a subset of the Master MIB.

   A text file opens that you can load on to your appliance 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.

3. In the **System Location** text field, type a text string describing to users of SNMP clients where your appliance is physically located.
4. In the **System Contact** text field, type your name, email address, or phone number so users of SNMP clients can contact you.
5. Click **Modify**.

SNMP MIBs are periodically updated. If you use SNMP to monitor your appliance, Mirapoint recommends downloading the MIB files from the appliance 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`.

Obtaining SNMP OIDs

You can obtain a complete list of all Mirapoint-specific SNMP Object Identifiers (OIDs) by reading the MIB definition files. For more information, see Monitoring External Systems via SNMP above. All Mirapoint-specific OIDs are identified by the following string:

```
iso.org <http://iso.org>.dod.internet.private.enterprises.mirapoint
```

This translates to the following string in numerical terms:

```
1.3.6.1.4.1.3246
```

Any specific OID starts with that string and has additional fields tacked on in order to get to the specific data you are looking for. For example, storage space is defined in the MIB as:

```
storageSpace OBJECT IDENTIFIER ::= { storage 1 }
```

This requires us to find the identifier for storage, which is:

```
storage OBJECT IDENTIFIER ::= { mirapoint 1}
```

So, in order to obtain the storage space OID you would use:

```
iso.org <http://iso.org>.dod.internet.private.enterprises.mirapoint.storage.storagespace
```

Which translates to the following string in numerical terms:

```
1.3.6.1.4.1.3246.1.1
```

If you are using an SNMP monitoring solution, such as HP Openview or Sun Net Manager, you should be able to import the Mirapoint MIBs so you do not have to specify these OIDs explicitly.

For more information on adding SNMP Hosts and SNMP Traps, see Adding SNMP Hosts on page 50 and Adding SNMP Traps on page 51.

Viewing the Message Queue

The queue-related Administration Suite pages (**Home > Queue**) provide information on and control of the appliance's message queue.

The message queue can be a valuable tool for tracking down a pegged appliance problem. However, only by observing your queue over time can you determine what a large queue for your appliances is. To determine why a large number of messages are being queued, use the **Sort Message Queue (Reason)** page to look for frequently occurring reasons. For more information, see Common Reasons Found in the Queue on the facing page.

About the Queue

Mail systems route mail through a Message Transfer Agent (MTA). MTAs accept messages from mail clients, mail enabled applications, and other MTAs. The MTA processes the message (i.e., 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/Junk Mail 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 (or stalled) for an external reason, or to sort and understand the traffic passing through the queue. You can perform these tasks on a running or working queue. Sometimes, after drilling-down into a queue, you might want to suspend the delivery process and clean up the queue (e.g., you are the victim of a spammer and there are thousands of messages backing up your resources). For more information, see Temporarily Stopping Mail Service on next page and Viewing and Acting on Sorted Messages on page 241.

Common Reasons Found in the Queue

When viewing a queue, especially a large queue, you will want to try and find common reasons. The following are some common reasons found when viewing a queue:

- 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, blacklist, or some other configuration setting.
- Operation Timed Out—Usually indicates that a target server is unreachable on the network. Either the appliance is down, the network is down, the appliance does not exist, or the appliance is overloaded to the point where it cannot 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 appliances.
- 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 do *not* have SMTP recipient check turned on, i.e., the **Reject Messages for Unknown Recipients** option set to **No** for the SMTP service.) 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 Viewing and Acting on Sorted Messages on page 241.
- 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. There are three values to monitor:

- Large queues—If the **Entries not yet processed** value 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, look at the other graphs, logs and reports, and try to isolate the bottleneck.
- Maximum queue size—If the **Total queue entries** value 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 yet processed** value 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 have not been processed, your appliance's performance is suffering. 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 retry. 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.

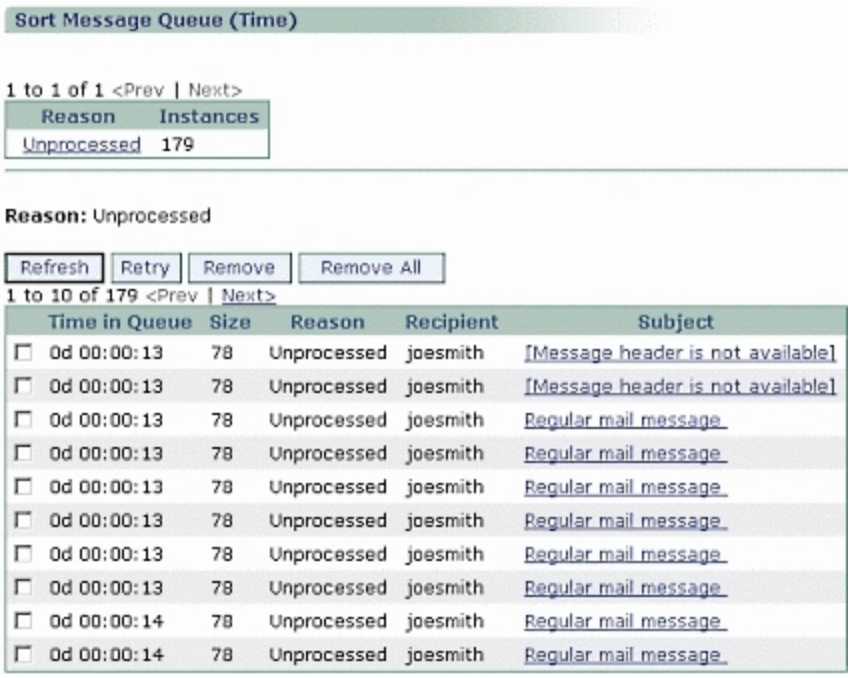
Temporarily Stopping Mail Service

If your queue is excessively large, you might want to temporarily stop all SMTP traffic. To do this, go to the SMTP service's **Main Configuration** page (**Home > 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. Make sure that you wait a few minutes before restarting the service by clicking **Start it**. You can also stop inbound mail without stopping the processing of the queue by altering the SMTP service's **TCP Port** (or Listen Port) within the **Inbound Connection Settings** section. 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.

Sorting the Message Queue

Use the **Sort Message Queue** pages (**Home > Queue > Sort**) 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. Once messages are displayed, you can act on them.

Figure 27 Sort Message Queue



You can use the following sort factors on messages:

- **Sort by Reason** - Messages are sorted by reason queued. The most common reason is listed first with the number of messages queued for that reason given.
- **Sort by 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.
- **Sort by 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.
- **Sort by 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.
- **Sort by 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.
- **Sort by Time** - Messages are sorted by time queued. The longest time length is listed first with the number of messages queued for that time given.

Additional information about sorting the message queue is provided in the following sections:

- About Message Envelopes and Headers on next page
- Viewing and Acting on Sorted Messages on page 241

About Message Envelopes and Headers

To view the envelope and headers of a message in the queue:

1. Go to **Home > Queue > Sort**.

   The **Sort Message Queue (Reason)** page is displayed by default.

2. Click any of the sort factor links in the left navigation menu (e.g., **Sort by From Host**, **Sort by From Address**, etc.).
3. Click a link in the **Subject** column of the message queue search results table.

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 within WebMail Direct Standard Edition or viewing the message in the **Message Pane** for WebMail Corporate Edition.

- **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 appliance 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 one of 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 (carbon copy) or Bcc (blind carbon copy) 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; may 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 it.
  - **Content-Type** - The MIME Content-Type used in a message such as text/plain, text/html, multipart/related, multipart/alternative, image/gif, and so on.
  - **MIME-Version** - Indicates that the message is MIME-formatted. The value is typically `1.0`.

- **X headers** - X headers are added by the mail processing function for various reasons. In general, they provide additional information about the message. Mirapoint uses the following X headers as indicated:
  - **X-DSN-Junkmail**- If this header is present, the message is a DSN (delivery status notification) for an undeliverable spam message. Its contents also contain the **X-Junkmail** header from the original message. You can use filters to discard all messages carrying an **X-DSN-Junkmail** header.
  - **X-DSN-Junkmail-Status** - Appears on DSN notices, includes the contents of the **X-Junkmail-Status** header from the original message, if any.
  - **X-DSN-Mirapoint-Virus** - If this header is present, the message is a DSN for a message in which a virus was detected. Its contents contain the **X-Mirapoint-Virus** header from the original message.
  - **X-Junkmail**: The UCE score that the message was given by the antispam engine that categorized it as junk mail. Example:

    ```
    X-Junkmail: UCE(190)
    ```

If a message has received an **X-Junkmail** header and, during domain or end-user content filtering, qualifies for the **X-Junkmail-Blacklist**, **X-Junkmail-Recipient- Whitelist**, **X-Junkmail-IP-Whitelist**, or **X-Junkmail-Blacklist** headers, then the antispam scanning **X-Junkmail** header is removed.

  - **X-Junkmail:RBL** - The message matched an RBL host list.
  - **X-Junkmail-Blacklist** - The message sender was on the Blocked Senders list for that domain or user. Examples:

    ```
    X-Junkmail-Blacklist: YES (by domain blacklist at example.com)
    ```

    ```
    X-Junkmail-Blacklist: YES (by user blacklist at example.com)
    ```

  - **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 Principal Edition Antispam. Example:

    ```
    X-Junkmail-Info: FORGED_RCVD_HELO,HTML_80_90,CLICK_BELOW
    ```

  - **X-Junkmail-IP-Whitelist** - The message IP was on the Allowed Senders list for that domain or user. Examples:

    ```
    X-Junkmail-IP-Whitelist: YES (by domain ip whitelist at example.com)
    ```

    ```
    X-Junkmail-IP-Whitelist: YES (by user ip whitelist at example.com)
    ```

  - **X-Junkmail-IWF** - Indicates whether or not Signature Edition RAPID Antispam with IWF (Internet Watch Foundation) was used to scan the message. Example:

    ```
    X-Junkmail-IWF: false
    ```

- **X-Junkmail-Loop-ID** - Inserted by some subsystems in order to prevent mail loops.
- **X-Junkmail-Premium-Raw** - Indicates that Premium Edition Antispam was used to scan the message.
- **X-Junkmail-Recipient-Whitelist** - The message recipient was on the Allowed Mailing Lists for that domain or user. Examples:

  ```
  X-Junkmail-Whitelistto: YES (by domain whitelistto at example.com)
  ```

  ```
  X-Junkmail-Whitelistto: YES (by user whitelistto at example.com)
  ```

- **X-Junkmail-Status** - The UCE score shown over the configured default UCE threshold and what host performed the scanning. Example:

  ```
  X-Junkmail-Status: score=0/50, host=example.com
  ```

  For more information, see About Antispam Scanning and Threshold on page 133.

- **X-Junkmail-Signature-Raw** - Indicates that Signature Edition RAPID Antispam was used to scan the message.
- **X-Junkmail-Whitelist** - The message sender was on the Allowed Senders list for that domain or user. Examples:

  ```
  X-Junkmail-Whitelist: YES (by domain whitelist at example.com)
  ```

  ```
  X-Junkmail-Whitelist: YES (by user whitelist at example.com)
  ```

- **X-Mirapoint-DKIM** - If DKIM security is enabled, this header indicates that the signature generation resulted in an error, of the form:

  ```
  X-Mirapoint-DKIM: [Invalid | Missing | Error | SigningError] extended-data
  ```

  Where *extended-data* specifies the type of error, invalid issue, or other data. If the signature generation was successful, a **DKIM-Signature** header is added instead. For more information on DKIM, see the *Mirapoint Administration Protocol Reference* or the *Mirapoint MOS Configuration Guide*.

- **X-Mirapoint-Received-SPF** - Added during an SPF (sender policy framework) check. It contains the sender's IP address, name from HELO/EHLO used in the SMTP greeting, the complete MAIL-FROM identity, and the enforcement-check result. Example:

  ```
  X-Mirapoint-Received-SPF: 192.168.62.170 example.com jdoe@example.com 0 fail
  ```

- **X-Mirapoint-IP-Reputation** - Added during a reputation check. It contains the reputation type, reputation source, scoring center's reference ID, and action performed. For more information about Reputation Hurdle, see the *Mirapoint MOS Configuration Guide* and the *Mirapoint Administration Protocol Reference*. Example:

  ```
  X-Mirapoint-IP-Reputation: reputation=Good-1,
  source=Queried,
  refid=0001.0A090301.4ADF21FC.0113,actions=spf tag
  ```

- **X-Mirapoint-Old-Envelope-From** - Keeps the original MAIL FROM header information (when using wiretaps the FROM is re-written).
- **X-Mirapoint-Old-Envelope-To** - Keeps the original RCPT TO header information (when using wiretaps the TO is re-written) .
- **X-Mirapoint-Virus** - Added during antivirus scanning to show attachment status. You can filter out messages from which viruses were removed, as it is no longer common for viruses to attach themselves to legitimate content.
- **X-Mirapoint-Virus-Scanfailure** - Added when the antivirus scanner failed to scan an attachment. Encrypted (password-protected) files cannot be virus-scanned.

  Malicious software can be distributed as password-protected compressed (e.g., zip) files that end-users are fooled into decrypting and opening. However, in general, the majority of encrypted attachments are legitimate user data.

- **X-Mirapoint-RAPID-Raw** - Indicates that the RAPID Antivirus scanner was used to scan the message. Example:

```
X-Mirapoint-RAPID-Raw:
score=unknown(0),refid=str=0001.0A020202.4ADFAF98.0118,ss=1,fgs=0,
ip=209.116.21.110,
so=2009-06-29 21:33:33,
dmn=2009-08-10 00:05:08
```

- **X-Mirapoint-State** - Tracks the filtering already done and remaining to be done.
- **X-old-subject** - Keeps the original subject (when the subject line has been modified).

The X-headers listed in this section are added by the Mirapoint MTA. However, any mail agent (such as another server or a client application that is sending the message) can add X- headers.

Only the envelopes and headers of messages are available for viewing on the message queue-related administration 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.

Viewing and Acting on Sorted Messages

To view sorted messages:

1. Go to **Home > Queue > Sort**.

   The **Sort Message Queue (Reason)** page is displayed by default

2. Click any of the sort factor links in the left navigation menu (e.g., **Sort by From Host**, **Sort by From Address**, etc.).

   The sort page for that factor displays with a status table list of sets of messages matching the sort factor in order of frequency as well as the number of Instances (queued messages) for each set.

3. Click an underlined sort factor link in the status table.

   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.

4. Use the following options to on displayed messages:

   - **Refresh** - Refreshes 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 click **Remove All**. This is different from the **Remove All** option on the **Get Queue Summary** page (**Home > Queue > Summary**) that wipes the entire queue.

To remove all messages in the queue for a particular domain, use the **Sort by To Address** factor to isolate all of the messages in a particular domain. Once you have all of those messages displayed, you can click **Remove All** to flush the queue. The **Remove All** option does not display unless there are messages in the queue.

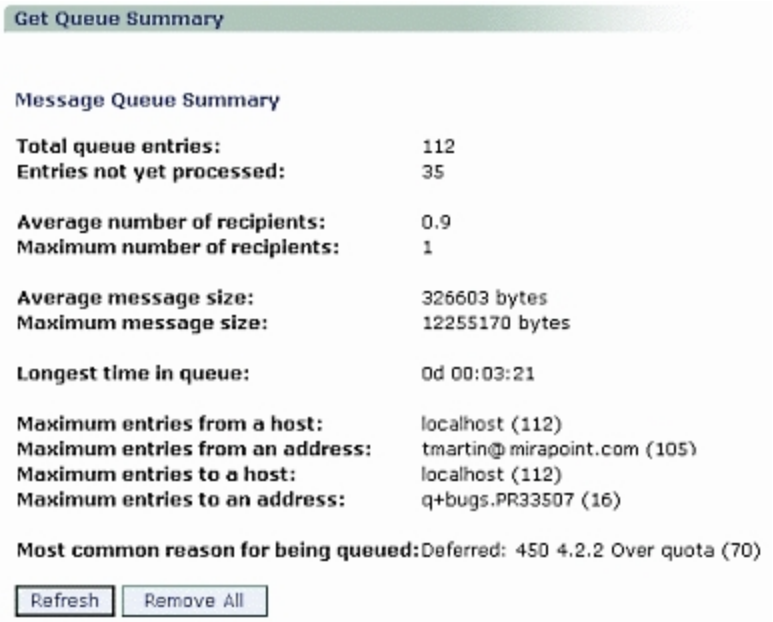
5. Click a link in the **Subject** column of the message queue search results table.

The **Envelope and Header** page for that message opens. For more information, see About Message Envelopes and Headers on page 238.

Viewing the Queue Summary

Use the **Get Queue Summary** page (**Home > Queue > Summary**) to get information on the current state of the queue.

Figure 28 Viewing the Queue Summary



The page displays the following options:

- **Refresh** - Immediately updates the queue.
- **Remove All** - Clears the entire queue.

Use the links on the left navigation menu to sort or search the queue. For more information see, see Sorting the Message Queue on page 236 and Searching the Message Queue on next page.

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.

The top three lines provide the following statistics on the over-all state of the queue:

- **Total queue entries** - The total number of entries in the queue.
- **Entries not yet processed** - The number of entries in the queue waiting for processing.
- **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 KBs (kilobytes), passing through the queue.
- **Max message size** - The maximum message size, in KBs.

The bottom six lines give the current statistics for each of the factors available through the **Sort Message Queue** 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 sent messages.
- **Maximum entries from an address** - The address, and number of sent messages.
- **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.

Searching the Message Queue

Use the **Search Message Queue** page (**Home > Queue > Search**) 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 29 Search Message Queue

The message 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 or equal to (>=) operator. Default Boolean operators can be overridden by prefixing the field entry with one of the other operators, such as the less than or equal to (<=) or equals (=) operator. For a list of default Boolean operators used by the search engine, see Operators for Search Parameters on the facing page.

Only the envelopes and headers of messages are available for viewing; the content, or body, of a message is restricted for viewing by the addressed recipients only.

To search for a message in the queue:

1. Go to **Home > Queue > Search**.

   The **Search Message Queue** page appears.

2. Type the appropriate data into any or all of the following text fields:

- **Queue ID** - The identification number system-assigned when the message arrives. Type in 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. Type in 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 in Operators for Search Parameters below.
- **Minimum Size** - The minimum size of the message. Type in an integer and select a size unit from the drop down list to restrict your search to messages that are not smaller than a given size. You can use the operators described in Operators for Search Parameters below.
- **Reason** - An explanation for why the message was not delivered. Type in a text string to search for a message that may be in the queue. Suggested reason searches, using the asterisk (*) wildcard, for example: `*Deferred: Connection refused*`, `*Deferred: Operation timed out*`, `*Deferred: Over quota*`, and `*read error*`.
- **Recipients** - The specified recipients of the message. Type in 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.

3. Click **Search**.

The search results display in a table below or a message displays indicating that the message is not in the queue. For more information, see Viewing and Acting on Sorted Messages on page 241.

Operators for Search Parameters

Operator definitions:

- = (equals)
- >= (greater than or equal to)
- <= (lesser than or equal to)

Table 30 Boolean Operators

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

You can use an empty string (""), which is equivalent to the wildcard character asterisk (*), meaning all message queue IDs.

Using Appliance Logs, Reports, and Graphs

This section describes the logs, reports, and performance graphs that are generated to monitor message traffic, security screening, and system operation.

The following topics are included:

- Receiving Daily and Weekly Reports on the facing page
- Abbreviations Used in Logs on page 259
- Viewing Mail Reports on page 260
- Viewing Login Reports on page 266
- Viewing Security Reports on page 270
- Viewing the System Information Report on page 274
- Viewing the Command Report on page 275
- Viewing the Folder Report on page 275
- Viewing the User Audit Trail Report on page 276
- Viewing the Admin Audit Trail Report on page 277
- Viewing Performance Graphs on page 277

All of the reports are more valuable when you have developed a good baseline understanding of your appliance. By monitoring the graphs and reports daily, you can familiarize yourself with the appliance's normal patterns and will be able to spot unusual activity more easily.

The **About Logs/Reports** page (**Home > Logs/Reports**) provides the following links:

- Mail - Shows all email traffic going through the appliance, and other appliance events.
- Logins - Shows connections to the system through the many access protocols and interfaces that the appliance offers.
- Security - Shows security-related events, including the identification of junk mail and virus-bearing messages, and content-filtering activity.
- System - Shows all appliance log events (for that day) in chronological order.
- Commands - Shows every administration protocol command received by the appliance on the selected day and all command responses.
- Folders - Shows all folders on the appliance hierarchically and alphabetically, the largest 50 folders, and the 50 folders that are closest to over quota.
- User Audit Trail - Shows all events for the selected user, day, and event type.
- Admin Audit Trail - Shows all administrative actions chronologically for the selected day.

Receiving Daily and Weekly Reports

The appliance 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 more information, see Reserved Distribution List Names on page 64 and Internal Distribution Lists for Monitoring on page 209.

Each day, the appliance sends the detailed mail and system logs to the **daily-reports** DL. Each week, the appliance sends a summary of the week's email traffic to the **weekly-reports** DL. The only default member on these lists is `Administrator`. However, you can add list members and send the daily and weekly reports to other addresses, including remote addresses if desired on the **Add Distribution List** page (**Home > Distribution Lists**). For more information, see Managing Distribution Lists on page 62.

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

The following reports are generated each day and sent to the **daily-reports** DL 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 more information, see Viewing Login Summary Information on page 267.
- A local mail summary—Each message delivered to or received from a local user. For more information, see Viewing Local Mail Traffic Information on page 261.
- A remote mail summary—Each message delivered to a remote recipient. For more information, see Viewing Remote Mail Traffic Information on page 262.
- Detailed connection logs—All connections and connection attempts to the POP, IMAP, and administration services for the selected day chronologically. For more information, see Viewing Detailed Login Information on page 268.
- Detailed mail logs—Chronological list of all SMTP transactions for the selected day. For more information, see Viewing Detailed Mail Logs on page 264.
- Folder size/quota information—Shows all folders on the appliance hierarchically and alphabetically, the largest 50 folders, and the 50 folders that are closest to over quota. For more information, see Viewing Folder Size and Quota Information on page 275.

The system log and security reports are each sent separately. The security reports listed below are sent as attachments to messages titled **Security**:

- Virus Summary—A summary of viruses found on your appliance during the selected day. For details, see Viewing Virus Scanning Summary Information on page 270.
- Virus Statistics—Detailed information about viruses found. For more information, see Viewing Detailed Virus Scanning Information on page 271.
- Content Filtering Summary—Detailed information about content filtering policies applied to messages on your appliance. For more information, see Viewing Content Filtering Information on page 272.
- Spam Summary—Detailed information about messages identified as junk mail. For more information, see Antispam Reports on page 255.
- Failed Connections by User—The failed login attempts by user for the selected day. For more information, see Viewing Failed Logins by User on page 269.
- Failed Connections by IP Address—The failed login attempts by connecting system IP address for the selected day. For more information, see Viewing Failed Logins by Remote IP Address on page 270.
- 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 more information, see Viewing MailHurdle Host Summary Information on page 273.
- 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 more information, see Viewing To Address and From Address Summary Information on page 273.
- 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 more information, see Viewing To Address and From Address Summary Information on page 273.

Weekly Reports

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** DL can facilitate troubleshooting if you encounter problems with your appliance and need to contact Mirapoint Technical 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 table details the format of weekly reports generated by a Message Server or RazorGate. You can refer to this information when writing scripts to extract information from weekly reports. Depending on the MOS version, your weekly reports might not include all of the field listed below. Mirapoint is constantly adding new fields to help monitor and provide better diagnostics for the appliance.

Table 31 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 rule groups 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 appliance. MIR for Message Server; SA for RazorGate.	MIR

Field	Description	Example(s)
ARRAYS	The arrays configured on the appliance; 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 appliance.	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. For more information, type `Help About Storage` in the CLI. (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 appliance. (Does not apply to RazorGates)	7
CALENDARSETTINGS	A list of calendar settings that have non-default values. (Does not apply to RazorGates)	timeout maxnumevents
CHASSIS	The appliance hardware	RG100
CONFENABLED	A list of features enabled on the appliance. (Not available on RazorGate 100s)	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 controller	2130S
COSENABLED	A list of features enabled by class of service on the appliance. (Not available on RazorGate 100s)	pop imap quota

Field	Description	Example(s)
CPU	The CPU type and speed in megahertz	686 2400
DEFAULTAUTHORIZATION	The authentication type accepted by the appliance. For more information, type `Help About Auth` in the CLI.	plaintext:local
DEFAULTLOCALE	The default locale on the 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 branding dictionary is native (factory installed) or non-native (custom installed). (Does not apply to RazorGates)	NonNative
DIRLOGGINSETTINGS	A list of directory logging settings that have non-default values	authentication index protocol replication
DIRSETTINGS	A list of directory settings that have non-default values	password-hash security
DISKS	The configuration of the RAID. (Not available on RazorGate 100s)	0.0.2.0 70007 Inuse Optimal (ECC no) 0.c2.0.0 0.a2.0.0 0.0.1.0 70007 Inuse Optimal (ECC no) 0.c2.0.0 0.a2.0.0 0.0.0.0 70007 Spare Optimal (ECC no) 0.c2.0.0 0.a2.0.0
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 appliance	68
DLSMEM	The total number of members in all distribution lists	66
DOMAINS	The number of delegated domains on the appliance. (Not available on RazorGate 100s)	9
ENET	The number of available ethernet ports	2
EXCEPTIONAL	A list of unusual system events, with a time string, event keyword, and short description for each event. Events are separated by blank lines. (format: yyyymmddhhmm)	200211080812 SYSTEM.REBOOT 200211091458 SYSTEM.REBOOT

Field	Description	Example(s)
FAILOVER	Whether failover is enabled or disabled. (Does not apply to RazorGates)	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 megahertz	686 2400
HWCPUCOUNT	Number of CPUs installed in the appliance	1
HWMEMORY	Megabytes of RAM installed in the appliance	1024
HWMODEL	The hardware model of the appliance	M400 RazorGate 100
HWSTORAGE	The type of disk enclosure on the appliance	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 login) settings that have non-default values	mta
LCD	The keypad and LCD panel firmware version number. (Not available on the M 50, RG 350s, or RG 100s)	3.2
LDAPSETTINGS	LDAP enabled features	autoprovision cachetimeout localcostable
LICENSES	A list of all applied licenses, user counts where applicable, and expiration dates where applicable	User-limit 750 SSL (strong encryption) SSH Signature Edition Rapid Antispam 750 users 01/12/2007 WebMail 300 users POP 750 users

Field	Description	Example(s)
		Sophos Antivirus 750 users 01/27/2007 Message Server
LOCALES	A list of all locales installed on the appliance	en_US.ISO_8859-1 ja_JP.utf-8
LOCALEUNANNOUNCED	A list of `Locale Set Unannounced` CLI command settings that have non-default values. For more information, type `Help About Locale` in the CLI.	ko_KR.utf-8
LOGINFOOTER	Indicates if the login footer is on or off (i.e., the language selection links on the WebMail **Login** page).	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 RazorGates)	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 (i.e., mailboxes) on the appliance. (Does not apply to RazorGates)	91
MAILBOXSETTINGS	A list of mailbox settings that have non-default values. (Does not apply to RazorGates)	broadcast
MEM	The megabytes of RAM installed in the appliance	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

Field	Description	Example(s)
		reversemx
NAMEDBRANDS	The number of named brands on the appliance. (Does not apply to RazorGates)	7
NDMPSETTINGS	A list of NDMP settings that have non-default values	port
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 appliance	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. (Does not apply to RazorGates)	0X210000e08b056b2
QUOTAPOLICY	A list of `Quota Setpolicy` CLI command settings that have non-default values. For more information, type `Help About Quota` in the CLI.	defaultsendoverquotamessage overquota sendoverquotamessage
RADIUSSETTINGS	A list of RADIUS settings that have non-default values	secret timeout
RAID	The RAID configuration used by the appliance	RTR
REBOOTS	A list of date and times in the previous week (one on each line) when the appliance rebooted. (format: yyyymmddhhmm)	200211080812 200211091458
REPORTVERSION	The report format version number	3.10
SERIAL	The appliance serial number	ESDW5420201
SERVICESENABLED	A list of the services enabled on the appliance	POP IMAP Calendar

Field	Description	Example(s)
		WebMail
SERVICESSTARTED	A list of the services started on the appliance	POP IMAP WebMail
SMTPSETTINGS	A list of SMTP settings that have non-default values	Omr Ldaprouting
SNMPSETTINGS	A list of SNMP settings that have non-default values	Syscontact Syslocation
SOFTVERSION	The software version number	3.10.1-FCS
SSLCERTIFICATE	Indicates if the SSL certificate is Mirapoint-issued or not	Mirapoint
STANDBY	The presence of the standby appliance and its Ethernet address. (Does not apply to RazorGates)	INACTIVE (no standby head is designated for failover)
STORAGE	The type of disk enclosure on the appliance	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 RazorGates)	local
SYSTEMBRAND	Indicates if there is a system brand. (Does not apply to RazorGates)	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 appliance	49
VIRTDOM	The number of virtual domains on the appliance. This field was deprecated as of MOS 3.0. (Not available on RazorGates)	0
VIRTDOMMEM	The total number of members in all virtual domains. Virtual domains were deprecated as of MOS 3.0. (Not available on RazorGates)	0
VIRUSSCAN	The antivirus license on the appliance and its configuration	LICENSED SOPHOS VERSION Sophos Antivirus SAVI2 2.2.03.098, Pattern file: 3.63, Incremental patterns: netdex-a nethf-c opaservc, Last updated: Sat Apr

Field	Description	Example(s)
		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 field list. For example, the third number in the LOCMSGRCV field's list is the number of messages delivered locally during the hour ending at the third hour in the TIMES field list.

The following table explains the meaning of each entry in the comma-separated list for each field.

Table 32 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 operations (Not available on RazorGates)
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 number of bytes received on the primary network interface per hour
FXPOBYTOU	The number of bytes sent on the primary network interface 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
FXPOPKTIN	The number of network packets received per hour
FXPOPKTOU	The 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 appliance over the previous one minute
LOAD15	The time-decaying average number of runable processes on the appliance over the previous 15 minutes
LOAD5	The time-decaying average number of runable processes on the appliance over the previous five minutes
LOCBYTRCV	The average number of kibi-bytes in all messages delivered locally per hour
LOCMSGRCV	The average number of kibi-bytes in all messages received by the appliance
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

Field	Description
MTAVERIFY.INITIALDENY	The Initial Deny setting for MailHurdle
POPCONN	Number of POP connections per hour
SMTPBYTRCV	The number of kilo binary bytes (kibi-bytes) in all messages received from remote appliances per hour
SMTPBYTSNT	The number of kibi-bytes in all messages sent to remote systems per hour
SMTPMSGRCV	The number of messages received from remote systems per hour
SMTPMSGSNT	The 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
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 RazorGates)
WEBMAIL.ATTACHADD	Number of times WebMail has performed the add attachment operation (Not available on RazorGates)
WEBMAIL.ATTACHDEL	Number of times WebMail has performed the delete attachment operation (Not available on RazorGates)
WEBMAIL.ATTACHREAD	Number of times WebMail has performed the read attachment operation (Not available on RazorGates)
WEBMAIL.CHECKMAIL	Number of times WebMail has performed the check mail operation since boot (Not available on RazorGates)
WEBMAIL.CHECKMAILMS	Milliseconds to process check mails operations since boot
WEBMAIL.CLEARALL	Number of times WebMail has performed the clear all operation since boot (Not available on RazorGates)
WEBMAIL.COMPACT	Number of times WebMail has performed the compact operation since boot (Not available on RazorGates)

Field	Description
WEBMAIL.COMPOSE	Number of times WebMail has performed the compose operation since boot (Not available on RazorGates)
WEBMAIL.DORMANT	Number of WebMail sessions inactive after an hour (not available on RazorGate)
WEBMAIL.FOLDERADD	Number of times WebMail has performed the folder add operation since boot (Not available on RazorGates)
WEBMAIL.FOLDERDEL	Number of times WebMail has performed the folder delete operation since boot (Not available on RazorGates)
WEBMAIL.FOLDERPAGE	Number of times WebMail has accessed the folder page since boot (Not available on RazorGates)
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)
WEBMAIL.LOGINMS	Milliseconds to process WebMail logins since boot (available for proxy only on RazorGate)
WEBMAIL.LOGOUT	Number of WebMail logouts since boot (available for proxy only on RazorGate)
WEBMAIL.MSGDEL	Number of times WebMail has performed the message delete operation since boot (Not available on RazorGates)
WEBMAIL.MSGDELMS	Milliseconds to process WebMail deletes since boot (not available on RazorGate)
WEBMAIL.MSGGOTO	Number of times WebMail has performed the message go-to operation since boot (Not available on RazorGates)
WEBMAIL.MSGMOVE	Number of times WebMail has performed the message move operation since boot (Not available on RazorGates)
WEBMAIL.MSGQUOTE	Number of times WebMail has replied in-line to a message since boot (Not available on RazorGates)
WEBMAIL.MSGREAD	Number of times WebMail has performed the message read operation since boot (Not available on RazorGates)
WEBMAIL.MSGREADMS	Milliseconds to process WebMail reads since boot (not available on RazorGate)
WEBMAIL.MSGREPLY	Number of times WebMail has performed the message reply operation since boot (Not available on RazorGates)
WEBMAIL.MSGSENT	Number of times WebMail has performed the message sent operation since boot (Not available on RazorGates)
WEBMAIL.MSGSENTMS	Milliseconds to process WebMail replies since boot (not available on RazorGate)
WEBMAIL.SEARCH	Number of times WebMail has performed the search operation since boot (Not available on RazorGates)
WEBMAIL.SELECT	Number of times WebMail has performed the select operation since boot (Not available on RazorGates)
WEBMAIL.SELECTALL	Number of times WebMail has performed the select all operation since boot (Not available on RazorGates)
WEBMAIL.SORT	Number of times WebMail performed the sort operation since boot (Not available on RazorGates)
WEBMAIL.TOC	Number of times WebMail has listed the table of contents, message list, for a folder since boot (not available on RazorGate)

Field	Description
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

Abbreviations Used in Logs

The following table provides definitions for the various abbreviations used in the logs:

Table 33 Abbreviations Used in Logs

Abbreviation	Description
" "	Empty command arguments
ADMIN	Administration service
CLR	Cleartext or non-secure
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
SVC	Service
TLS	Secure connection
WEBML	WebMail

Specific actions, such as changing WebMail user settings or visiting pages in the Administration Suite, will trigger administration protocol logins and commands. These internal logins are reported as `CLR:PLAIN` if plaintext is a permitted access method, regardless of the method used for external access.

Viewing Mail Reports

The **About Mail Reports** page (**Home > Logs/Reports > Mail**) provides links to reports that show all email traffic going through the appliance, as well as other events. Each day, the appliance 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.

The **About Mail Reports** page provides the following links:

- Top - The most frequent mail users for the selected day.
- Local - Each message delivered to or received from a local user.
- Remote - Each message delivered to a remote recipient.
- Traffic Summary - A summary of the mail traffic.
- Detailed - 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 appliance getting reset to zero. This is because the description for the statistics should match SNMP, and they get reset when you restart Sendmail.

Viewing the Top Mail Users

The **Top Mail Users** page (**Home > Logs / Reports > Mail > Top**) displays a report that summaries of the messages sent by each of the top 100 message originators for the selected date. 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, if necessary.

Having a null string (< >) at the top of this report does not necessarily reflect an issue with the data. The `Null Sender` is used for bounce messages and non-deliverable responses. If there are a lot of spam emails going through the appliance, a null string is likely to be at the top of this report.

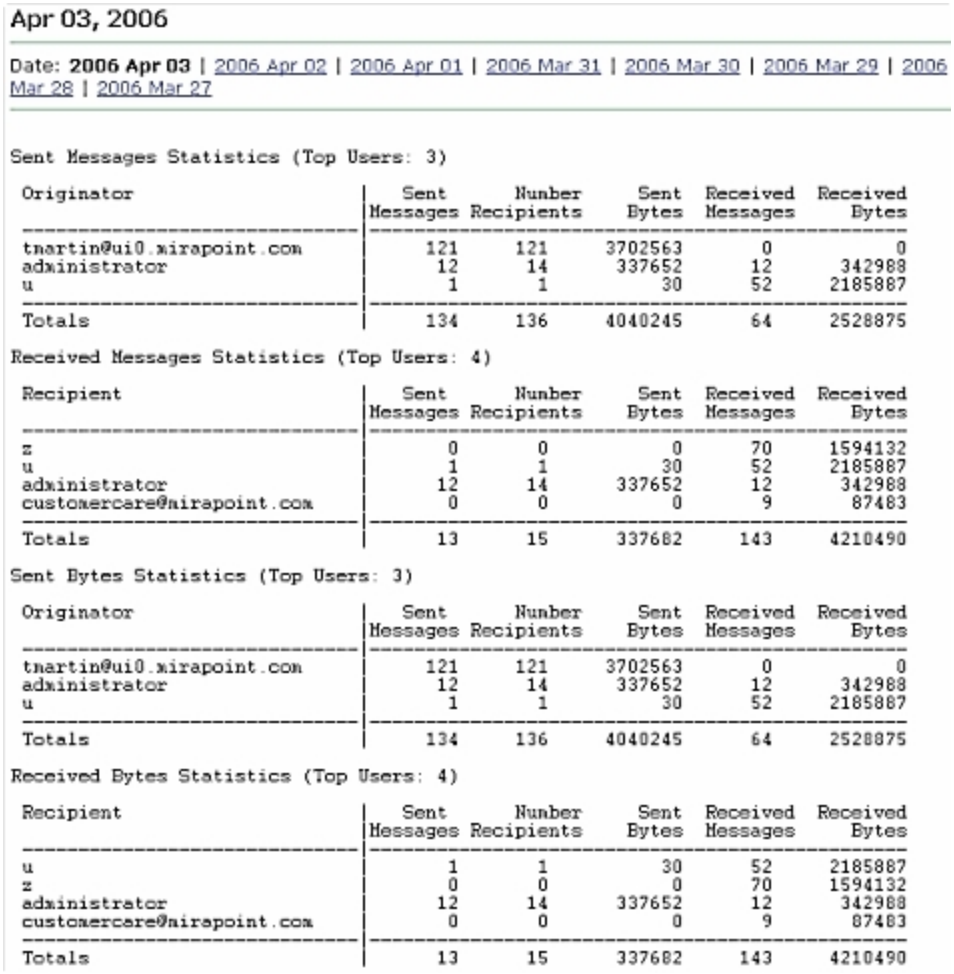
There are several top 100 lists (only a few might display):

- **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.

These lists contain the following fields:

- **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

Figure 34 Top Mail Users Page



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

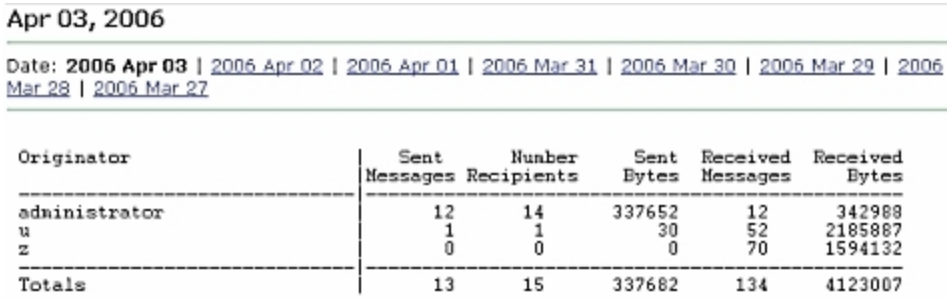
Viewing Local Mail Traffic Information

The **Local Mail Traffic** page (**Home > Logs/Reports > Mail > Local**) displays a report that shows data about the messages sent and received by each local email address on the appliance. 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, if necessary.

This report contains the following fields:

- **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

Figure 35 Local Mail Traffic Page



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

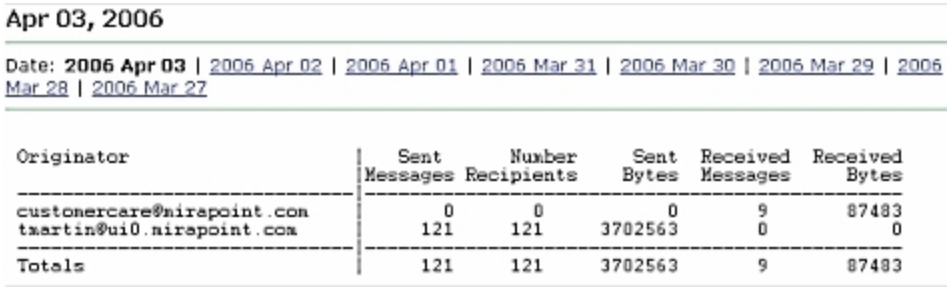
Viewing Remote Mail Traffic Information

The **Remote Mail Traffic** page (**Home > Logs/Reports > Mail > Remote**) displays a report that 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, if necessary.

This report contains the following fields:

- **Sent Messages** - The number of messages sent to the appliance by the remote address
- **Number Recipients** - The total number of recipients of all messages sent to the appliance by the remote address
- **Sent Bytes** - The total number of bytes sent to the appliance by the remote address
- **Received Messages** - The number of messages received by the remote address from the appliance
- **Received Bytes** - The total number of bytes received by the remote address from the appliance

Figure 36 Remote Mail Traffic



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@nirapoint.com	0	0	0	9	87483
tmartin@ui0.nirapoint.com	121	121	3702563	0	0
Totals	121	121	3702563	9	87483

Viewing Traffic Summary Information

The **Mail Traffic Summary** page (**Home > Logs/Reports > Mail > Traffic Summary**) displays a report that 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 section of the report, the following two tables of data appear:

  - Average Size Summary - A distribution of messages by message size
  - Average Number of Recipients Summary - A distribution of messages by number or recipients

  For more information, see Filtering Code Descriptions on page 265.

Use this report to see how busy the appliance 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 appliance.

Viewing Message Events by Hour

The **Message Events by Hour** summary shows the following fields for each hour of the selected date:

- **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

Viewing Average Size Summary Information

The **Average Size Summary** table shows the number of messages in each of several size ranges handled by the appliance during the most recent hour. Messages larger than 8 MB (megabytes) are counted in the same range.

This table contains the following fields:

- **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

Viewing Average Number of Recipients Summary Information

The **Average Number of Recipients Summary** table 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.

This table contains the following fields:

- **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

Viewing Detailed Mail Logs

The **Details Mail Logs** page (**Home > Logs/Reports > Mail > Detailed**) displays a report that lists all SMTP transactions for the selected day chronologically. This report is helpful in tracing a message through the appliance showing everything that happened to the message up to the point that it is delivered or leaves the appliance.

Full mail traffic logs for the day can be quite large, Mirapoint recommends using the search function to find references. For more information, see Searching Mail Logs on page 266.

Most web browsers provide a way to save a linked file directly to your disk without displaying it. If you find that the detailed reports are too large for your browser to display, you can save them to your local machine and view them using a text editor.

An example of the format of each transaction record is:

```
originator
   queue-id <message-id@example-host-name>
      evt-time event
      evt-time event...
```

Where:

- `originator` - The sender of the message
- `queue-id` - The unique ID that identifies the message within the mail queue
- `message-id@hostname` - 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 `@`*`hostname`*, where the value of `hostname` depends on the configuration of the originating host machine of the message
- `evt-time` - The time the event occurred
- `event` - The actual event description. The following is a list of common events:

- `received` *`num-bytes num-recipients host-received-from`* - The message was received.
- `filtering` *`code`* - The message was filtered for recipient. For more information, see Filtering Code Descriptions below.
- `Quarantined message deleted` - The message was manually deleted from quarantine.
- `Quarantined message approved as` *`queue-id`* - The message was approved and queued for delivery from quarantine.
- `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.
- `Sender blacklisted:` *`message-id@example-hostname`* - The *`message-id@example-hostname`* was placed on the recipient's blacklist due to a `Uce Addexception` CLI command setting. For more information, see the *Mirapoint Administration Protocol Reference*.
- `Sender is whitelisted by` *`recipient`* - The originator of the message was placed on the recipient's whitelist.
- `Split from` *`queue-id`* - The message was copied from `queue-id` and assigned a new queue ID to facilitate internal processing.
- `Split from quarantined message` - The quarantined message was approved and a new copy of the message, split off from the original quarantined message, was delivered.
- `UCE blacklist triggered from` *`host-received-from`* - The blacklist was triggered due to a `Uce Add block` CLI command setting (i.e., reject list). For more information, see the *Mirapoint Administration Protocol Reference*.

- `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; or, when recipient is unknown: `[response]`.

Filtering Code Descriptions

For the `event` option, `filtering` *`code`*, various codes are used to indicate what filtering took place. The `code` translates as follows.

- `A` - Already Done (this service already done; not repeating)
- `AV` - Antivirus
- `AS` - Antispam
- `D` - Default (this service done by default)
- `DS` - Domain Signatures
- `DF` - Domain Filters
- `IAV` - Antivirus, Inbound Only
- `IAS` - Antispam, Inbound Only
- `IDS` - Domain Signatures, Inbound Only
- `IDF` - Domain Filters, Inbound Only
- `N` - Not Allowed (Class of Service (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` - Whitelist (Allowed Senders list)
- `Accept` - Host from which to accept `X-Mirapoint-State` header

Searching Mail Logs

The **Search Mail Logs** page (**Home > Logs/Reports > Mail > Search**) allows you to search the mail logs and view reports based on the specified text and dates.

To search the mail logs:

1. Go to **Home > Logs/Reports > Mail > Search**.

   The **Search Mail Logs** page appears.
2. Click the **Date** link for the day you want to search.
3. In the **Search** text field, type the text string you want to find.
4. (Optional) In the **in last** text field, type 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.
5. Click **Search**.

The **Detailed Mail Logs** report for that date displays. The fields are described in Viewing Detailed Mail Logs on page 264.

Viewing Login Reports

The **About Login Reports** page (**Home > Logs/Reports > Logins**) provides links to reports that show connections to the system through the access protocols and interfaces that the appliance offers. These include WebMail, WebCal, POP, IMAP, and the Administration Protocol.

The **About Login Reports** page provides the following links:

- Top - The most frequent logins for the selected day.
- 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.
- Traffic Rates - The number and rate of logins for each hour of the selected day. Changing the appliance's timezone setting during the report period causes a gap or repetition in the hours listed.
- Detailed - All connections and connection attempts to the POP, IMAP, and Administration services for the selected day chronologically.
- Failed by User - The failed login attempts by user for the selected day.
- Failed by IP - The failed login attempts by connecting system IP address for the selected day.

Viewing Top Logins By User

The **Top Logins By User** page (**Home > Logs/Reports > Logins > Top**) displays a report that lists by user login name the 100 users who made the most connections to the system.

Each line in the report contains the following fields:

- **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 directly).
- **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), `LCL` (local user administrator) `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) or `KERB5` (Kerberos version 5).
- **Stat** - The status of the connection. No value means the connection was successful and `FAIL` means the connection was unsuccessful.
- **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`.

Viewing Login Summary Information

The **Login Summary** page (**Home > Logs/Reports > Logins > Summary**) displays a report that 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 as the **Top Logins By User** page report. For more information, see Viewing Top Logins By User above.

Viewing Login Traffic Rates

The **Login Traffic Rates** page (**Home > Logs/Reports > Logins > Traffic Rates**) displays a report that 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.

The report contains the following fields:

- **Time** - The hour to which the statistics apply.
- **POP/ Rate** - These two columns give the number of POP logins during the hour and the rate of logins in logins per second for that hour.
- **IMAP/Rate** - These two columns give the number of IMAP logins during the hour and the rate of logins in logins per second for that hour.
- **Admind** - The number of Administration service logins during the hour.
- **WebMail** - The number of WebMail logins during the hour.
- **WebCal** - The number of WebCal logins during the hour.
- **XMLcal** - The number of XML calls for WebCal during the hour.
- **Other** - The number of logins to other services during the hour.
- **Bad** - The number of failed login attempts for all services during the hour.

Viewing Detailed Login Information

The **Detailed Login Report** page (**Home > Logs/Reports > Logins > Detailed**) displays a report that 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 activity-count

Where:

- `event` - The login event. This is one of the following: `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 directly).
- `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), `LCL` (local user administrator) `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) or `KERB5` (Kerberos version 5).
- `IP-addr` - The IP address of the connecting host.
- `user` - The login name of the connecting user.
- `duration` - (for the `LOGOUT` event only) The duration of the connection in seconds.
- `activity-count` - A count of the number of appends (app), deletes (del), and expunges (exp) done by the user.

Viewing Failed Logins by User

The **Failed Logins By User** page (**Home > Logs/Reports > Logins > Failed By User**) displays a report that lists failed login attempts for the selected day by user. Users are listed in order by most failed login attempts.

Each line in the report contains the following fields:

- **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 directly).
- **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), `LCL` (local user administrator) `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) or `KERB5` (Kerberos version 5).
- **Stat** - The status of the connection. This 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.

Viewing Failed Logins by Remote IP Address

The **Failed Logins By Remote IP Address** page (**Home > Logs/Reports > Logins > Failed By IP**) displays a report that lists failed login attempts for the selected day by the IP address of the remote system attempting the connection. IP addresses are listed in order by 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 Viewing Failed Logins by User on previous page.

Viewing Security Reports

The appliance maintains daily logs of security-related events on the primary appliance, including the identification of junk mail and virus-bearing messages, and content filtering activity. The **About Security Reports** page (**Home > Logs/Reports > Security**) provides links to reports that contain this daily log information.

The **About Security Reports** page provides the following links:

- Antivirus - Summary and detailed information about viruses found on your appliance.
- Antispam - Detailed information about messages identified as junk mail.
- Content Filtering - Detailed information about content filtering policies applied to messages on your appliance.
- MailHurdle - Detailed information about MailHurdle policies applied to messages on your appliance.

If you have a 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 appliance is hit by some denial of service (DoS) or spam attack. If you are seeing that some valid mails are getting filtered (i.e., rejected/discard), then take a look at the content filtering report. The content filtering report tells you which filter triggered on a particular message.

Viewing Antivirus Reports

The **About Antivirus Reports** page provides links to reports that show a recent history of virus scanning activity on the appliance. The following reports are available:

- Summary - Displays the **Virus Scanning Summary** report (**Home > Logs/Reports > Security > Summary**), showing a summary of viruses found on your system during the selected day.
- Detailed - Displays the **Detailed Virus Scanning Information** report (**Home > Logs/Reports > Security > Detailed**), showing detailed information about these viruses.

Viewing Virus Scanning Summary Information

The **Virus Scanning Summary** report contains the following lists 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** lists have the following fields:

```
address                 virus-name              count
```

The **Viruses Found** list has following fields:

```
virus-name              count
```

Where:

- `address` - The address that sent or received the virus
- `virus-name` - The name of the virus, as identified by the virus-scanning software
- `count` - The number of instances of this virus sent or received by this address

Viewing Detailed Virus Scanning Information

The **Detailed Virus Scanning Information** report lists, in table format, every virus event chronologically for the selected day. Each table row contains the following fields:

```
xport   Date:
        Virus: name in [mime-part] (filename)
        Recipient:
        Sender:
        Action:
```

Where:

- `xport` - The message transport protocol; this field always has the value SMTP
- `Date` - The date and time that virus was found
- `Virus: name in [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), 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
  - `QUARANTINED` - meaning that the message was forwarded to the specified quarantine address. For more information on the quarantine filter action, see How Antivirus Quarantine Works on page 107.

Viewing Antispam Information

The **Antispam Information** page (**Home > Logs/Reports > Security > Antispam**) provides a report that shows the history of antispam scanning activity on the system for the selected day. The report contains the following lists:

- **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 lists include the following fields:

```
address                 sent-recv   count
```

Where:

- `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

Viewing Content Filtering Information

The **Content Filtering Information** page (**Home > Logs/Reports > Security > Content Filtering**) displays a report that 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
```

Where:

- `domain` - The domain name (such as `example.com`) or pseudo-domain (such as `primary`, `local`, `nonlocal`, or `any`) to which the policy applies. For more information, see Creating a Message Filter on page 177.
- `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. For more information, see Creating a Message Filter on page 177.
- `count` - The number of messages to which this policy was applied during the selected day

Viewing MailHurdle Reports

The **About MailHurdle Reports** page (**Home > Logs/Reports > Security > MailHurdle**) provides links to reports that categorize the email addresses and domains responsible for spamming your appliance.

The About MailHurdle Reports page only displays if MailHurdle is licensed and enabled.

There are three summary reports:

- Host - displays a report that breaks down the information by hostname
- To Address - displays a reports that breaks down information by To address
- From Address - displays a report that breaks down information by From address

Use the MailHurdle 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. You can then exempt the sender or recipient, respectively, from MailHurdle using the Allowed Senders and/or Allowed Mailing Lists filters. For more information, see Managing Allowed Senders on page 136 and Managing Allowed Mailing Lists on page 141.

Viewing MailHurdle Host Summary Information

The **MailHurdle Host Summary** page (**Home > Logs/Reports > Security > MailHurdle > Host**) displays a report that breaks down the information by host name. It is sorted by the percentage of messages rejected, and then total number of rejections.

This report has the following fields:

```
From Hostname        % Delayed     Msg Rejects     Msg Accepts     Sending IP
```

Where:

- `Hostname` - The host running MailHurdle.
- `% Delayed` - The percentage of messages from that sender IP, that were delayed by MailHurdle because no valid triplet existed.
- `Msg Rejects` - The number of messages that did not retry within the allotted time period and were rejected.
- `Msg Accepts` - The number of messages that did retry within the allotted time period and were accepted for delivery.
- `Sending IP` - The IP address from which the spam came.

Viewing To Address and From Address Summary Information

The **MailHurdle To Address Summary** page (**Home > Logs/Reports > Security > MailHurdle > To Address**) and **MailHurdle From Address Summary** page (**Home > Logs/Reports > Security > MailHurdle > From Address**) display reports that break down the same information for each From and To address, respectively. The information is first sorted by the IP addresses, and then each chunk is sorted by the percent of rejections, and then the total number of rejections.

The **MailHurdle To Address Summary** report contains the following fields:

```
To          % Rejected     Msg Rej     Msg Acpt     Sender IP
```

Where:

- `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.

The **MailHurdle From Address Summary** report contains the following fields:

```
From        % Rejected      Msg Rej      Msg Acpt      Sender IP
```

Where:

- `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.

Viewing the System Information Report

The **System Information** page (**Home > Logs/Reports > System**) displays a report for a specified date that lists all system log events (for that day) in chronological order. This report includes **System Alert** messages not related to the persistent conditions reported on the **Alerts** page (**Home > Monitoring > Alerts**). To get a more complete analysis of system activity, view the **Alerts** page in addition to this report.

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 appears within the system information report.

The format for each line is:

```
year month day hh:mm:ss event cause
```

Where:

- `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

Viewing the Command Report

The **Command Report** page (**Home > Logs/Reports > Commands**) provides a report that lists every Administration Protocol command received by the appliance 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
```

Where:

- `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 a > or < character, which indicates whether `cmd-resp` is a command (>) or a command response (<)
- `cmd-resp` - The text of the command or command response. For more information about Administration Protocol commands, see the *Mirapoint Administration Protocol Reference*.

Viewing the Folder Report

The **Folders Report** page (**Home > Logs/Reports > Folders**) displays a report that provides various folder statistic information.

Additional information about the folder report is provided in the following sections:

- Viewing Folder Size and Quota Information below
- Viewing the Largest 50 Folders on next page
- Viewing the Top 50 Folders Nearest Quota on next page

Viewing Folder Size and Quota Information

The **Folder Size & Quota Information** section lists all folders on the appliance hierarchically and alphabetically. For example, the folders `user.fred.Draft` and `user.fred.Sent` would be represented as:

```
user
  fred
     Draft
     Sent
```

There is a **Folder Size & Quota Information** section for the primary domain and for each delegated domain on the appliance. Each line in the report contains the following fields:

- **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`

Viewing the Largest 50 Folders

The **Largest 50 Folders** section lists the largest 50 folders on the appliance by size, starting with the largest. Each line in this section has **Folder name** and **Size** fields, as described in Viewing Folder Size and Quota Information on previous page, except that **Folder name** is the full folder path, such as `user.fred.Draft` and not indented hierarchically.

Viewing the Top 50 Folders Nearest Quota

The **Top 50 Folders Nearest Quota** section lists the 50 folders that are closest to over quota, starting with the folder closest to quota. Each line in this section has **Folder name** and **Size** fields, as in the **Largest 50 Folders** section, and a **Quota Percentage** field that shows the percentage of quota that the folder is using. For example, a folder that is occupying 9 KB and has a quota of 10 KB has a quota percentage of 90%.

Viewing the User Audit Trail Report

The **User Audit Trail** page (**Home > Logs/Reports > User Audit Trail**) displays a report that searches for and lists all events for the selected user, day, and event type.

To view or download the User Audit Trail report:

1. Go to **Home > Logs/Reports > User Audit Trail**.

   The **User Audit Trail** page appears.

2. Select a **Date** link for the day you want to search.
3. In the **User** text field, type the user name you want to search for.
4. Select one or more of the **Events** checkboxes. The following event types are available:
   - **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
5. Click **Search** to view the reports or **Download** to download them to your local machine.

Each line in the report uses the following format:

```
hh:mm:ss GMT-offset: event
```

Where:

- `hh` - The two-digit hour of the event
- `mm` - The two-digit minute of the event
- `ss` - The two-digit second of the event
- `GMT-offset` - The signed, four-digit offset from Greenwich Mean Time (GMT), for example, `-0800`, which means GMT minus eight hours.
- `event` - An event log entry generated by the `Log Watch` command-line interface (CLI) command. For more information, type `Help About Log` in the CLI.

Viewing the Admin Audit Trail Report

The **Admin Audit Trail** page (**Home > Logs/Reports > Admin Audit Trail**) displays a report that lists all administrative actions chronologically for the selected day. Click **View** to display this report on screen or **Download** to save it to a file on your local machine.

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
```

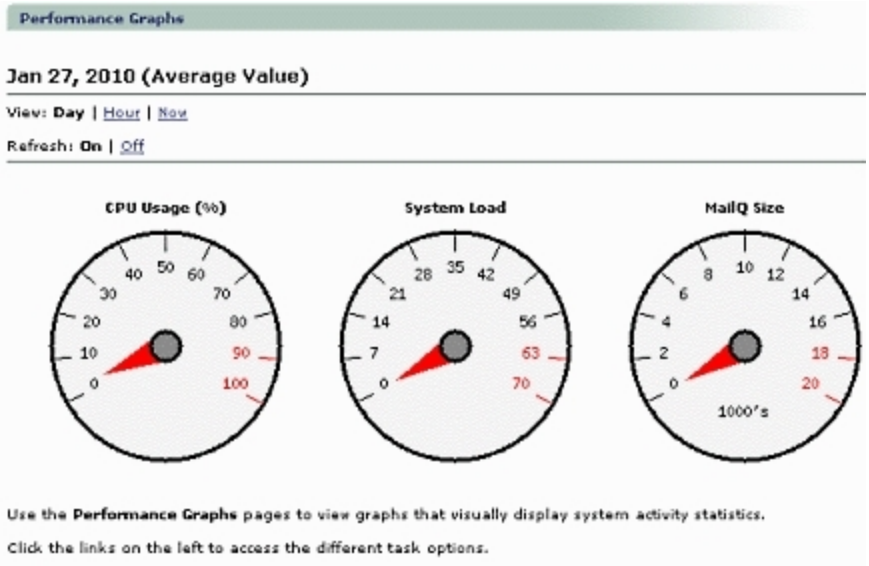
The remaining fields are as follows:

- `user` - The login name of the user performing the action. For delegated domain users, this includes the domain name
- `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`.

Viewing Performance Graphs

The **Performance Graphs** page (**Home > Performance Graphs**) displays three dial-type gauges.

Figure 37 Performance Graphs - Gauges



The values displayed are averages over the last day in the **Day** view, over the last hour in the **Hour** view, and an instant update in the **Now** view for:

- **CPU Usage (%)** - Percentage of the system CPU is use.

  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** - The run-queue of the system averaged over the past minute. This represents the number of processes waiting for resources. Busy appliances range from 20 to 50. Anything over 65 is considered overloaded. If you receive an alert based on `SYSTEM.LOAD`, check Performance Graphs.

  On a RazorGate, high system load could be caused by a spam or virus attack, so check the **Junk Mail Statistics** performance graphs (**Home > Performance Graphs > Junk Mail**). Network connections or degraded RAID disk could be the cause, so check the **Network Traffic** and **Disk Usage Information** performance graphs (**Home > Performance Graphs > Network** and **Home > Performance Graphs > Disk** respectively).

  The load trend typically increases over time because more users are using the appliance, 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 appliance resides in when the load trend moves above an average load of 4.0.

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.

- **MailQ Size** - The number of messages in process of being routed to another message transfer agent (i.e., Outbound Message Router) or to a local mail store (i.e., Inbound Message Router).

  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. Sometimes you will find a spike (i.e., rapid and short increase) in the mailQ size. This can mean several things:

  - You are the victim of a spammer.
  - 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.
  - Network failures. Runtime services, such as DNS or LDAP, are not accessible.

  Mirapoint appliances provide commands to further interrogate your mailQ to determine root cause for these spikes. For more information, type `Help About Mailq` in the CLI.

Additional information about performance graphs is provided in the following sections:

- About Performance Graphs below
- Pie Chart Categories on next page
- Viewing Mail Traffic on page 281
- Viewing POP/IMAP Activity on page 283
- Viewing WebMail Activity on page 284
- Viewing Junk Mail Statistics on page 284
- Viewing LDAP Directory Statistics on page 286
- Viewing Miscellaneous Services on page 288
- Viewing External Server Monitoring Information on page 289
- Viewing Disk Usage Information on page 291
- Viewing Network Traffic on page 293
- Viewing CPU Activity on page 295

About Performance Graphs

The performance graph-related administration pages provide a graphical representation of the activity on your appliance and only applicable graphs display. 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 in the **Day** or **Hour** view, a **Refresh** option displays. The **Refresh** option, when **On** (the default), causes the appliance to update the graph data every fifteen seconds. Click **Off** to stop the automatic updates.

The vertical axis of each graph is scaled to show the range of actual values to be presented. The graphs all start at zero. Each tick mark along the horizontal axis of a graph represents the following information:

- **Week** view - Each tick is one day
- **Day** view - Each tick is one hour
- **Hour** view - Each tick is 10 minutes.

In the graph plots, gaps can appear corresponding to reboots or changes in the system clock setting, indicated by a red line. On most performance graph pages, the graphs for the current week display by default. Click **Day** to view today's performance statistics or **Hour** to view statistics for the last hour.

Pie Chart Categories

Several graphs are pie charts that show percentages of a total by subsystem (i.e., category). The pie charts only count the actual disk reads/writes not reads and writes in and out of the buffer cache.

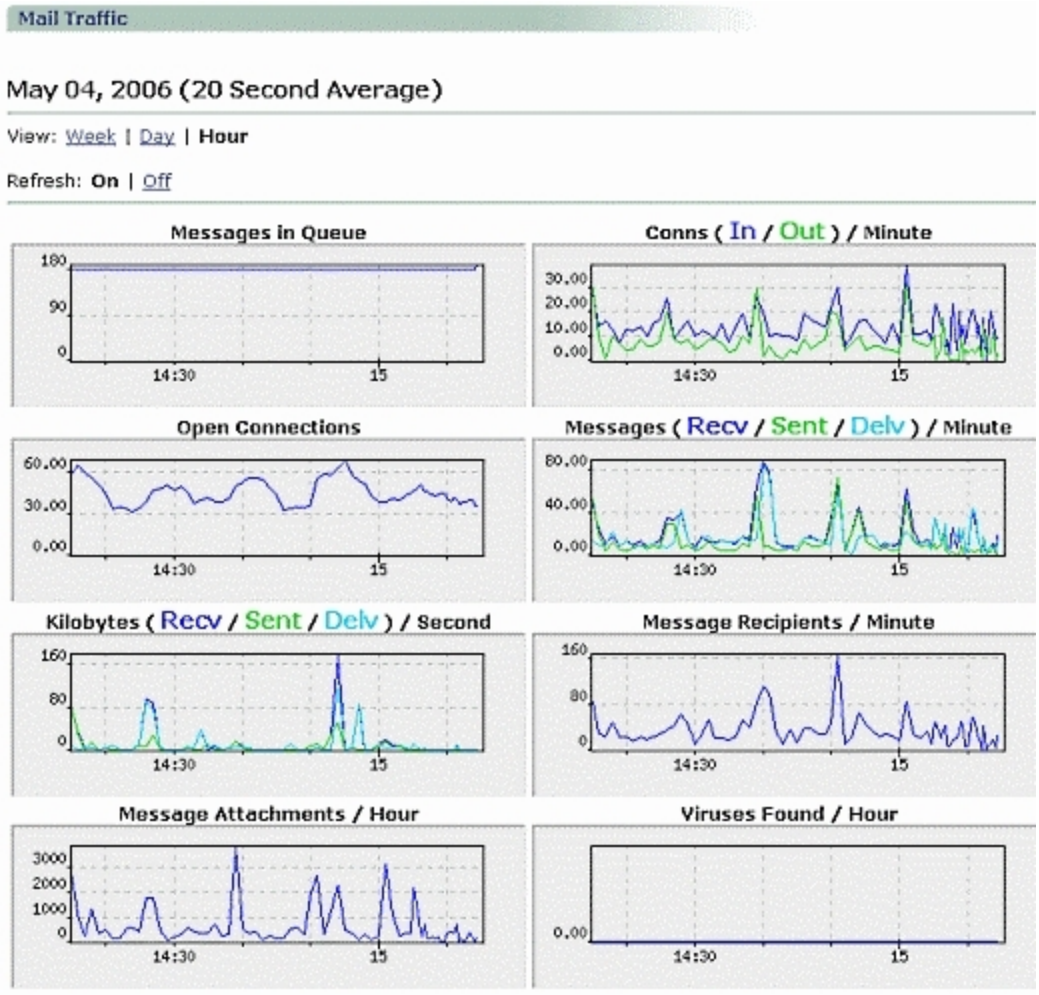
The possible categories are:

- Administration - Administration service
- Antispam - Antispam scanning
- Antivirus - Antivirus scanning
- 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-line interface (CLI) command
- Directory - Directory Server
- Filtering - Message filtering
- Idle - Unused capacity (Used in the **CPU Usage (%)** chart only)
- IMAP - IMAP service
- LDAP Client - LDAP client operations
- Logging - Log and MUL event generation
- Mail Delivery - SMTP service (local message delivery)
- Mail Transfer - SMTP service (except for local message delivery)
- Message Store - Internal message store management
- Monitoring - Appliance health monitoring activity
- Other - Combination of categories too small to be displayed individually and activity not classified in any other category. On appliances with a light load, this category can constitute a large percentage of total activity
- POP - POP service
- Periodic - Periodic automatic system self-maintenance activity, this includes tasks that are run using the `Schedule` command within the CLI
- Proxies - IMAP, POP, and HTTP proxy operations
- Security - SSL and SSH operations
- Upgrade - Messaging Operating System (MOS) upgrades and patch installations

Viewing Mail Traffic

The **Mail Traffic** page graphs (**Home > Performance Graphs > Mail**) shows tick marks along the horizontal axis representing one day of elapsed time in the **Week** view, one hour of elapsed time in the **Day** view, and ten minutes of elapsed time in the **Hour** view.

Figure 38 Mail Traffic Performance Graphs



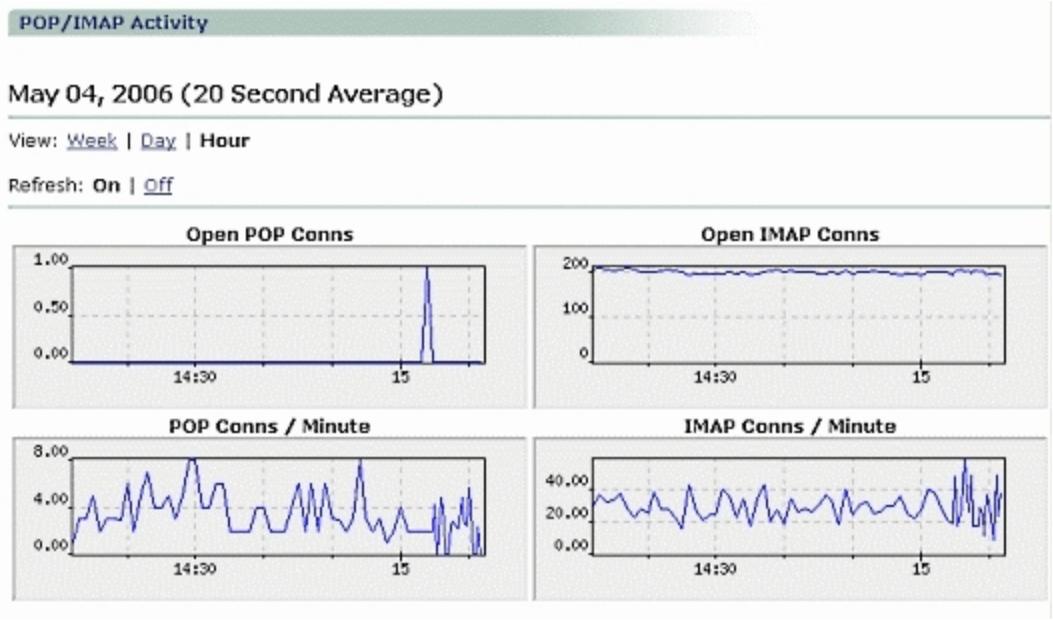
- **Messages in Queue** - Number of messages currently in the SMTP delivery queue.
- **Conns (In/Out) / Minute** - Number of incoming (In) and outgoing (Out) SMTP connections per minute, shown in different colors.
- **Open Connections** - Number of currently open SMTP connections.
- **Messages (Recv / 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.

Sharp changes in the queue size generally indicate that there is 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, the **Mail Traffic** performance graph metrics can tell you about when it started, which is often a vital clue.

Viewing POP/IMAP Activity

The **POP/IMAP Activity** page graphs (**Home > Performance Graphs > POP/IMAP**) 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 39 POP/IMAP Performance Graphs



- **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

The **POP Conns/Minute** graph provides an indication of how many users are using POP3. The **IMAP Conns/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.

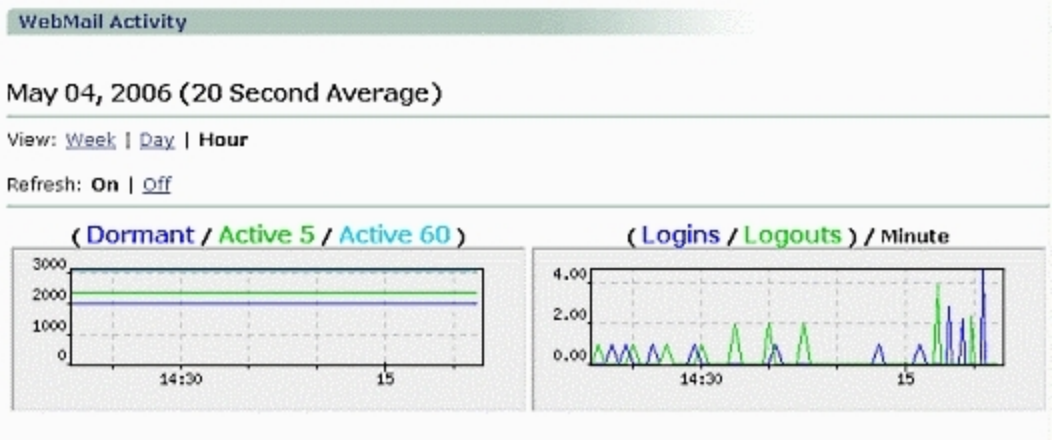
If the load average indicates a problem, and the CPU utilization indicates IMAP/ POP3 as a problem area, then these graphs might show a temporary spike indicating the cause. However, more investigation using the detailed logs is needed to narrow down the ultimate source of the problem.

Viewing WebMail Activity

The **WebMail Activity** page graph (**Home > Performance Graphs > WebMail**) statistics, **Dormant**, **Active 5**, and **Active 60**, represent buckets of time: connections idle for more than 60 minutes (dormant), connections active within the last 5 minutes, and connections active within the last 60 minutes. If the idle timeout period elapses, the connection is automatically terminated. The remaining WebMail 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. The **WebMail Activity** performance graphs are a good way to get a baseline understanding of how users on your appliance are using WebMail.

WebMail sessions are persistent across reboots. So, if a reboot occurs while users are logged in to WebMail, the reboot is not reflected in the graph.

Figure 40 WebMail Performance Graphs

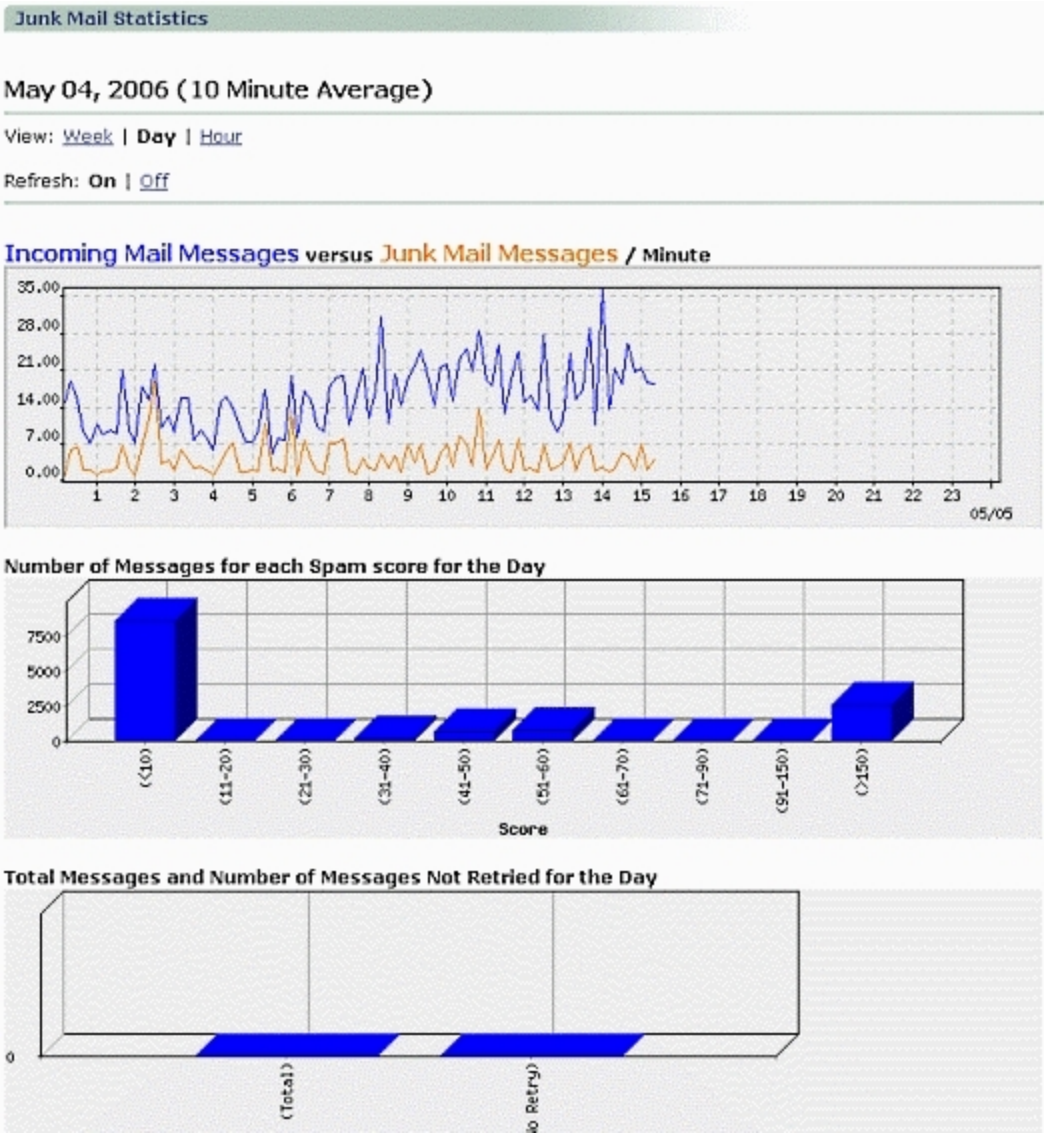


- **(Dormant / Active 5 / Active 60)** - This graph displays the following statistics:
  - **Dormant**: The number of sessions that have been idle for more than 60 minutes and less than the WebMail timeout setting, usually 360 minutes.
  - **Active 5**: The number of sessions that were active within 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 **Day** view, or it displays the average of 6 of these samples on the **Week** view.
- **(Logins / Logouts) / Minute** - Number of logins or logouts per minute since boot.

Viewing Junk Mail Statistics

The **Junk Mail Statistics** page (**Home > Performance Graphs > Junk Mail**) 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 41 Junk Mail Performance Graphs



- **Incoming Mail Messages versus Junk Mail Messages** - This graph shows two lines:
  - Incoming messages per minute (represented by a blue line)
  - Incoming junk mail messages per minute (represented by an orange line)
- **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 **Antispam Configuration** page (**Home > Antispam > Configuration**) 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 Antispam Scanning and Threshold on page 133.
- **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. For more information, see Managing MailHurdle on page 148.

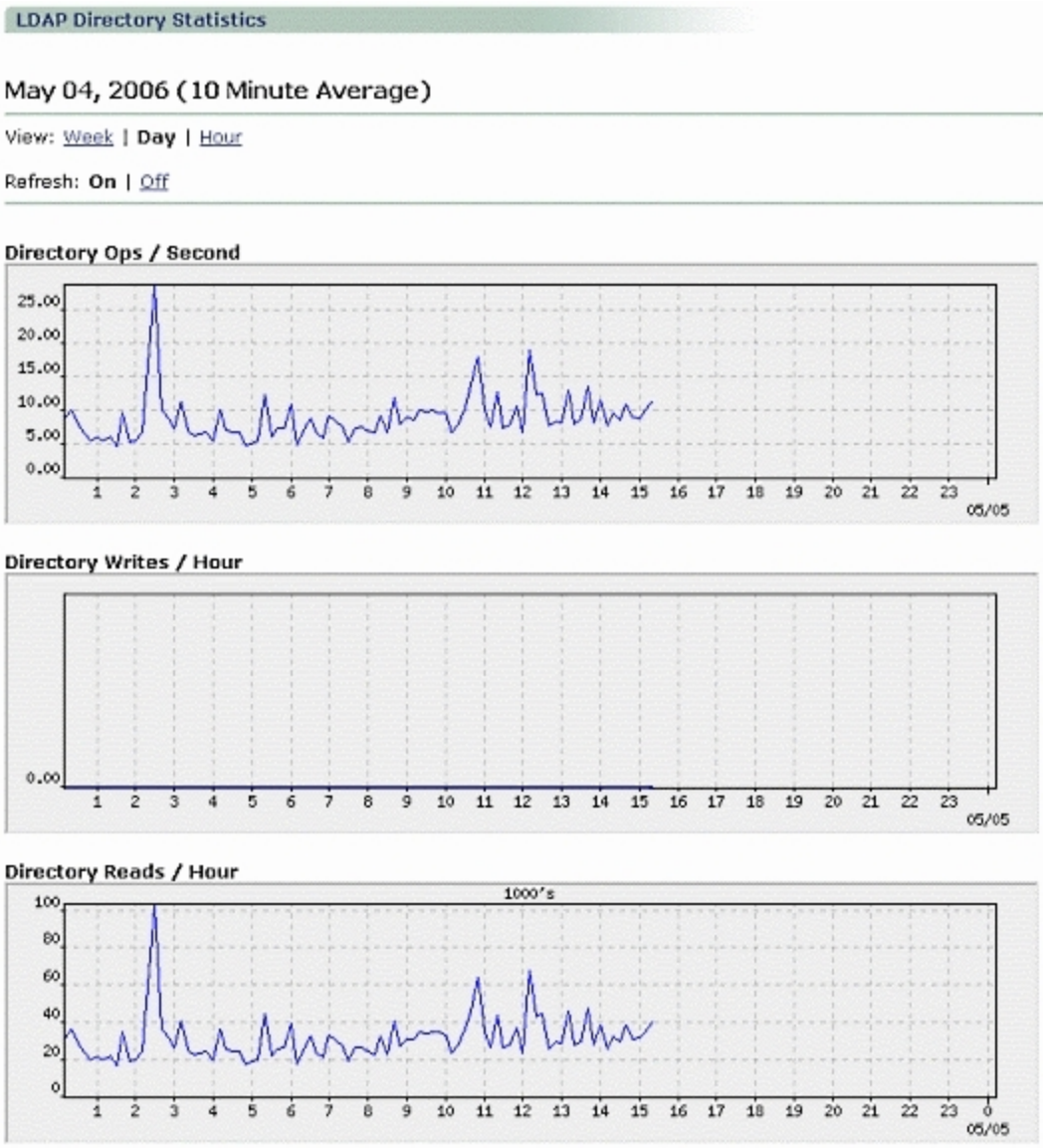
  In the **Total Messages and Number of Messages Not Retried for the Day** graph, the **Total** value represents the total number of messages received in a day (for the selected day). The **No Retry** value represents that no retry was accepted before the **Initial-Active** timeout (12 hours by default). It is 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.

Check the pattern for **Incoming Mail Messages versus Junk Mail Messages**. This data 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 **Advanced Content Filters** page (**Home > Content Filtering > Advanced**). For more information, see Creating Content Policies on page 172 and Creating Advanced Content Filters on page 173. You can also look for spam attacks in the **Junk Mail Statistics** graphs and check the logs to see if you can block IP addresses that are the source of the attacks.

Viewing LDAP Directory Statistics

The **LDAP Directory Statistics** page graphs (**Home > Performance Graphs > Directory**) 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 42 LDAP Directory Performance Graphs



- **Directory Ops / Second** - Number of directory server operations per second

The **Directory Ops/Second** graph shows the load on the Directory Server—the number of logins and transfers minus the effect of the cache. An overloaded Directory Server can result in user authentication timeouts and message bounces, so it is critical to ensure that your configuration can support the expected load. For a dedicated Directory Server, the overload point is 3,000 per second. In a mixed environment (for example, Message Server plus Directory Server), the overload point is 500.

- **Directory Writes / Hour** - Number of directory server writes per hour
- **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 minute
- **Connections / Minute** - Number of directory server connections per minute

In viewing the **Connections/Minute** graph, a peak could indicate a spam attack.

- **Completed Replications / Hour** - Number of server replication operations completed per hour

The **Entries Added/Hour**, **Entries Removed/Hour**, and **Completed Replications/Hour** graphs indicate true activity. If any of these graphs indicate activity that has not actually occurred, you may have been hacked.

High disk usage on a Directory Server-only appliance, 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 Directory Server capacity before you reach this point and load balance the Directory Servers with a Layer 4 load balancer. For more information on disk usage, see Viewing Disk Usage Information on page 291.

Viewing Miscellaneous Services

The **Miscellaneous Services** page graph (**Home > Performance Graphs > Misc**) 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.

The **Open Admin Conns** value is the number of open administration service connections.

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.

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 appliance, 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 (e.g., greater than 50) indicates a high load system on the provisioning system. Actions include:

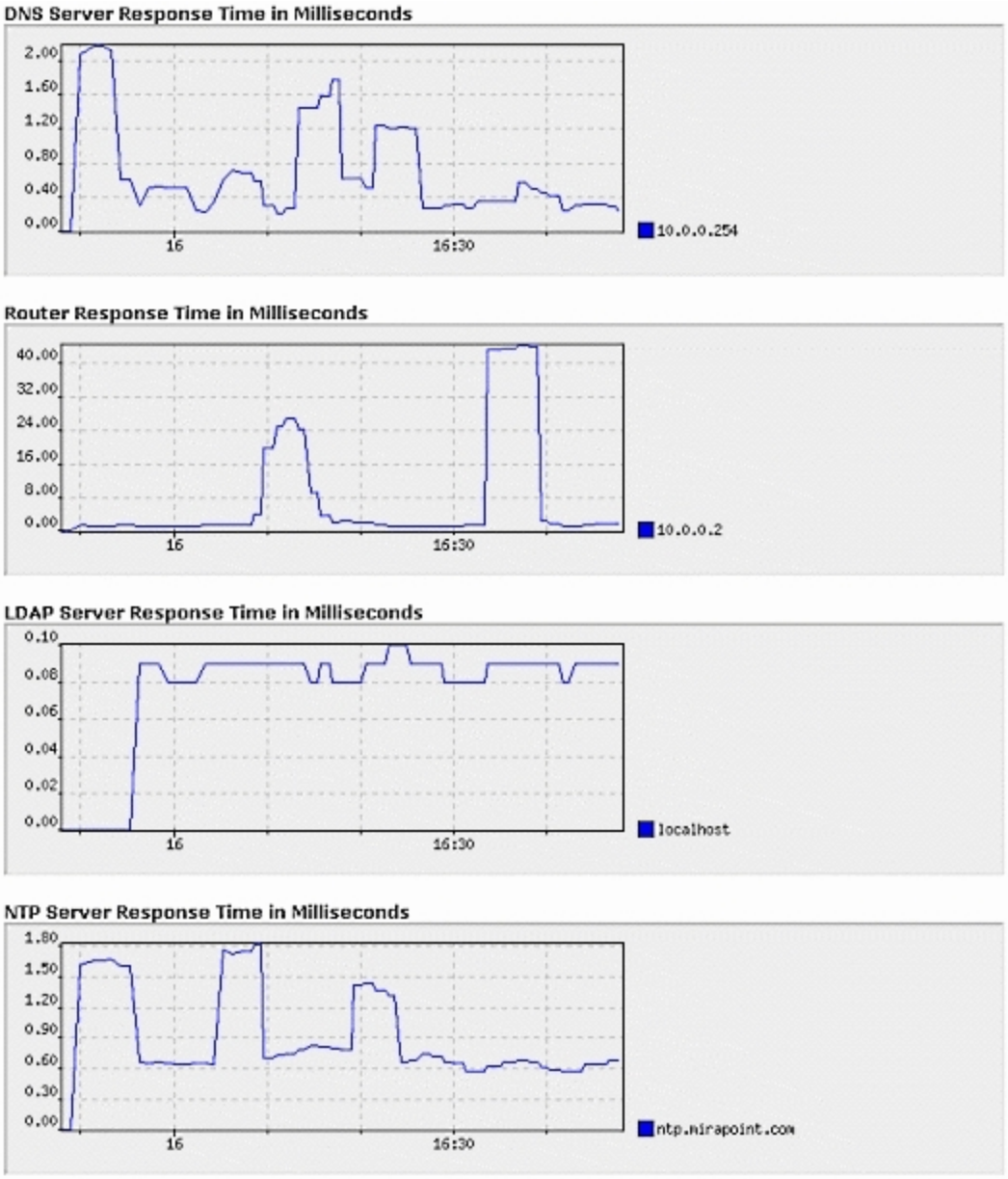
- Determining if the load is normal
- Re-designing the provisioning system to pool administration connections. A system that pools connections can support hundreds of thousands of users with no more than 30-40 connections.

Viewing External Server Monitoring Information

The **External Server Monitoring** page graphs (**Home > Performance Graphs > External**) 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 only display for configured servers.

Figure 43 External Performance Graphs



- **DNS Server Response Time in Milliseconds** - Response time of each Domain Name Server (DNS).

  The DNS Server Response Time is of concern if it slows to 1 second for 5 minutes. Less than 100 milliseconds is normal and anything over 500 milliseconds is an issue. If response time is 0, then no queries are happening. This is normal during initial configuration, but after deployment, DNS queries are happening most of the time on appliance that are operating normally.

- **Router Response Time in Milliseconds** - Response time of each network router.

  The Router Response Time is of concern if it exceeds 150 milliseconds and is a serious issue if it exceeds 500 milliseconds. This graph should show a consistent response time, any sustained peak is cause for concern.

- **LDAP Server Response Time in Milliseconds** - Response time of each Lightweight Directory Access Protocol (LDAP) server.

  The LDAP Server Response Time is of concern if it exceeds 100 milliseconds and is a serious issue 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.

- **NTP Server Response Time in Milliseconds** - Response time of each Network Time Protocol (NTP) server.

  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.

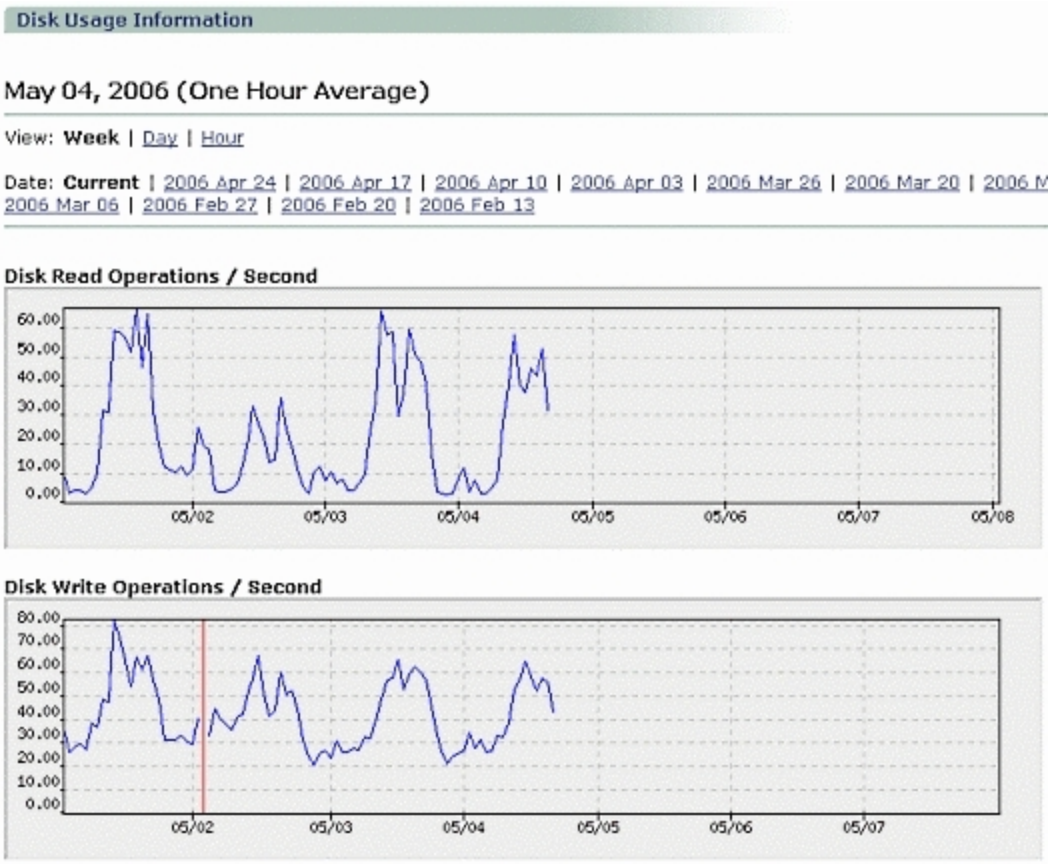
- **LDAP Server Response Time in Milliseconds** - Response time of each external Lightweight Directory Access Protocol (LDAP) server.
- **NIS Server Response Time in Milliseconds** - Response time of each Network Information Service (NIS) server.
- **RBL Server Response Time in Milliseconds** - Response time of each Realtime 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).

All of the graphs should show peaks at the same time. If not, you probably have a network problem, not a server problem. Make sure that you check your hardware (i.e., network cables, wires, etc.). Also, if you disable network monitoring (i.e., use the `Mon Disable Netmonping` command in the CLI), all response times in the **External Server Monitoring** graphs are flat-lined. For more information, type `Help Mon Disable` in the CLI.

Viewing Disk Usage Information

The **Disk Usage Information** page graphs (**Home > Performance Graphs > Disk**) 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 44 Disk Usage Performance Graphs



- **Disk Read Operations/ Second** - Number of disk read operations per second for one day. Measures block transfers.
- **Disk Write Operations/ Second** - Number of disk write operations per second one day. Measures block transfers.
- **Disk read activity by category** and **Disk write activity by category** - Show the percentage of total disk reads/writes performed by each subsystem. For a list of possible subsystems, see Viewing Disk Usage Information on previous page. The 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.
- **(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 **(Mail Store/System) % files used** percentage should be about half the **(Mail Store/System) % disk used** percentage.

High disk traffic is bad. Check your **POP/IMAP Activity** and **LDAP Directory Statistics** performance graphs (**Home > Performance Graphs > POP/IMAP** and **Home > Performance Graphs > Directory**, respectively) to troubleshoot the cause for the high traffic. Also, sluggish performance could come from any number of subsystems. Check the **Disk read activity by category** and **Disk write activity by category** pie charts to find causes.

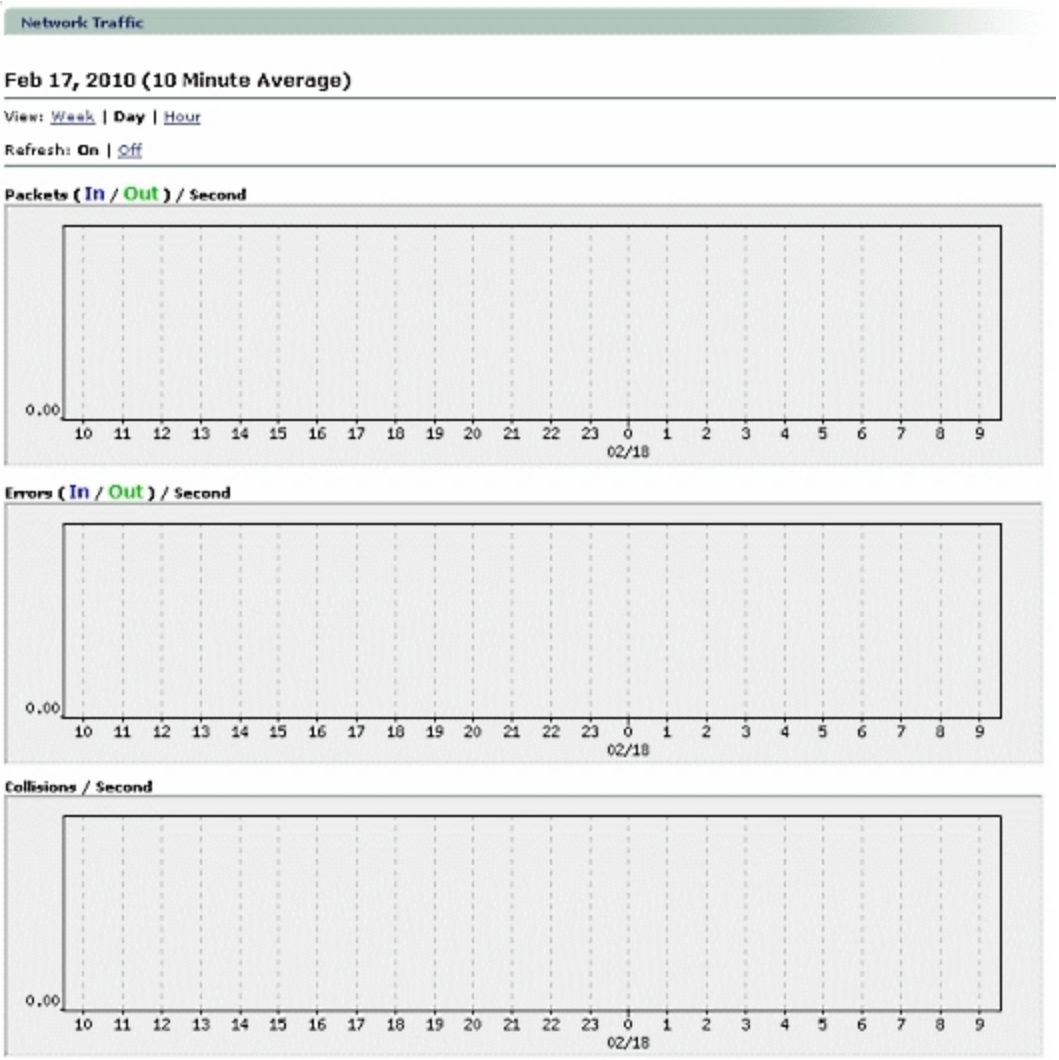
Figure 45 Disk Usage Pie Charts

If the **Disk Usage Information** performance 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.

Viewing Network Traffic

The **Network Traffic** page graphs (**Home > Performance Graphs > Network**) 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 46 Network Traffic Performance Graphs

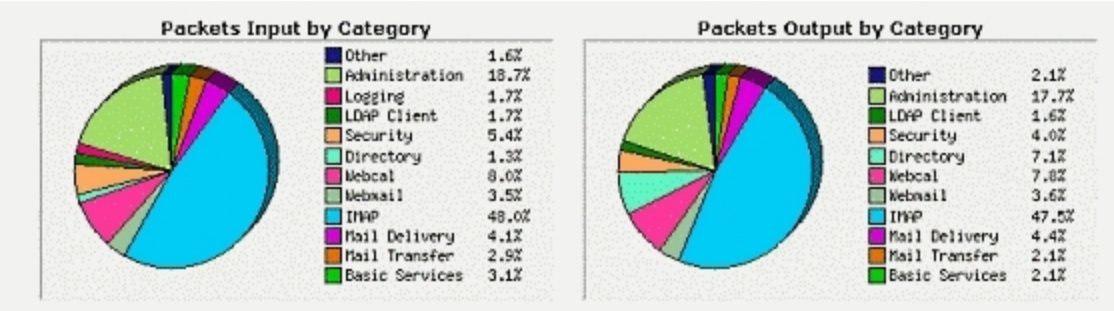


- **Packets (In / Out) / Second** - Number of incoming and outgoing network packets per second.
- **Errors (In / Out) /Second** - Number of incoming and outgoing network errors per second.
- **Collisions / Second** - Number of network packet collisions per second.
- **Packets Input by Category** and **Packets Output by Category** - Shows the percentage of total network packets received/sent by each subsystem. For a list of possible subsystems, see Pie Chart Categories on page 280.

If the **Network Traffic** page's pie charts are flat-lined, your network is down. If you see anything in the **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, i.e., a sustained peak, you need to check the network. A few spikes are normal, lots of spikes or sustained spikes is cause for concern. For more information on setting the NIC speed or duplex, type `Help Netif Set`in the CLI.

A sudden increase in the **Packets (In / Out) / Second** graph might indicate a denial of service (DoS) attack if it does not correspond with normal usage patterns. The **Packets Input by Category** and **Packets Output by Category** pie charts show what subsystems are getting and sending packets.

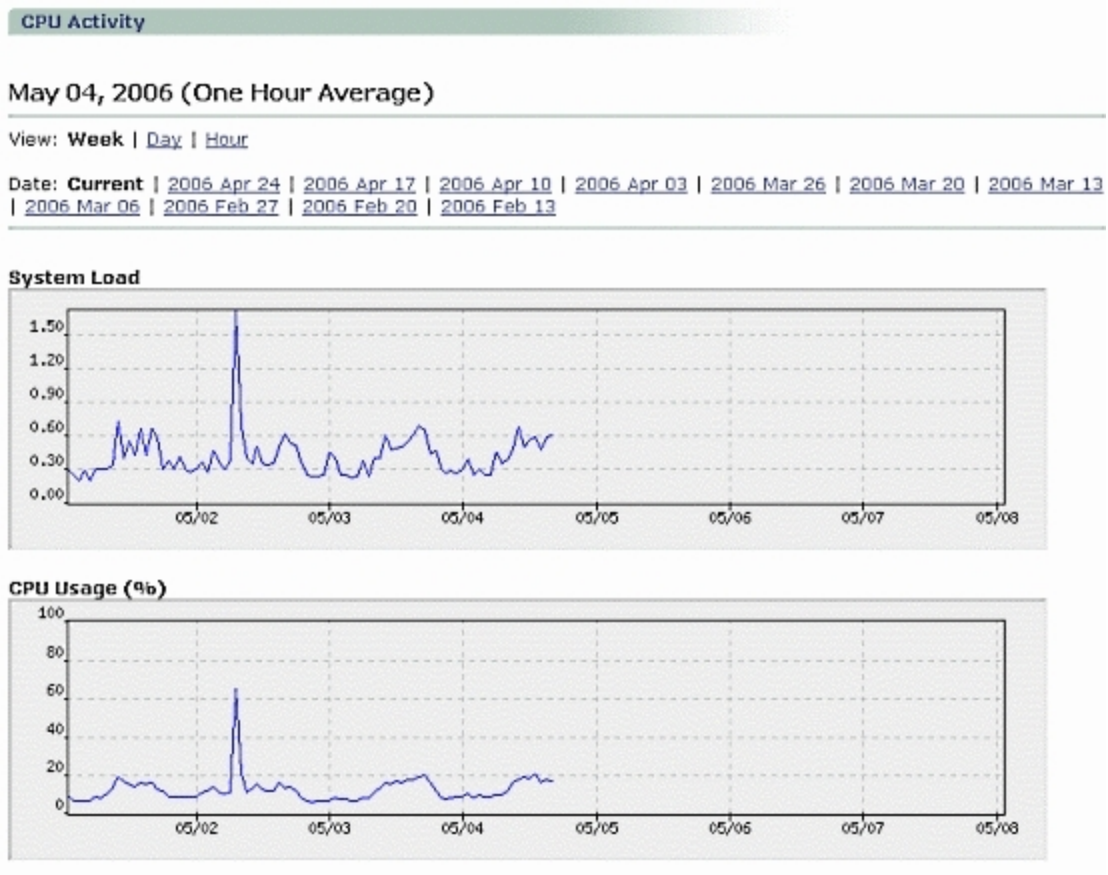
Figure 47 Network Traffic Pie Charts



Viewing CPU Activity

The **CPU Activity** page graphs (**Home > Performance Graphs > CPU**) 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 48 CPU Activity Performance Graphs



- **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 280.

If the **CPU Usage (%)** graph shows that the CPU is pegged, look at the **CPU Usage by Category (%)** pie chart to see what is 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.

Chapter 6: Managing Class of Service

This chapter describes how to create and manage Classes of Service (COSs) using the LDAP Class of Service Editor. Classes of Service allow you to create a set of policies and apply that policy set to a domain or an individual user.

The **Class of Service** page (**Home > Class of Service**) allows you to configure classes of service that can then be granted to users through the LDAP Enabled **Add User** page (**Home > Users**). The **Class of Service** page only displays if you have COS enabled and configured for your appliance. In order to do this you must also have LDAP provisioning configured properly using the command-line interface (CLI). When configured properly in the CLI, this page displays an **LDAP Enabled** label at the bottom of the page. For more information, see Enabling LDAP Provisioning for Junk Mail Manager on page 169 and Adding Users on page 57.

If a user is created on a domain that already has a COS assigned to it, that user automatically inherits that domain's COS. However, you can assign a different COS to a user in the domain, and that assignation will override the domain's COS. Also, if you remove a COS assignation from a user (i.e., assign them as **No COS**) the user 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.

The following topics are included:

- About Class of Service below
- Finding a Class of Service on next page
- Creating a Class of Service on next page
- Configuring a Class of Service on page 299
- Deleting a Class of Service on page 302
- Configuring Class of Service Message Features

About Class 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.

COS is a way of parceling different available features per a *class*. For example, a Gold class of service might include all available features, a Silver class might include fewer features, and a Bronze class might include only the most basic mail and/or calendaring features.

In addition to large features, such as Calendar and Junk Mail Manager (JMM), classes of service can be used to offer special security features such as antispam or SSL, or enhancement features such as External Mail or Message Undelete. Service classes can also be set with a mail quota for the entire class.

To control access to a particular service, you must enable Class of Service LDAP checking for that service, otherwise, all users can access the service if it is licensed and enabled. 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 appliance 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.

Once you have determined what classes you want to create with which features and options, you assign entire domains or individual users to that class. The domain or individual user is then bound by the features and restrictions defined for that class. For more information, see the *Mirapoint MOS Configuration Guide*.

Finding a Class of Service

To find a configured COS:

1. Go to **Home > Class of Service**.

   The **LDAP Class of Service Editor** page appears.

2. Type the name of the COS you want to search for in the **COS Name** text field. For more information on using wildcards, see Using Patterns and Wildcard Characters on page 191.
3. Click **Find** to display only those classes of service matching the entered name (ten names display per page).

Creating a Class of Service

To create a COS:

1. Go to **Home > Class of Service**.

   The **LDAP Class of Service Editor** page appears.

   If you do not have access to this page, make sure that you have successfully enabled COS and your LDAP server using the command-line interface (CLI). For more information, see the *Mirapoint MOS Configuration Guide* and *Mirapoint Administration Protocol Reference*.

2. In the **COS Name** text field, type the name you want for the COS (e.g., `Gold`).
3. Click **Add**.

The name of the new COS appears in the table. The option to add users to the COS also appears on the **Add Users** page (**Home > Users**).

To edit a COS:

1. Go to **Home > Class of Service**.

   The **LDAP Class of Service Editor** page appears.

2. In the table, click the **Edit** icon (✎) next to the name of the COS you want to edit. Click **Prev** and **Next** to page through the list of names, as needed. For more information, see Configuring a Class of Service below.

To remove a COS:

1. Go to **Home > Class of Service**.

   The **LDAP Class of Service Editor** page appears.

2. In the table, select the name of the COS you want to delete. Click **Prev** and **Next** to page through the list of names, as needed.
3. Click **Delete**.

Configuring a Class of Service

COS must be enabled using the command-line interface (CLI) during the set up of the Internal Directory service (an LDAP directory service is required for COS). For more information, see the *Mirapoint MOS Configuration Guide* and *Mirapoint Administration Protocol Reference*.

Once COS is enabled, and the LDAP server is set up (along with the LDAP GUI), you need to configure it with the services that you want it to include.

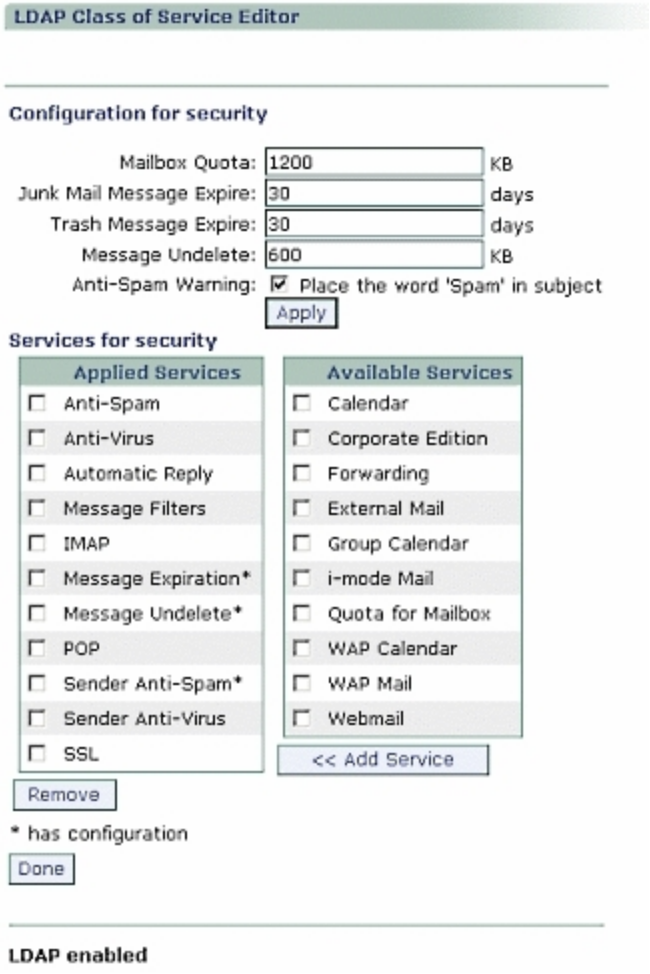
To configure a COS:

1. Go to **Home > Class of Service**.

   The **LDAP Class of Service Editor** page appears.

2. In the table, click the **Edit** icon (✎) next to the name of the COS you want to configure. Click **Prev** and **Next** to page through the list of names, as needed.

   Additional options appear within the **The LDAP Class of Service Editor** page.



3. Select the checkboxes next to the services that you want to make available to users of this COS.

The COS is entered to your directory server LDAP database, therefore, services that are not available on the appliance you are configuring can still be selected validly if they are licensed on the appliance that will use the COS.

The following services might be available (depending on licensing):

- **Antispam** - Inbound antispam scanning
- **Antivirus** - Inbound antivirus scanning
- **Automatic Reply** - WebMail auto-reply feature
- **Calendar** - WebCal Direct (Personal)
- **Corporate Edition** - WebMail/WebCal Corporate Edition
- **Message Filters** - WebMail message filters feature
- **Forwarding** - WebMail mail forwarding (vacation mail) feature
- **External Mail** - WebMail External POP mail feature
- **Group Calendar** - WebCal Direct (Group)
- **IMAP** - Message sending and receiving service
- **Junkmail Manager (JMM)*** - Spam mail management feature
- **Message Expiration*** - WebMail automatic message deletion
- **Message Undelete*** - Retrieve recently deleted messages feature
- **POP** - Message sending and receiving service
- **Quota for Mailbox** - Allows a quota to be set
- **Sender Antispam*** - Outbound antispam scanning
- **Sender Antivirus** - Outbound antivirus scanning
- **SSL** - HTTPS secure connections
- **WebMail** - WebMail Direct Standard Edition

Services that require additional configuration are starred (*).

If you create a COS and do not select any services, then all services are available by default.

5. Click **Add Service**.

Not all services should be COS enabled on every appliance. For example, the **Sender Antispam** and **Sender Antivirus** services should only be enabled on an appliance acting as an outbound message router (OMR). 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 (IMRs).

6. Depending on which services you elected to add to the new COS, you must set additional configuration options:

- **Mailbox Quota** - How many messages the user can receive before being over-quota and having messages rejected.
- **Trash Message Expire** - This option must be set for the **Message Expiration** service. How often the users **Trash** mail folder automatically deletes all messages.
- **JMM Message Expire** - This option must be set for the **Junkmail Manager (JMM)** service. How often a user's **Junk Mail** folder automatically deletes all messages.

Any mail folder can be configured to automatically delete messages by editing the LDAP attributes directly using the `Mailbox Msgexpirenow` CLI command. However, you must use the **LDAP Class of Service Editor** within the Administration Suite in order to configure the **Junk Mail** and **Trash** folders for this feature.

- **JMM Mailbox Quota** - This option must be set for the **Junkmail Manager (JMM)** service. How many messages a user can receive in their Junk Mail folder before being over-quota and having messages rejected.
- **Message Undelete** - This option must be set for the **Message Undelete** service. Provides a `deletedmessages` folder hierarchy where messages deleted from user folders (a two-step process) can be retrieved by an administrator. Some IMAP clients allow users to access the `deletedmessages` folder and retrieve messages themselves.
- **Antispam Warning** - This option must be set for the **Sender Antispam** service. Places the text `Spam?` in the **Subject** line of messages that were ranked as spam (junk mail) by the antispam scanner.

7. Click **Apply**.
8. Click **Done**.

You can now go to the **Add User** page (**Home > Users**) and apply classes of service to user accounts.

Deleting a Class of Service

You can delete, as well as create, a COS from the **LDAP Class of Service Editor** page.

To delete a COS:

1. Go to **Home > Class of Service**.

   The **LDAP Class of Service Editor** page appears.

2. In the table, click the **Delete** icon (✕) of the COS you want to delete. Click **Prev** and **Next** to page through the list of names, as needed.

   A confirmation page displays.

3. Click **OK**.

Appendix A: Managing Branding and Localization

Branding is a process that allows you to modify the look of a Mirapoint application (i.e., WebMail, Junk Mail Manager, etc.) by editing style sheets, images, etc. Branding can be applied system-wide to the primary domain or applied individually to delegated domains. This gives you the ability to reflect your company's corporate identity within the application. Use the branding-related administration pages to publish (i.e., upload) branded system zip files, upload custom dictionaries, select a brand, etc.

Mirapoint highly recommends reading the *Mirapoint Branding Guide* prior to branding any applications on your appliance.

Localization is the process of changing the language in which an application is presented. Your appliance's web pages can be localized using any Unicode characters. Localization can be applied system-wide to the primary domain and to delegated domains individually.

A localized appliance has the following qualities:

- The appliance is able to display foreign character sets.
- Some text fields are able to store foreign character sets. These fields also accept the input of foreign character sets.

Mirapoint also provides Localization Patches (L-Patches) for the appliance. An L-Patch is a special localization software upgrade not included in other releases. Each language is deployed in its own L-Patch, and its name reflects the relative MOS release number (e.g., 4.1.6, 3.10.6, etc.). You can download available L-Patches from the Mirapoint Technical Support website.

This appendix provides information on the following topics:

- Process Overview on next page
- Publishing a Brand on page 305
- Managing the Dictionary on page 306
- Selecting a Brand on page 310
- Downloading a Brand on page 311
- Deleting a Brand on page 312
- Assigning a Brand on page 314
- Customizing the Over-Quota Message on page 316
- Branding and Localization Tasks and Tips on page 318
- Installing a User Interface Localization on page 320

Process Overview

The branding process involves customizing the downloaded default files followed by the publishing of the customized files. The default files are downloaded as a zip file that includes WebMail (with Junk Mail Manager) and Calendar file sets of HTML templates, process files, images and online help files.

The branding process involves the following tasks:

1. Planning Your Brand/Creating a Custom Brand Document. The Custom Brand Document is your record of the changes implemented to produce your custom brand.
2. Setting Up Your Branding Environment. You must select a branding method, then download and unzip the default branding files. For more information, see Determining a Brand Method below and Downloading a Brand on page 311.
3. Customizing the Branding Files.
4. Testing Your Brand.
5. Zipping Your Brand Files.
6. Publishing Your Brand Files. For more information, see Publishing a Brand on the facing page.
7. Assigning Your Brand. For more information, see Assigning a Brand on page 314.

For more information on how to restore the default system brand to any domain, see Deleting a Brand on page 312. For detailed information on all of these tasks, see the *Mirapoint Branding Guide*.

The localization process can involve the branding process described here, or you can simply install a canned localization patch (L-Patch), or modify only the locale files of the factory system brand template files that you downloaded.

Determining a Brand Method

There are two methods of publishing a brand:

- System Brand—One domain automatically uses the system brand that you publish unless otherwise specified.
- Named Brand—Use a file set identical to the system brand for multiple domains, which provides the ability to use different Login pages per domain; and provides the ability to set the over-quota message per brand or per domain.

The appliance is capable of servicing multiple domains, each domain can have a separate named brand, and each brand can have multiple locales. This means each brand can be displayed in several languages, if desired. Named brands and the system brand have slightly different properties, and named brands can have different login pages per domain. Furthermore, the over-quota message can be set per brand or per domain.

Depending on how many brands you plan to do at a time, there are different procedures for each method. For more information about setting up system and named brands, see the *Mirapoint Branding Guide*.

Publishing a Brand

Use the **Publish** page (**Home > System > Branding > Publish**) to upload your branded files. Once you have downloaded, unzipped, customized, and zipped the branded files, you are ready to publish them to your appliance. For information on downloading the files, see Downloading a Brand on page 311.

To speed up publishing, delete directories that you do not want to brand. The system automatically uses the system default files if a directory is missing. Maintain the original structure, but `Mirapoint_apps_X.X` must be the top-level directory. Below that top-level directory are the directories you are including in your brand, in their original structure with their original names.

To publish your branded files:

1. Go to **Home > System > Branding > Publish**.

   The **Publish** page appears.

2. Select the **Type of brand**:
   - **System Brand**: Brands any domain assigned to system brand. Only one brand can be the system brand.
   - **Named Brand**: Brands any delegated domain assigned to it. If you select **Named Brand**, enter a name for the brand in the **Name** text field, the name you enter here is independent of the actual zip file name. For more information, see Changing Brands on next page.

3. In the **Specify the file to upload** text field, type the file path and name of your brand zip file or click **Browse** and navigate to the brand zip file if necessary. If the brand zip file you want to use was derived from an earlier Messaging Operating System (MOS) version, select **Use older zip file**.
4. Click **Publish**.

   The specified brand zip file is loaded onto your appliance. Your system brand takes the place of the default factory system brand. If you publish a named brand, you must next assign domains to it using the **Assign Brand** page. For more information, see Assigning a Brand on page 314.

Sometimes you need to stop and re-start the WebMail and WebCal (i.e., Calendar) services in order for the publishing process to complete.

Changing Brands

The name you give a named brand when you upload it is independent of the actual zip file name, this allows you to change named brands. At any time, you can publish any zip brand file set and use the same named brand name. All domains assigned that named brand automatically use the new brand files without you specifically reassigning them to the changed brand. For information on how to return to the default factory system brand, see Deleting a Brand on page 312.

Only one brand can be published at a time, if you try to publish more than one brand at a time a server busy message is displayed. If you have problems publishing or changing brands or errors are being displayed, see the troubleshooting information within the *Mirapoint Branding Guide*.

Managing the Dictionary

Use **Dictionary** page (**Home > System > Branding > Dictionary**) to download or publish dictionaries for use with the spelling function in your system brand or any named brand. All published dictionaries are available to all users on the appliance regardless of brand or domain. You can download a system dictionary, customize it, and then publish it, or you can publish a dictionary that you have obtained from another source.

This section contains the following information:

- Dictionary File Types below
- Dictionary Naming Convention on the facing page
- Downloading a Dictionary on the facing page
- Publishing Custom or Additional Dictionaries on page 308

Dictionary File Types

A dictionary has two types of files:

- The affix file defines word affixes for the associated dictionary and differs per language or locale. The affix file size is limited to 1 MB, and the line length is limited to 512 characters.
- The word file is a text file containing 7 or 8 bit characters, each separated with a carriage return. The maximum dictionary size is 2 MB, no word can be longer than 80 bytes, and only one word per line is allowed. Words may have trailing affix designators. There can be one or more word files.

The path of the dictionary is derived from the specified name of the dictionary.

The appliance supports Ispell-endorsed dictionaries. They can be found at the International Ispell Dictionary website. If you use a dictionary downloaded from the Ispell site, you will need to modify the directory structure before zipping it and uploading it to your Mirapoint appliance. Make sure that the affix file that you download is at the top-level of the directory structure and that the dictionary you choose (choose only one, often Ispell offers you more than one dictionary in a download) is in a directory named `dictionaries`.

Dictionary Naming Convention

The dictionary naming convention is as follows:

- Name - The first part of the dictionary name. This creates the directory where the dictionary lives and also displays in the **Dictionary** text field.
- Charset - The second part of the dictionary name, the coded graphic character set. All of the system dictionaries are based on the ISO-8859 family. You have the option of using other Ispell supported charsets, but you must specify the correct charset for your dictionary as the system uses the specified charset to translate the dictionary to UTF-8.
- Language - The third part of the dictionary name. In the form *`language_locale`*. For example, `fr_FR` (French language, French locale), `fr_CA` (French language, Canadian locale), `en_US` (English language, United States locale), or `en_BR` (English language, British locale).

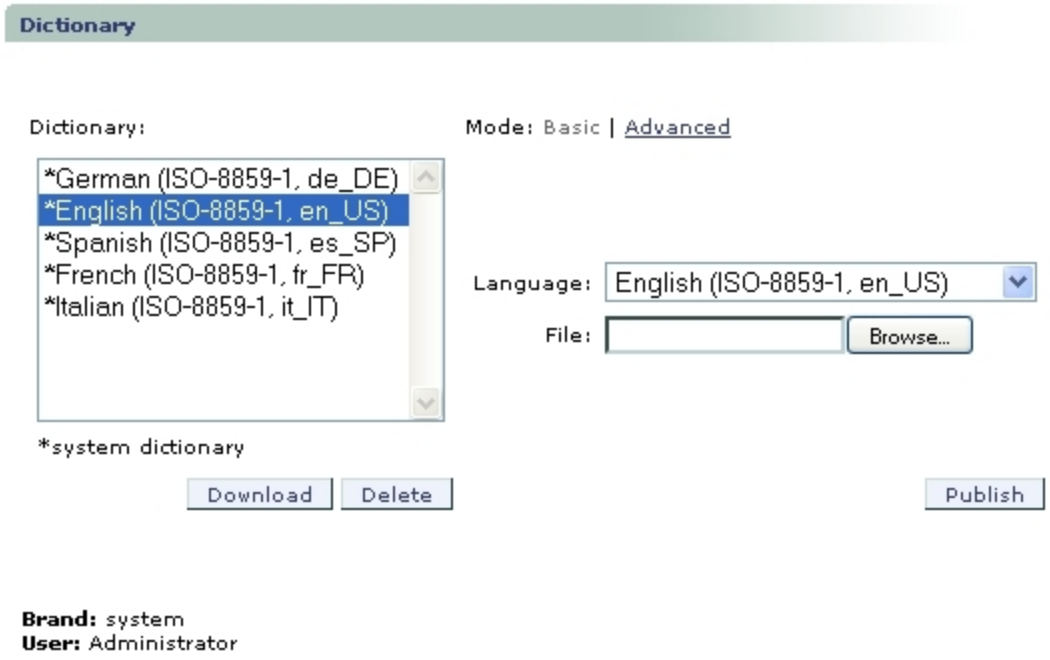
The **Dictionary** page provides a **Basic** Mode view for downloading, deleting, or publishing dictionaries. Also provided is an **Advanced** Mode view for specifying a **Name**, **Locale** and **Charset** for your additional dictionary.

Downloading a Dictionary

To download a dictionary for a brand:

1. Go to **Home > System > Branding > Dictionary**.

   The **Dictionary** page's **Basic** Mode view displays (the **Advanced** Mode is described in Publishing Custom or Additional Dictionaries on next page).



2. Choose one of the default dictionaries available to you in the **Dictionary** text box.
3. Click **Download**.

   A **File Download** dialog box displays.

4. Leave **Save this file to disk** selected and click **OK**.

   A **Save As** dialog box displays. Use the default directory, `Downloads`, or browse to a directory of your choice.

5. Click **Save**.

The dictionary zip file is downloaded to the specified directory. You can unzip the file, customize it, zip it, and upload it as a custom dictionary.

Publishing Custom or Additional Dictionaries

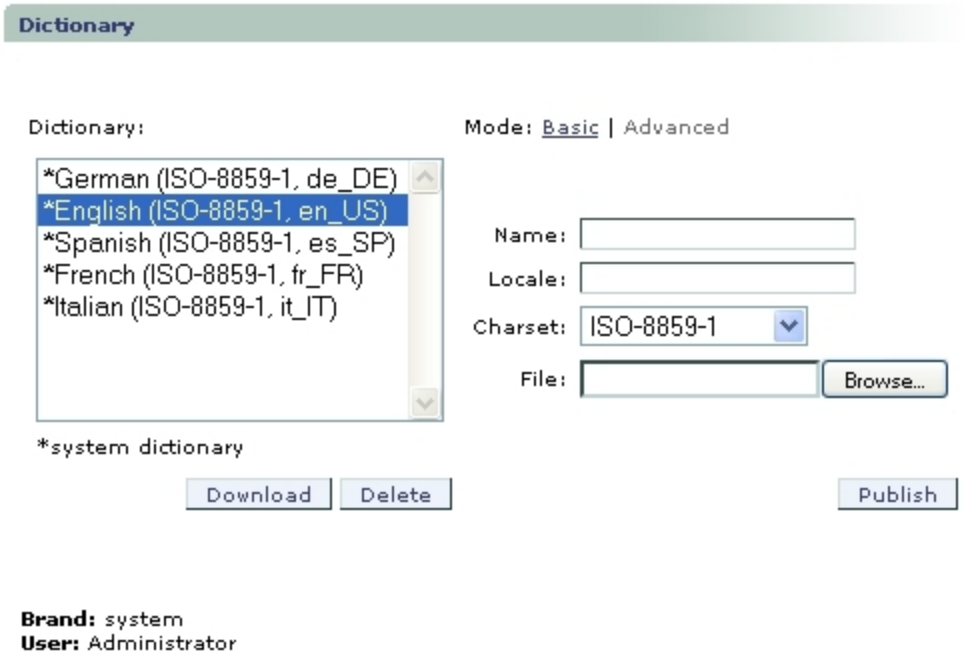
To publish a custom dictionary or additional dictionaries that you have loaded to your system:

1. Go to **Home > System > Branding > Dictionary**.

   The **Dictionary** page appears.

2. From the **Dictionary** page's **Basic** Mode view, select the appropriate language designation for your dictionary in the **Language** list. If you want to use a name that is not in the list, you must use the **Advanced** Mode view (see step 3).
3. (Optional) In order to use a name not in the **Language** drop-down menu, click **Advanced**.

   The **Advanced** Mode view appears.



a. Type in a **Name** for the dictionary.

b. Type in a **Locale** for the dictionary.

c. From the **Charset** drop-down menu, select a character set for the dictionary.

The appliance reads the specified **Charset** and uses it to instantiate the dictionary. It is important to choose a character set that matches the dictionary you are uploading.

4. In the **File** text field, type a directory path and filename, or use **Browse** to select a dictionary zip file on your local machine.
5. Click **Publish**.

When a dictionary is uploaded, the appliance reads the specified **Name**, **Locale**, and **Charset**, and uses that information to store the dictionary.

To delete a custom dictionary or additional dictionaries:

1. Go to **Home > System > Branding > Dictionary**.

   The **Dictionary** page appears.

2. Select one of the custom dictionaries that you have uploaded to the **Dictionary** text box. You cannot delete system dictionaries.
3. Click **Delete**.

Selecting a Brand

To select a brand to configure:

1. Go to **Home > System > Branding > Select Brand**.

   The **Select Brand** page appears.

2. Select the brand in the **Named brands** text box (or select the **System Brand**).
3. Click **Select Brand** for a named brand or **Select** for the system brand.

The brand you selected is indicated in the lower left corner of the page and is available for modification from in the other **Branding** pages.

If the brand selected was a named brand, only the selected brand displays as an option on the **Download** page (**Home > System > Branding > Download**) . If the brand selected was the system brand, a selection of brands display as options on the **Download** page. Four categories of files might be present on the **Download** page:

- The factory system brand zip files, UNIX and DOS formats of the same file, are always displayed:
  - `Mirapoint_apps_X.X.DOS.zip`
  - `Mirapoint_apps_X.X.UNIX.zip`

- If your system was upgraded, an additional set corresponding to the upgraded version displays.
- If L-Patches were installed, an additional set displays. These zip files contain the factory system brand files, plus any L-Patches. If you want to brand a localized version of the factory system brand, download the appropriate localized zip file and modify it.
- If a custom system brand was published, that file displays and can be downloaded.

If the brand selected was a named brand, the **Delete Brand** page (**Home > System > Branding > Delete Brand**) offers the option to delete that brand. If the brand selected was the system brand, the **Delete Brand** page offers the **Restore to the factory default system brand** option. Clicking **Delete** causes your current system brand to be reverted to the factory system brand.

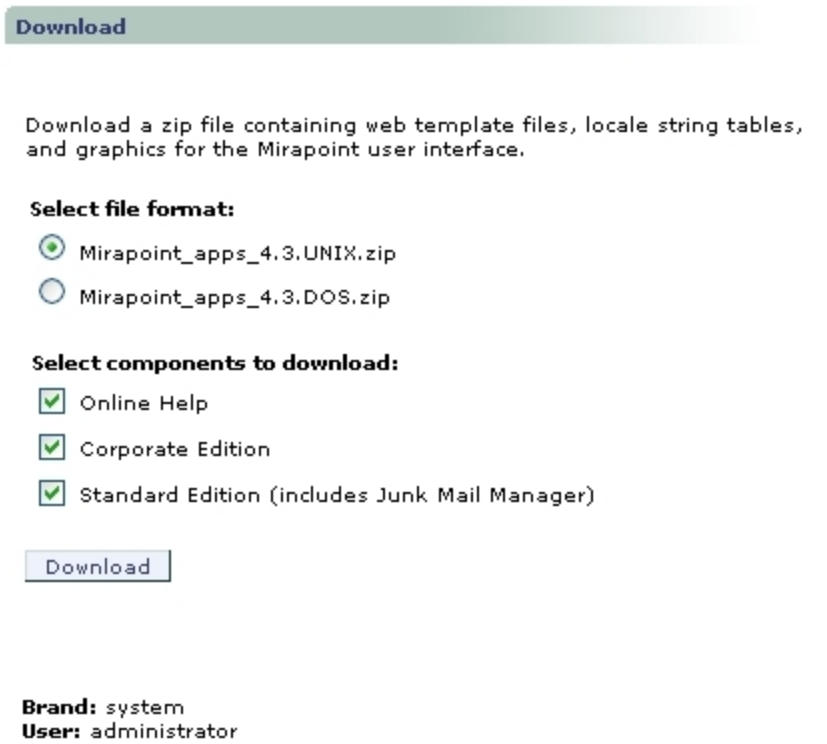
Downloading a Brand

Use the **Download** page (**Home > System > Branding > Download**) to download the system brand zip file or named brand zip files that you have previously published. Before you can customize the web pages for your appliance, you must download the factory system brand template files.

To download a brand:

1. Go to **Home > System > Branding > Download**.

   The **Download** page displays. If you selected a named brand on the **Select Brand** page (**Home > System > Branding > Select Brand**), the **Download** page provides only that brand's zip file for you to download.



2. Within the **Select file format** area, select the appropriate radio button from the list of template system brand zip files.

   If you have previously published a custom system brand, that zip file is also available as a selection.

3. Within the **Select the components to download** area, select only the components that you want to brand in order to reduce download and publish time. You can choose from the following components:

   - **Online Help** - These are the files for Corporate Edition and Standard Edition online help. These files are fully brandable.
   - **Corporate Edition** - These are the files for WebMail Corporate Edition. These files are quick brandable only (style sheets and Login page).
   - **Standard Edition (Includes Junk Mail Manager)** - These are the files for WebMail Direct Standard Edition and Junk Mail Manager. These files are fully brandable.

   For more information on branding and localization, see Process Overview on page 304.

4. Click **Download**.

   A file download dialog box displays.

5. Click **Save** (or **OK** depending on your web browser) and navigate to a directory of your choice where you want to save the file. If you are going to create a named brand, you might want to create a directory for the named brand at this time.

Deleting a Brand

Use the **Delete Brand** page (**Home > System > Branding > Delete Brand**) to remove a named brand from your appliance. Additionally, you use this page to restore (or revert) your current system brand to the factory system brand that came with your appliance. If you did not make any changes to your system brand, you might not need to take this step. Use the **Assign Brand** page (**Home > System > Branding > Assign Brand**) to restore a domain to your current system brand. For more information, see Assigning a Brand on page 314.

In order to delete a brand or to restore the factory brand, you must first select the appropriate brand. For information on, see Selecting a Brand on page 310. If you go to the **Delete Brand** page without selecting a brand first, a warning message, `No brand has been selected`, will appear.

This section contains the following information:

- Deleting a Named Brand below
- Restoring the Factory Default System Brand on the facing page

Deleting a Named Brand

If a brand has domains assigned to it, you must assign those domains to a different named brand, or the system brand, before attempting to delete the brand. If you attempt to delete a brand that has domains assigned to it, you get a warning message, `This brand has assigned domains`. To disassociate a domain with a brand, use the **Assign Brand** page. For more information, see Assigning a Brand on page 314.

To delete a named brand:

1. Go to **Home > System > Branding > Select Brand**.

   The **Select Brand** page appears.

2. Click on a brand in the **Named brands** text box.
3. Click **Select Brand**.

   The brand you selected is indicated in the lower-left corner of the page and is available for modification from in the other branding-related administration pages.

4. Click **Delete Brand**.

   The **Delete Brand** page appears with a message at the top indicating the selected named brand.

5. Click **Delete**.

If the brand does not have domains assigned to it, it is deleted. If the brand has domains assigned to it, a warning message displays, `This brand has assigned domains`. In order to delete the brand in this case, you must disassociate all domains with it (see Assigning a Brand on next page), and then repeat this procedure.

During the deletion process, the appliance is locked for one minute while it updates internal settings. The lock time should not be longer than one minute.

Restoring the Factory Default System Brand

To restore the factory default system brand:

1. Go to **Home > System > Branding > Select Brand**.

   The **Select Brand** page appears.

2. Under **System Brand**, click **Select**.

The system brand you selected is indicated in the lower left corner of the page and is available for modification from in the other branding-related administration pages.

3. Click **Delete Brand**.

   The **Delete Brand** page appears with a message at the top, `Restore to the factory default system brand`.

4. Click **Delete**.

Your custom system brand is reverted to the factory system brand. All domains assigned to the system brand now have the factory default system brand restored to their interfaces.

If for some reason you cannot log in to your appliance using the Administration Suite, complete the following steps:

1. Log in to the command-line interface (CLI) using the administrator username and password.
2. Type in the following command to revert to the factory settings:

   ```
   Brand Delete system
   ```

   The `system` brand is returned to its default factory state.

Sometimes you need to stop and restart the WebMail and WebCal (i.e., Calendar) services in order for the publishing process to complete.

Assigning a Brand

Use the **Assign Brand** page (**Home > System > Branding > Select Brand**) to assign domains to named brands and remove domains from brands.

To assign a brand:

You must upload the named brand and select it before you can assign domains to it. For more information,

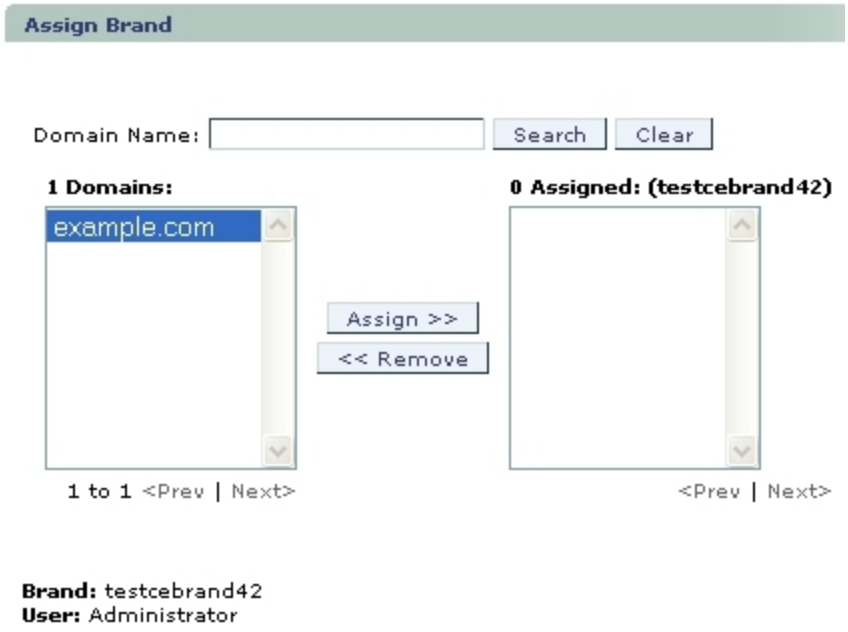
see Selecting a Brand on page 310. If you want to assign a brand to a delegated domain, make sure you have properly configured those domains. For more information, see the *Mirapoint Message Server Administrator's Guide*. If you go to the **Assign Brand** page without selecting a named brand or creating your domains, the **Assign Brand** page options do not display.

1. Go to **Home > System > Branding > Select Brand**.

   The **Select Brand** page appears.

2. Select a brand from the **Named brands** text box.
3. Click **Select Brand**.
4. Click **Assign Brand**.

   The **Assign Brand** page appears.



5. To find a domain, in the **Domain Name** text field, type in a domain name and click **Search**. You can use the asterisk (*) wildcard, but you must include the suffix (for example, .com, .net, .org, and so on). Clearing the text field and clicking **Search** causes all of the available domains to display in the **Domain** text box.
6. Highlight the domains in the **Domain** text box that you want assigned to the selected brand.
7. Click **Assign**.

Those domains appear in the **Assigned** text box. On your next log in to that domain, you will see the selected named brand.

To remove an assigned brand:

1. Go to **Home > System > Branding > Select Brand**.

   The **Select Brand** page appears.

2. Select a brand from the **Named brands** text box.
3. Click **Select Brand**.
4. Click **Assign Brand**.

   The **Assign Brand** page appears.

5. Highlight the domains in the **Assigned** text box that you want removed from the selected brand.
6. Click **Remove**.

Those domains are removed from the **Assigned** text box and re-appear in the **Domains** text box. If you log out and log back in to the Administration Suite, those domains will use the current system brand.

Customizing the Over-Quota Message

Use the **Over-Quota Message** page (**Home > System > Branding > Over-Quota Message**) to customize the warning message that is delivered when a user's folder has gone over its allocated size limit. You can also select the character set used to encode the message. For example, if you select **Japanese (ISO-2022-JP)**, Japanese characters are used in the message.

To customize a brand's over-quota message:

1. Go to **Home > System > Branding > Select Brand**.

   The **Select Brand** page appears.

2. Select a brand from the **Named brands** text box.
3. Click **Select Brand**.
4. Click **Over-Quota Message**.

   The **Over-Quota Message** page displays with the selected named brand indicated in the lower-left corner.

5. Customize the text in the **From**, **Subject**, and **Message** text fields as desired. You can also select a **Message Charset** (character set) for the message from the drop-down menu. The default is **Unicode (UTF-8)**.
6. Click **Set Message**.

The message you entered, along with the character set you specified (if any), is sent to users when their quota is exceeded. To revert to the brand's default over-quota message, click **Default Message**. The brand's default (factory brand) over-quota message, with your specified character set, is sent to users when their quota is reached.

The over-quota message you customize here is associated with the brand that you selected on the **Select Brand** page.

Branding and Localization Tasks and Tips

One of the most important issues when branding and publishing files for your appliance is that of file structure. It is essential that the original file structure be preserved. If you change the file structure, other than creating a new directory at the recommended level in the hierarchy for alternate set publishing, issues will occur. Follow the recommended guidelines when modifying the branding files, as discussed in Localization Guidelines on the facing page and Process Overview on page 304. If you deviate from these guidelines, your published files might not work. For more information on the branding and localization file structure, see the *Mirapoint Branding Guide*. If you run into a serious issue while branding, you can always restore the original factory system brand. For information on how to do this, see Restoring the Factory Default System Brand on page 313.

Preserving Your Brand - Appliance Upgrades and Patches

Messaging Operating System (MOS) upgrades and patches can be installed with the brands on your appliance remaining intact. You can also upgrade or patch an appliance and then choose to apply an older branded zip file from an earlier release. When you decide to preserve a previous brand, or apply an older brand zip file, the following circumstances apply:

- New features that are available through the web pages will not be available.
- Some bug fixes included in this patch may not be in effect.
- To access all the new features and bug fixes available in this release, you will have to re-brand your appliance.

Brand preservation is assured as a necessary requirement for a release, however additional steps may be needed. For more information about updating brands, see the *Mirapoint Branding Guide*. For important information about updates and patches, see the *Mirapoint System Software Release Notes* for your MOS version.

Application Entry Points

WebMail/WebCal Direct Standard Edition, WebMail/WebCal Corporate Edition, Junk Mail Manager (JMM), and the Administration Suites have their own default entry points (i.e., shortcut URLs). These URLs can be useful when testing your brand. You can go directly to the application using the following entry points:

- WebMail Direct Standard Edition: `http://hostname/wm`
- WebCal Direct Standard Edition (i.e., Calendar): `http://hostname/mc`
- WebMail/WebCal Corporate Edition: `http://hostname/em`
- Junk Mail Manager: `http://hostname/spam`
- Administration Suite (pre-release 3.4): `http://hostname/acctadmin` (when users without administration privileges access this login, they can only manage their accounts)
- Administration Suite (post-release 3.4, auto-detects licenses): `http://hostname/miradmin`

You can also change the default application that is displayed when you log in to the appliance. For more information, see Managing the Administration Service on page 30.

Localizing Address Book - WebMail vs. Calendar

Address Book for WebMail Direct Standard Edition is slightly different than Address Book for WebCal Direct Standard Edition (i.e., Calendar). Variables are used to change elements when Address Book is accessed by WebMail or by Calendar.

In order to support the ability to specify the character set of a file used to import data into address book, the vartab file `addrbook/locale/localename/csvheaders.var` provides the field name definitions for CSV files produced by Outlook. A record in this file is composed of up to six parameters, describing Outlook CSV fields for a given language.

The default `csvheaders.var` comes with some languages (i.e., English, French, Italian, Spanish, Portuguese, Chinese, Taiwanese, Korean, German). A disabled entry, `english_short`, lists the fields that are supported by Address Book. You can add your own language, and control which languages are enabled.

For example, in WebMail Direct Standard Edition Address Book's **Import/Export** page, there is a **Language** and a **Charset** drop-down menu. When you access the **Import/Export** page, the language that is selected by default is **English**. This is because the factory brand `csvheaders.var` file contains this line: `english_default="true"` (and for all the other languages: `japanese_default="false"`, `french_default="false"`, etc.). If you want your language to be the default selection, brand the `csvheaders.var` file, set `english_default="false"`, then for the desired language set *language*`_default="true"`. For more information about branding address book, see the *Mirapoint Branding Guide*.

Localization Guidelines

The following list addresses rules that are important to follow when translating the brandable files.

- Always preserve the original line formatting of the files.
  - Do not delete end-of-line characters to consolidate consecutive lines.
  - Do not rearrange or delete key/value pairs from the vartab files (for example, `locale.var` and `cell.var` files). This facilitates textual differences.
- Never use ISO-Latin-1 in the brandable files.
  - Only use UTF-8 (or HTML entities where applicable).
- Fix any syntax errors you introduce into the vartab files (for example, `locale.var` and `cell.var` files).
  - Your system will reveal any syntax errors when you try to publish the files. You will not be allowed to successfully publish the files that contain syntax errors.
- Use caution when translating INPUT tags in an HTML form.
  - When localizing HTML form buttons, the only portion that can be translated is the `'value=translate_here'` portion. All other INPUT tags should not be translated in order to avoid functional breakage.
- Always preserve the instances of `$(variable)` semantics in the brandable files.

- Never modify the `$(variable)` text that appear in the HTML templates and `cell.var` files; but you can modify the value in the key/value pair associated with any `$(variable)`.

Installing a User Interface Localization

Several non-English language localizations are available for the various Mirapoint web user interfaces (i.e., WebMail Direct Standard Edition, WebCal Direct, and the Administration Suites). These are published on the Mirapoint Technical Support website as localization patches (L-Patches). For more information, see Managing Branding and Localization on page 303 and the *Mirapoint Patch Release Notes*.

To specify a particular localization as the default localization for Mirapoint user interfaces, you can use the `Locale Set Default` command within the command-line interface (CLI).

Additional information about user interface localizations is provided in the following sections:

- Localizing Junk Mail Manager Messages below
- Displaying Available Localizations on Login Pages below

Localizing Junk Mail Manager Messages

You must use the CLI to localize Junk Mail Manager (JMM) welcome and summary messages.

To set the JMM message locale:

1. Log in to the CLI as an administrator.
2. Type in the following commands, respectively:

   `Message Set` *`locale`* `MESSAGE.JUNKMAIL.WELCOME`

   `Message Set` *`locale`* `MESSAGE.JUNKMAIL.SUMMARY`

   Replace *`locale`* with the locale name that you want to set. For example, to use the French locale:

   ```
   Message Set fr_FR.8859-1 MESSAGE.JUNKMAIL.WELCOME
   ```

   To see what the current text is for each message, use the `Message Get` command.

For more information, type `Help Message Set` in the CLI.

Displaying Available Localizations on Login Pages

When one or more localizations are installed on an appliance, you can use the `Locale Set Loginfooter On` command to display a list of available localizations on the login page of the Mirapoint web user interfaces. Users can individually choose the locale they want to use from that list.

Index

A
Access Control List 54
Alerts 84, 217, 219, 274
  alerts table 220
  system information report 274
Allowed Mailing Lists 141, 148, 161
Allowed Senders 93, 126, 132, 136, 139, 141, 148, 161, 180, 239, 266, 273
Antispam 13, 17, 24, 45, 83, 91, 125-126, 134, 136, 138, 141, 144-146, 148, 156-157, 163, 172, 174, 224, 239, 248, 266, 270, 281, 286, 301
  allowed mailing lists 141, 148, 161
  allowed senders 132, 139, 141
  blocked senders 45, 136
  junk mail 13, 21, 24, 59, 73, 125, 128, 141, 148, 155, 157, 163, 172, 180, 225, 234, 239, 260, 270, 278, 286, 288, 296, 302, 318
  Junk Mail Filter 126, 136, 141, 159
  Junk Mail Manager 155
    quarantine 159
  MultiScan 128
  Principal Edition 128, 135, 239
  RBL host list 91, 239
  reject list 145, 265
  relay list 46, 132, 144, 153
  Signature Edition 135, 239, 252
Antivirus 14, 55, 83, 93, 105, 108, 114, 120, 124, 174, 225, 241, 249, 266, 270, 281, 301
  common virus attachments 176
  configuring 109, 114, 120
  content filtering 15
  F-Secure 105, 108, 114, 122
  RAPID 55, 105, 120, 124, 241
  Sophos 21, 105, 108, 114, 120, 226, 253, 271
  updating 105
B
Blocked Senders 45, 91, 126, 133, 136, 138, 152, 161, 239
Branding
  default entry points 318
  over-quota message 167
C
Calendar
  delegated domains 34
Content Filters 172
  advanced filters
    common virus attachments 176
    destination domain 174
    MIME and filtering attachments 175
  blocked attachments 199
  blocked messages 197
  corporate word list 204
  Junk Mail Manager quarantine 159
  objectionable word list 206
  redirected attachments 202
  send to quarantine folder 15
  wire taps 193
    example entries 194
D
Delegated Domains 94
  calendar 34
  mail signature 68
Distribution Lists
  reserved DL names 64
Domain Name Server 9, 14, 23-24, 29, 45, 90, 103, 126, 144, 146, 153, 226, 279, 290
Domains
  delegated domains 94
  destination domain 137, 139, 142, 168, 173, 193, 195, 197, 199, 202, 204, 206
H
Halt/Reboot 88
Host ID 9, 81
I
Import/Export
  configuration data 87
J
Junk Mail Manager 12, 14, 48, 59, 69, 90, 126, 132, 136, 139, 141, 155, 157, 161, 169, 171, 174, 297, 318, 320
  configuration 157
    routing options 156
  enabling provisioning 169
  junk mail domain
    adding 162
    allowed mailing lists 168
    allowed senders 168
    blocked senders 168
    local vs. remote 156
    message filters 168
  junk mail user accounts 163
    bulk creating 169
    finding 164
  order of filters and lists 156
  over-quota message 167
  quarantine filter action 159
  summary message 171
  troubleshooting 159

welcome message 166
L
LDAP 13, 30, 39, 45, 55, 61, 65, 69, 93, 102, 127, 155, 157, 165, 169, 227, 286, 290, 292, 297
enabling provisioning for Junk Mail Manager 169
Junk Mail Manager 159
LDAP enabled 297
routing with Mirapoint schema 19
routing with non-Mirapoint schema 19
M
MailHurdle 83, 90, 92, 126, 134, 137, 140-141, 148, 155, 248, 270, 286
advanced options 151
allowed hosts 151
checking triplets 153
configuring 149
deploying 148
flushing triplets 154
SMTP authentication 150
Message Queue 234
queue summary 242
searching 244
sorting 236
Monitoring
storage information 211
system and data storage 211
N
Network Settings
interface 24, 226
NTP server 290
time 16, 28
P
Password
changing 15, 80
Performance Graphs 277, 281, 283-284, 286, 288-289, 291, 293, 295
cpu 295
disk 291
external 289
junk mail 284
mail 281
misc 288
network 293
POP/IMAP 283
WebMail 284
Q
Quarantine Administrator 15, 54, 106, 120, 124, 182, 196, 198, 200, 203, 205, 207, 241
R
RBL Host List 91, 239
Reject List 145, 265
Relay List 46, 132, 144, 153
Reports 58, 84, 96, 130, 148, 219, 246, 260, 266, 270, 274-277
admin audit trail 246, 277
commands 275
folders 275
folder size and quota 275
logins 266
detailed logins 268
failed logins by remote IP 270
failed logins by user 269
login summary 267
login traffic rates 268
top logins by user 267
mail 260
detailed mail logs 61, 264
local mail traffic 261
top mail users 260
traffic summary 263
security 270
antispam 271
antivirus 270
content filtering 272
MailHurdle 272
system 274
user audit trail 276
Routing 14, 69, 227
domain to mail host mapping 20, 69
LDAP mail group queries 14, 69
LDAP server with Mirapoint schema 19
LDAP server with non-Mirapoint schema 19
LDAP user queries 14, 69
local message router 19
local routing table 19
mail domains 70
Microsoft Active Directory 19
S
Security 90
certificates 97
SSL 101
trusted admins 103
Selective Restore
SAN storage device 255
Services 30
administration 30
calendar (WebCal) 33
HTTP 35
LDAP 34
SMTP 43
Setup Wizard 13, 23, 55, 69, 81, 125, 157
Signature 68
U
UCE Score 125, 130-131, 145-146, 160, 180, 239, 265, 286
User Accounts 18, 23-24, 54, 62, 161, 169, 222, 255, 302
junk mail user accounts 163
bulk creating 169

Utilities 13, 22, 81, 83
appliance updates 85
licenses 2, 9, 14, 81, 324
service reporting 21, 81, 83

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 preinstalled 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.