



MX Control Console

Administrative User Manual

This Software and Related Documentation are proprietary to MX Logic, Inc.

© Copyright 2003 **MX Logic, Inc.**

The information contained in this document is subject to change without notice and should not be construed as a commitment by MX Logic. MX Logic assumes no responsibility for any errors or omissions that may appear in this document.

MX Logic, Inc.

9780 Mount Pyramid Court, Suite 350

Denver, CO 80112

This issue: June 2003

Contents

1 Introduction and Login

1.1	About MX Control Console	2
1.2	About This Manual	3
1.3	MX Control Console Functionality	4
	<i>Domain Selection</i>	4
	<i>Menu Bars</i>	5
	<i>Graphics Display Options (Display Tabs)</i>	5
1.4	Logging into the MX Control Console	7

2 Overview Tab

2.1	Viewing Overview Information	9
-----	------------------------------------	---

3 Quarantine Tab

3.1	Introduction – Quarantine Tab Functionality	12
3.2	Viewing & Managing VIRUS Quarantined Messages	14
3.3	Viewing & Managing SPAM (Junk Email) Quarantined Messages	16
3.4	Viewing & Managing ATTACHMENT Quarantined Messages	18
3.5	Viewing & Managing CONTENT Quarantined Messages	20
3.6	Searching for Quarantined Messages by User (Recipient)	22

4 Policies Tab

4.1	Introduction – Policies Tab Functionality	25
4.2	Maintaining Allow/Deny Lists	27
4.3	Maintaining the Exempt Users List	30
4.4	Maintaining Anti-Spam Policies	31
4.5	Maintaining Anti-Virus Policies	33
4.6	Maintaining Attachment Policies	35
4.7	Maintaining Content Policies	39
4.8	Maintaining HTML Shield Policies	41

5 Setup Tab

5.1	Setting up Inbound Servers	44
5.2	Enabling/Disabling Spam Reporting.....	46
5.3	Changing Your Password.....	48

6 Users Tab

6.1	Searching for Users & Viewing User Details.....	50
6.2	Changing User Roles & Settings.....	53
6.3	Accessing Quarantined Messages for a User	55

7 Reporting Tab

7.1	Introduction – Reporting Tab Functionality.....	58
7.2	Viewing Traffic Overview	60
7.3	Viewing the Threats Overview.....	61
7.4	Viewing a Spam Threats Report.....	62
7.5	Viewing a Virus Threats Report.....	63
7.6	Viewing a Content Threats Report.....	65
7.7	Viewing an Attachment Threats Report.....	66
7.8	Viewing a User Activity Report.....	67
7.9	Viewing an Event Log Report.....	68
7.10	Viewing an Audit Trail Report.....	70

FAQs	71
-------------	-----------

Glossary	74
-----------------	-----------

1 INTRODUCTION & LOGIN

1.1	About MX Control Console	2
1.2	About This Manual	3
1.3	MX Control Console Functionality	4
1.4	Logging into the MX Control Console	7

1.1 About MX Control Console

Welcome to MX Logic's web-based administrative portal: MX Control Console. With its easy-to-use, intuitive interface, the Console allows you to quickly configure and change MX Logic Email Defense Service's email filtering policies for your domain(s). These filtering policies include:

- Allow/Deny policies
- Exempt Users policies (creating a list of exempt users)
- Anti-Spam policies
- Anti-Virus policies
- Attachment control policies
- Content keyword policies
- HTML shield policies

In addition to configuring filtering policies, MX Control Console allows you to:

- Review and manage quarantined messages
- Administer setup configurations (including inbound servers and spam reporting) and change your password
- Managing users within your domain(s)
- Monitor the threats for all of your domains
- Obtain message traffic reports and statistics
- View user activity
- Audit MX Control Console usage and system changes

1.2 About This Manual

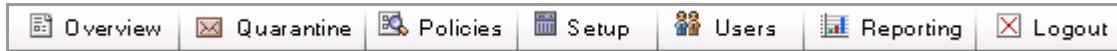
This manual provides step-by-step instructions for performing tasks necessary to maintain your domain's MX Logic Email Defense Service. It is intended for an MX Logic Email Defense Service system administrator proficient in general company operating procedures. You need not have an in-depth knowledge of computer systems to use MX Control Console; however, you should be familiar with the Windows environment. If you require more detailed and technical information on how MX Logic Email Defense Service operates and how changes to the Console settings can affect your environment, see the *MX Logic Email Defense Service Operations Manual*.

This manual groups together tasks and functions by the MX Control Console tab from which you perform each task:

- **Overview Tab** – Contains a snapshot of message traffic and general information over the past 24 hours
- **Quarantine Tab** – Enables you to view and manage quarantined messages
- **Policies Tab** – Enables you to configure all filtering policies
- **Setup Tab** – Enables you to configure MX Logic Email Defense Services to filter your domain(s)
- **Users Tab** – Enables you to view user details and change user roles and settings
- **Reporting Tab** – Enables you to generate message traffic and threat reports

1.3 MX Control Console Functionality

When you first enter the MX Logic Control Console, the *tab bar* displays along the top of the window.



- Overview
The **Overview** screen presents a snapshot of traffic to your domain and other information from MX Logic. This is the first page you see when you log in.
- Quarantine
The **Quarantine** screen allows you to review and take action on any messages quarantined because they contain viruses, unwanted content, attachments, or HTML, or because they are junk email (“spam”). Messages are quarantined only if you configure your filtering policies to take this action.
- Policies
The **Policies** screen allows you to configure and modify policies that will instruct MX Logic Email Defense Service how to handle viruses, spam, unwanted attachments, unwanted content, and unwanted HTML in messages intended for recipients on your network. You can also create customized “Allow” and “Deny” lists (regarding message senders) as well as an Exempt Users list (regarding users/recipients) for your domain.
- Setup
The **Setup** screen enables you to configure MX Logic Email Defense Service to deliver inbound SMTP traffic to your domain properly and to enable/disable Spam Reporting. You can also change your password from this screen.
- Users
The **Users** screen enables you to manage users within your domain, including reviewing user details and changing user passwords, roles, and Spam Report frequency.
- Reporting
The **Reporting** screen enables you to generate message traffic reports for threats (virus, spam, etc.) intended for your network. You can generate reports and statistics for threat activity for a given domain and time period (one day, one full week, or an entire month). You can also view (audit) MX Control Console usage and policy changes.
- Logout
The **Logout** tab/button allows you to exit the MX Control Console.

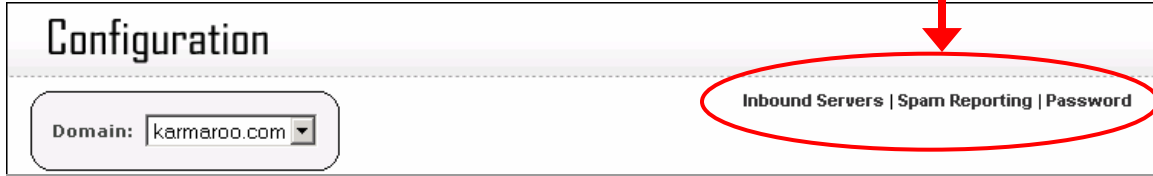
Domain Selection

You can only configure or modify one domain at a time. If you manage multiple domains, always be sure you have the correct domain selected from the **Domain** drop-down list:



Menu Bars

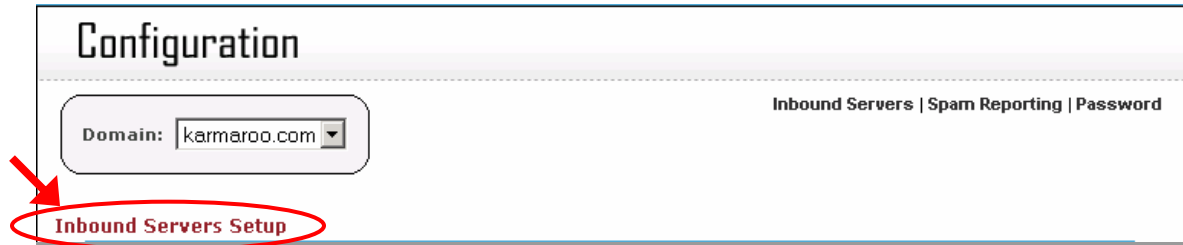
The menu bars that display for each tab-screen enable you to navigate through all the functions available for that tab.



If the default screen contains all the possible functions for a tab, then no additional navigation is necessary; therefore, no menu bar displays (*e.g.*, the Policies tab-screen).





When a menu bar displays, the default screen is the left-most menu item listed.

Note: The menu items do not change appearance, no matter which menu-screen you select. The page is noted simply by the page title that appears beneath the Domain.

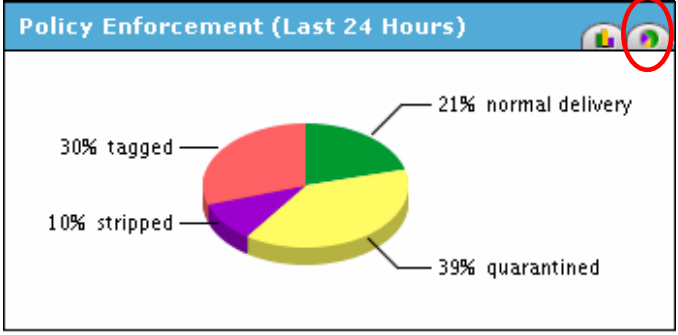
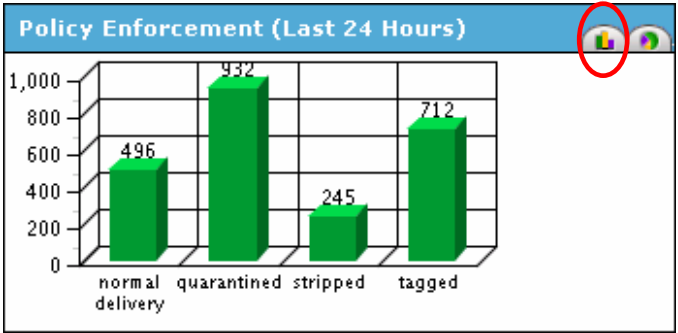
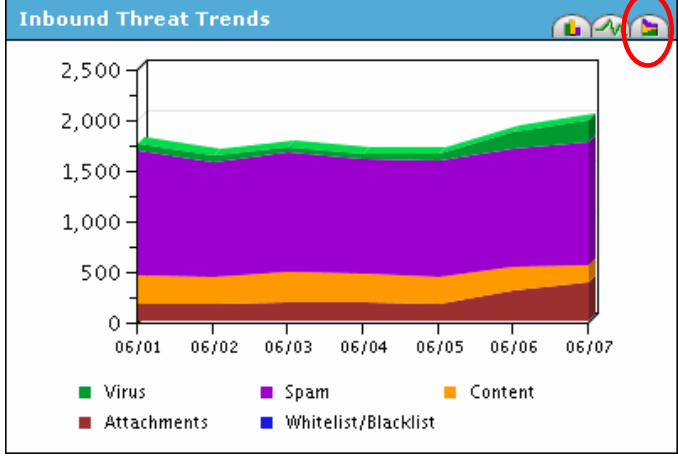
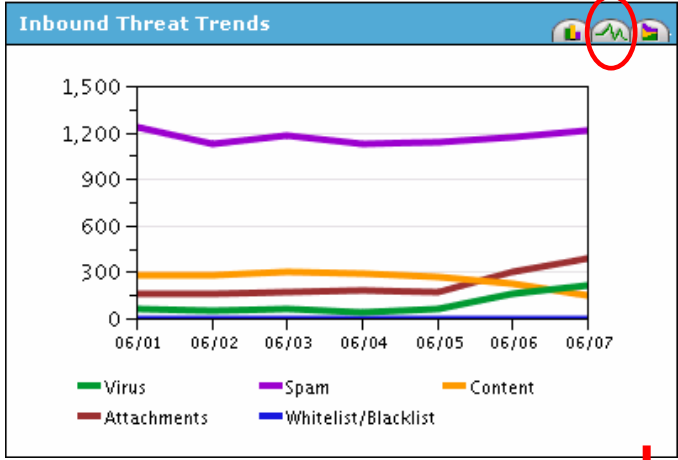
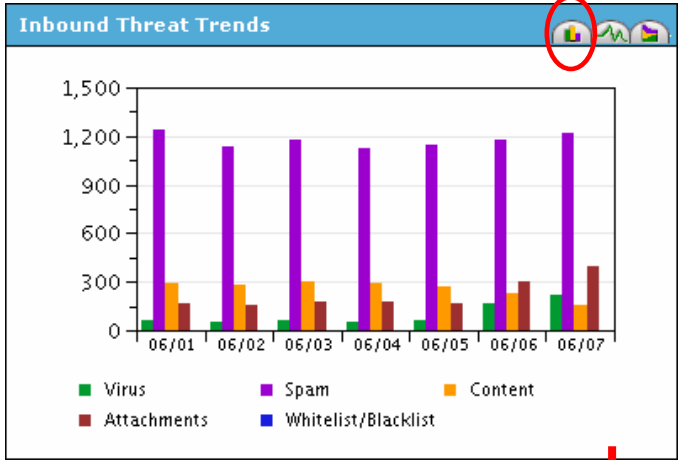


Graphics Display Options (Display Tabs)

When graphics are displayed in the MX Control Console, they often have display tabs on the right side of the title bar. These enable you to change the display style of that specific graphic. The options you will see are as follows:

-  This tab displays the graphic as a bar graph.
-  This tab displays the graphic as a line graph.
-  This tab displays the graphic as a solid (filled) line graph [*default*].
-  This tab displays the graphic as a pie chart [*default*].

The following are samples:

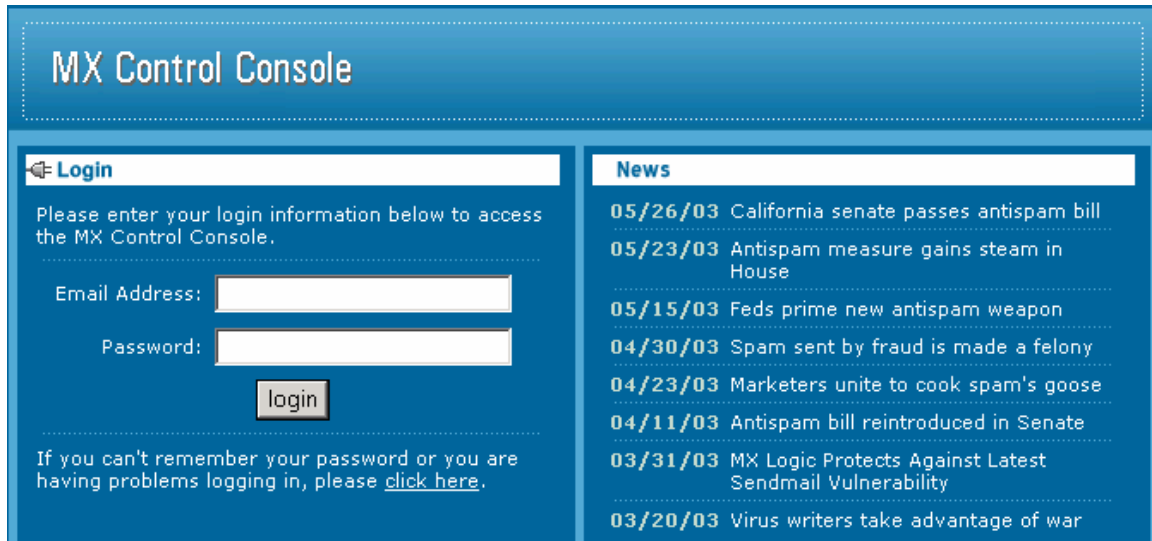


1.4 Logging into the MX Control Console

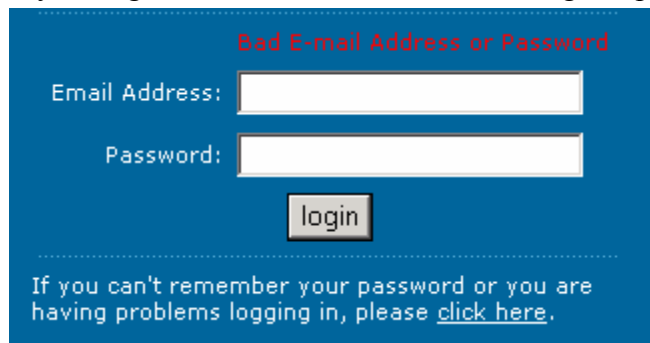
You can access the MX Control Console from any computer, using any Web browser, as follows:

1. From your Web browser, enter the following URL in the **Address** field:
<http://portal.mxlogic.com>

The MX Control Console login screen displays.



2. Enter your login information.
 - **Email Address**
 - **Password** (provided to you during the provisioning process)
3. Click the **login** button.
 - If your login is successful, MX Control Console will open, displaying the *Overview* page. (For details, see section 2.1 Viewing Overview Information, page 9.)
 - If your login is unsuccessful, an error message displays in red font on the login screen:



Try entering your information again, or to have information sent to you, click the **click here** text link and enter your email address.

2 OVERVIEW TAB

2.1 Viewing Overview Information _____ 9

2.1 Viewing Overview Information

From the Overview tab-screen, you can view high-level information on the traffic to your domain over the last 24 hours, as well as news and updates from MX Logic. When you log into the MX Control Console, this screen displays by default.

After you are logged into MX Control Console, you can access this tab-screen by clicking the Overview tab (Overview) on the tab bar.

Overview

24 Hour Snap Shot

Inbound Messages: 2240	Inbound Bandwidth: 2MB	Viruses: 188
Avg Inbound Size: 1.16KB		Spam: 1144
		Quarantined: 966

Quarantine Levels (6306 total)

Spam	4070
Viruses	1079
Attachments	
Content	1157

Traffic (Last 24 hours)

■ Inbound

Policy Enforcement (Last 24 Hours)

0% tagged	19% normal delivery
22% stripped	59% quarantined

What's New

03/04/03 *New feature:* [User Management](#) enables you to more easily manage your end users' spam quarantine, Spam Summary Reports, and password. Click [here](#) for the official announcement.

01/17/03 *New feature:* [HTML Shield](#) safeguards your employees from dangerous HTML tags and scripts. In addition, it can also detect spam beacons and web bugs.

11/26/02 *New feature:* Audit trail reporting provides a way to track what changes have been made to your policy configuration. You can view your latest audit report [here](#).

News Updates

[05/26/03](#) California senate passes antispam bill

[05/23/03](#) Antispam measure gains steam in House

[05/15/03](#) Feds prime new antispam weapon

[04/30/03](#) Spam sent by fraud is made a felony

[04/23/03](#) Marketers unite to cook spam's goose

[04/11/03](#) Antispam bill reintroduced in Senate

[03/31/03](#) MX Logic Protects Against Latest Sendmail Vulnerability

[03/20/03](#) Virus writers take advantage of war

This page contains the following information:

24-Hour Snap Shot This box shows a 24-hour snapshot of your domain's email traffic.

Quarantine Levels This box shows an overview of quarantined messages, by category.

Traffic This box shows a graph of traffic volume for the last 24 hours.
You can alter the style of this graph by selecting one of the three

graph-format tabs.

Policy Enforcement This box shows the percentage of messages stripped, blocked, tagged, quarantined, cleaned, and normally delivered over the past 24 hours, according to the policies you configured.

You can alter the style of this graph by selecting one of the two graph-format tabs.

What's New This box shows the latest information from MX Logic via links.

News Updates This box shows any updates on current email threats and other important email security news (links).

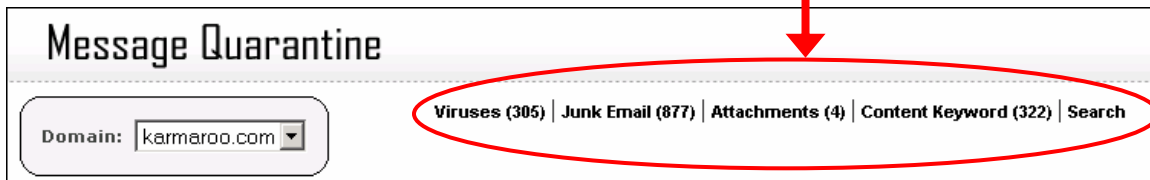
3 QUARANTINE TAB

3.1	Introduction – Quarantine Tab Functionality_____	12
3.2	Viewing & Managing VIRUS Quarantined Messages _____	14
3.3	Viewing & Managing SPAM (Junk Email) Quarantined Messages _____	16
3.4	Viewing & Managing ATTACHMENT Quarantined Messages _____	18
3.5	Viewing & Managing CONTENT Quarantined Messages _____	20
3.6	Searching for Quarantined Messages by User (Recipient)_____	22

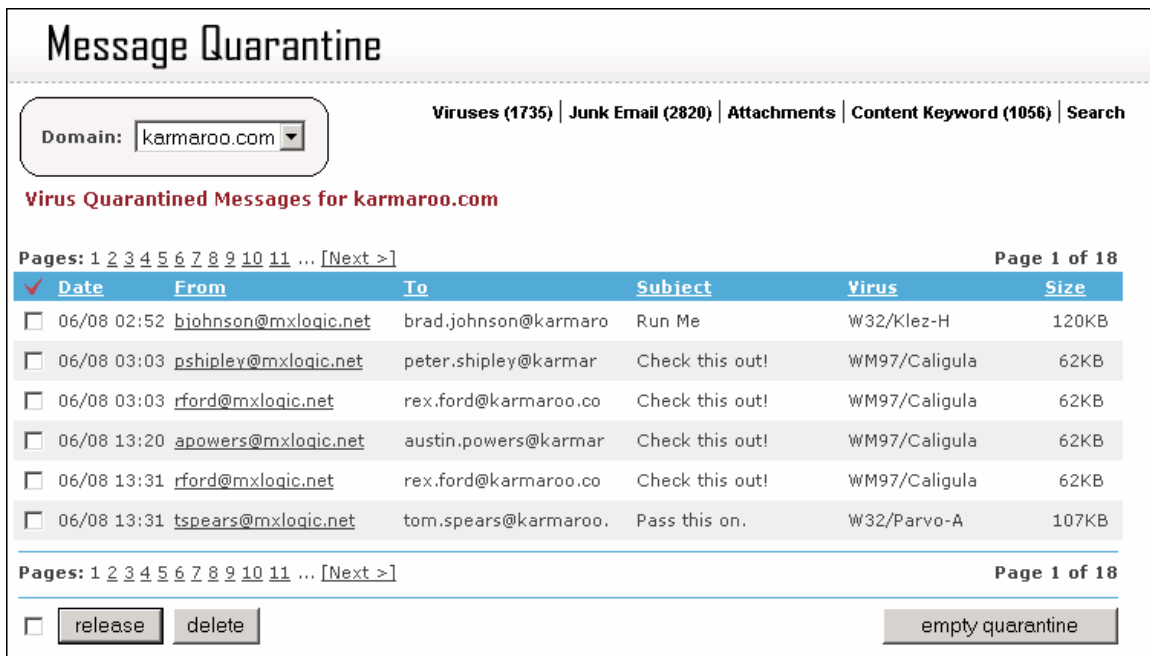
3.1 Introduction – Quarantine Tab Functionality

The Quarantine tab enables you to review and manage all quarantined messages

When you click the **Quarantine** tab (✉ Quarantine) on the tab menu, the menu bar displays the various screens you can access and includes the current total number of quarantined messages for each category in parenthesis:



By default, the first screen that displays is the Virus Quarantined Messages for the selected domain.



- You can change the domain displayed by selecting another value from the **Domain** drop-down list.
- You can sort the list by any of the headings by clicking the heading title. Clicking the heading again will sort the list in the opposite order.
- Each page lists up to 100 messages. You can view additional pages by either clicking the **Next >** or **< Prev** links or clicking on the specific page number link.
- For each quarantined message, you have the option to **delete** it completely, or to **release** it (sending it to the intended recipient).
- You can empty the entire contents (all pages) of certain quarantines by clicking the **empty quarantine** button, when available.

- You can view the actual message before release or deletion by clicking the linked email address in the **From** column.

A Safe Message View displays:

Message Quarantine

[Viruses \(1739\)](#) | [Junk Email \(2823\)](#) | [Attachments](#) | [Content Keyword \(1057\)](#) | [Search](#)

Safe Message View

From : apowers@mxlogic.net

To : austin.powers@karmaroo.com

Subject : Run Me

Date : Sun, 8 Jun 2003 11:41:01 -0600

Status : **Message quarantined by Virus module**

Attachments :

Filename	Size	Content Type	Scanned	Infections	Cleaned	Virus
(NONE)	113	text/plain	Yes	0	No	
demo.exe	89720	application/octet-stream	Yes	1	No	W32/Klez-H WORM_KLEZ.H W32/Klez.h@MM

This is a test message with a virus on it, we will then throw it through the virus scanner and see what happens

Message Action:

You can also release or delete a message from this detailed screen, using the **Message Action** buttons.

3.2 Viewing & Managing VIRUS Quarantined Messages

Those messages quarantined due to viruses are stored in Viruses Quarantine. Infected messages will appear on this screen only if you have selected “Quarantine the message” as one of your anti-virus policies. (To view or change virus policies, see section 4.5 Maintaining Anti-Virus Policies on page 33.)

This screen provides information on the date and time an infected message was delivered, the sender (**From**), the recipient (**To**), the subject of the message, the virus detected, and the message size.

When you click the **Quarantine** tab (Quarantine) on the tab menu, the Virus Quarantined Messages screen displays, by default.

You can also access this screen from any other Quarantine tab-screen by clicking **Viruses** on the menu bar.

Message Quarantine

Domain:

[Viruses \(294\)](#) | [Junk Email \(1246\)](#) | [Attachments](#) | [Content Keyword \(412\)](#) | [Search](#)

Virus Quarantined Messages for karmaroo.com

Pages: 1 2 3 [Next >]
Page 1 of 3

✓	Date	From	To	Subject	Virus	Size
<input type="checkbox"/>	05/29 23:53	apowers@mxlogic.net	austin.powers@karmar	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/30 00:48	bjohnson@mxlogic.net	brad.johnson@karmaro	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/30 01:19	pshiple@mxlogic.net	peter.shiple@karmar	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/30 01:32	tspears@mxlogic.net	tom.spears@karmaroo.	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/30 01:51	rford@mxlogic.net	rex.ford@karmaroo.co	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/31 19:06	apowers@mxlogic.net	austin.powers@karmar	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/31 20:50	apowers@mxlogic.net	austin.powers@karmar	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/31 20:50	pshiple@mxlogic.net	peter.shiple@karmar	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/31 20:51	pshiple@mxlogic.net	peter.shiple@karmar	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/31 21:38	tspears@mxlogic.net	tom.spears@karmaroo.	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/31 21:56	rford@mxlogic.net	rex.ford@karmaroo.co	Check this out!	WM97/Caligula	62KB
<input type="checkbox"/>	05/31 21:56	tspears@mxlogic.net	tom.spears@karmaroo.	Check this out!	WM97/Caligula	62KB

Pages: 1 2 3 [Next >]
Page 1 of 3

release
 delete

empty quarantine

1. To release or delete select messages, check (click) the corresponding checkboxes then either **release** or **delete** the selected messages using the buttons at the bottom of the page. (Clicking the checkbox again will deselect it.)
2. To release or delete all messages on the page displayed, click the single checkbox at the bottom of the page, and click either **release** or **delete**.
3. To empty the entire contents (all pages) of the quarantine, click the **empty quarantine** button.
4. To view the actual message, including virus details, before release or deletion, click the linked email address in the **From** column.

A Safe Message View displays:

Message Quarantine

[Viruses \(1739\)](#) | [Junk Email \(2823\)](#) | [Attachments](#) | [Content Keyword \(1057\)](#) | [Search](#)

Safe Message View

From : apowers@mxlogic.net

To : austin.powers@karmaroo.com

Subject : Run Me

Date : Sun, 8 Jun 2003 11:41:01 -0600

Status : Message quarantined by Virus module

Attachments :

Filename	Size	Content Type	Scanned	Infections	Cleaned	Virus
(NONE)	113	text/plain	Yes	0	No	
demo.exe	89720	application/octet-stream	Yes	1	No	W32/Klez-H WORM_KLEZ.H W32/Klez.h@MM

This is a test message with a virus on it, we will then throw it through the virus scanner and see what happens

Message Action:

You can also release or delete a message from this detailed screen, using the **Message Action** buttons.

3.3 Viewing & Managing SPAM (Junk Email) Quarantined Messages

Those messages quarantined due to spam are stored in Junk Email Quarantine. Messages with unwanted (or over-limit) attachments will appear on this screen only if you selected “Quarantine” as your Unwanted Attachment policy. (To view or change spam policies, see section 4.4 Maintaining Anti-Spam Policies on page 31.)

This screen provides information on the date and time the spam message(s) were delivered, the sender, the recipient, the subject of the message, the spam score (likelihood), and the size of the message.

1. From the Quarantine tab (Quarantine) menu bar, click the **Junk Email** text link.

Message Quarantine

Domain:

Viruses (294) | **Junk Email (1246)** | Attachments | Content Keyword (412) | Search

Junk Email Quarantined Messages for karmaroo.com

Pages: 1 2 3 4 5 6 7 8 9 10 11 ... [Next >]
Page 1 of 13

✓	Date	From	To	Subject	Spam Score	Size
<input type="checkbox"/>	06/01 22:27	pshiple@mxlogic.net	peter.shiple@karmar	Save up to 75% on In	High	3KB
<input type="checkbox"/>	06/01 22:27	bjohnson@mxlogic.net	brad.johnson@karmaro	Make YOUR Fortune on	High	5KB
<input type="checkbox"/>	06/01 22:27	apowers@mxlogic.net	austin.powers@karmar	Mortgage Quotes from	High	2KB
<input type="checkbox"/>	06/01 22:38	rford@mxlogic.net	rex.ford@karmaroo.co	Order Status for Cla	High	11KB
<input type="checkbox"/>	06/01 22:38	pshiple@mxlogic.net	peter.shiple@karmar	Quit Smoking Product	High	5KB
<input type="checkbox"/>	06/01 22:38	rford@mxlogic.net	rex.ford@karmaroo.co	You've Been Approved	High	5KB
<input type="checkbox"/>	06/01 22:49	apowers@mxlogic.net	austin.powers@karmar	Finally. Quality, A	High	11KB
<input type="checkbox"/>	06/02 02:51	pshiple@mxlogic.net	peter.shiple@karmar	Natural pain relief	High	7KB
<input type="checkbox"/>	06/02 02:51	pshiple@mxlogic.net	peter.shiple@karmar	Get a FREE Digital C	High	22KB
<input type="checkbox"/>	06/02 02:51	rford@mxlogic.net	rex.ford@karmaroo.co	New discovery ends s	High	5KB
<input type="checkbox"/>	06/02 03:02	bjohnson@mxlogic.net	brad.johnson@karmaro	Order Status for Cla	High	11KB
<input type="checkbox"/>	06/02 03:02	rford@mxlogic.net	rex.ford@karmaroo.co	Debt Free by 2003	High	5KB

Pages: 1 2 3 4 5 6 7 8 9 10 11 ... [Next >]
Page 1 of 13

release
delete

empty quarantine

2. To release or delete select messages, check (click) the corresponding checkboxes then either **release** or **delete** the selected messages using the buttons at the bottom of the page. (Clicking the checkbox again will deselect it.)

3. To release or delete all messages on the page displayed, click the single checkbox at the bottom of the page, and click either **release** or **delete**.
4. To empty the entire contents (all pages) of the quarantine, click the **empty quarantine** button.
5. To view the actual message, including spam details, before release or deletion, click the linked email address in the **From** column.

A Safe Message View displays:

Message Quarantine

[Viruses \(1103\)](#) | [Junk Email \(4147\)](#) | [Attachments](#) | [Content Keyword \(1171\)](#) | [Search](#)

Safe Message View

From : apowers@mxlogic.net

To : austin.powers@karmaroo.com

Subject : ** Your -approval-! **

Date : Sun, 1 Jun 2003 23:11:46 -0600

Status : **Message quarantined by Junk Email module (score High)**

Attachments :

Filename	Size	Content Type
(NONE)	508	text/html
(NONE)	0	

Times
 Your home refinance loan is approved!
 To get your approved amount go
 here.
 To be excluded from further notices go
 here.
 Times
 lgate
 7321duHJ3-271qDRt2989rpxT5-780Zsvz7045uMNG1-991DJjK3355QqeR3-157

Message Action:

You can also release or delete a message from this detailed screen, using the **Message Action** buttons.

3.4 Viewing & Managing ATTACHMENT Quarantined Messages

Those messages quarantined due to attachment type are stored in Attachments Quarantine. Messages with unwanted (or over-limit) attachments will appear on this screen only if you selected “Quarantine” as your Unwanted Attachment policy. (To view or change attachment policies, see section 4.6 Maintaining Attachment Policies on page 35.)

This screen provides information on the date and time the message(s) with unwanted attachments was delivered, the sender, the recipient, the subject of the message, the type of attachment that resulted in the message being quarantined, and the size of the attachment.

1. From the Quarantine tab (Quarantine) menu bar, click the **Attachments** text link.

Message Quarantine

Domain:

Viruses (305) | Junk Email (877) | **Attachments (4)** | Content Keyword (322) | Search

Attachment Quarantined Messages for karmaroo.com

	Date	From	To	Subject	Attachment Type	Size
<input type="checkbox"/>	06/18 11:01	bjohnson@mxlogic.net	brad.johnson@karmaroo	Managed Email Firewa	filter 'Managed Email Firewall Services.pdf'	444KB
<input type="checkbox"/>	06/18 11:12	bjohnson@mxlogic.net	brad.johnson@karmaroo	Managed Email Firewa	filter 'Managed Email Firewall Services.pdf'	444KB
<input type="checkbox"/>	06/18 11:12	bjohnson@mxlogic.net	brad.johnson@karmaroo	Managed Email Firewa	filter 'Managed Email Firewall Services.pdf'	444KB
<input type="checkbox"/>	06/18 11:12	tspears@mxlogic.net	tom.spears@karmaroo.	Managed Email Firewa	filter 'Managed Email Firewall Services.pdf'	444KB

release
delete

empty quarantine

2. To release or delete select messages, check (click) the corresponding checkboxes then either **release** or **delete** the selected messages using the buttons at the bottom of the page. (Clicking the checkbox again will deselect it.)
3. To release or delete all messages on the page displayed, click the single checkbox at the bottom of the page, and click either **release** or **delete**.
4. To empty the entire contents (all pages) of the quarantine, click the **empty quarantine** button.
5. To view the actual message, including attachment details, before release or deletion, click the linked email address in the **From** column.

A Safe Message View displays.

Message Quarantine

Viruses (305) | Junk Email (877) | Attachments (4) | Content Keyword (322) | Search

Safe Message View

From : bjohnson@mxlogic.net
To : brad.johnson@karmaroo.com
Subject : Managed Email Firewall Services
Date : Wed, 18 Jun 2003 11:01:15 -0600
Status : Message quarantined by Attachment Control module (filter 'Managed Email Firewall Services.pdf')

Attachments :

Filename	Size	Content Type
(NONE)	511	text/html
Managed Email Firewall Services.pdf	331493	application/pdf

Thank you for requesting MX Logic's white paper, "Managed Email Firewall Services." To learn more about MX Logic and our flagship service, MX Firewall, visit www.mxlogic.com.
 STOP SPAM, pornography and viruses from reaching your network.
 INCREASE CONTROL over email policy configuration and enforcement.
 DEPLOY QUICKLY with zero migration, zero integration and zero risk architecture.

Message Action:

You can also release or delete a message from this detailed screen, using the **Message Action** buttons.

3.5 Viewing & Managing CONTENT Quarantined Messages

Those messages quarantined due to content are stored in Content Keyword Quarantine. Messages with unwanted content will appear on this screen only if you selected “Quarantine” as one or more of your content policies. (To view or change content policies, see section 4.7 Maintaining Content Policies, on page 39.)

This screen provides information on the date and time the message with unwanted content was delivered, the sender, the recipient, the subject of the message, the keyword that resulted in the message being quarantined, and the size of the message.

1. From the Quarantine tab (Quarantine) menu bar, click the **Content Keyword** text link.

Message Quarantine

Domain:

[Viruses \(294\)](#) | [Junk Email \(1252\)](#) | [Attachments](#) | [Content Keyword \(413\)](#) | [Search](#)

Content Quarantined Messages for karmaroo.com

Pages: 1 2 3 4 5 [Next >] Page 1 of 5

	Date	From	To	Subject	Keyword	Size
<input type="checkbox"/>	06/01 09:29	rford@mxlogic.net	rex.ford@karmaroo.co	Increase your penis	'secret'	10KB
<input type="checkbox"/>	06/01 10:13	rford@mxlogic.net	rex.ford@karmaroo.co	Is your neighbor a c	'secret'	9KB
<input type="checkbox"/>	06/01 10:46	rford@mxlogic.net	rex.ford@karmaroo.co	Am I Crazy?? Or is t	'secret'	2KB
<input type="checkbox"/>	06/01 11:19	tspears@mxlogic.net	tom.spears@karmaroo.	Is your neighbor a c	'secret'	9KB
<input type="checkbox"/>	06/01 11:30	rford@mxlogic.net	rex.ford@karmaroo.co	YOUR OPINION COULD B	'confidential'	4KB
<input type="checkbox"/>	06/01 11:30	bjohnson@mxlogic.net	brad.johnson@karmaro	Let's Go Get Stoned	'proprietary'	11KB
<input type="checkbox"/>	06/01 11:30	bjohnson@mxlogic.net	brad.johnson@karmaro	Do your joints and b	'secret'	4KB
<input type="checkbox"/>	06/02 03:24	rford@mxlogic.net	rex.ford@karmaroo.co	Increase your penis	'secret'	10KB
<input type="checkbox"/>	06/02 03:35	bjohnson@mxlogic.net	brad.johnson@karmaro	Quit Smoking in 21 D	'proprietary'	1KB
<input type="checkbox"/>	06/02 03:46	apowers@mxlogic.net	austin.powers@karmar	Quit Smoking in 21 D	'proprietary'	1KB
<input type="checkbox"/>	06/02 03:46	rford@mxlogic.net	rex.ford@karmaroo.co	Sybil , Please Conf	'secret'	2KB
<input type="checkbox"/>	06/02 03:57	tspears@mxlogic.net	tom.spears@karmaroo.	Sybil , Please Conf	'secret'	2KB

Pages: 1 2 3 4 5 [Next >] Page 1 of 5

release delete

empty quarantine

2. To release or delete select messages, check (click) the corresponding checkboxes then either **release** or **delete** the selected messages using the buttons at the bottom of the page. (Clicking the checkbox again will deselect it.)

3. To release or delete all messages on the page displayed, click the single checkbox at the bottom of the page, and click either **release** or **delete**.
4. To empty the entire contents (all pages) of the quarantine, click the **empty quarantine** button.
5. To view the actual message before release or deletion, click the linked email address in the **From** column.

A Safe Message View displays:

Message Quarantine

[Viruses \(1126\)](#) | [Junk Email \(4215\)](#) | [Attachments](#) | [Content Keyword \(1186\)](#) | [Search](#)

Safe Message View

From : apowers@mxlogic.net
To : austin.powers@karmaroo.com
Subject : Quit Smoking in 21 Days Guaranteed!
Date : Sun, 1 Jun 2003 20:48:06 -0600
Status : Message quarantined by Content module (filter 'proprietary')

Attachments :	Filename	Size	Content Type
	(NONE)	1147	

Our powerhouse proprietary ALL HERBAL FORMULA is the very backbone of the FinalSmoke System. It completely removes your cravings to smoke and relieves the symptoms associated with nicotine withdrawal, so you can Finally kick the habit. In less than 30 days, you will be completely Smoke-Free, and on your way to healthy living.

Act Now and receive a FREE BONUS supply of our patented FAT BASHER, created to curb your appetite and the cravings that come when you quit smoking.

START YOUR SMOKE-FREE LIFE TODAY
 GUARANTEED!!!!!!

Message Action:

You can also release or delete a message from this detailed screen, using the **Message Action** buttons.

3.6 Searching for Quarantined Messages by User (Recipient)

You can search for quarantined messages for a particular recipient.

1. From the Quarantine tab (✉ Quarantine) menu bar, click the **Search** text-link.

The Search screen displays:

Message Quarantine

Domain:

[Viruses \(294\)](#) | [Junk Email \(1246\)](#) | [Attachments](#) | [Content Keyword \(412\)](#) | [Search](#)

Search Quarantined Messages for karmaroo.com

Recipient Email:
@karmaroo.com

2. Enter the recipient's exact email address, and click the **Search** button.

All results display on a single page:

Message Quarantine

Domain:

[Viruses \(1120\)](#) | [Junk Email \(4182\)](#) | [Attachments](#) | [Content Keyword \(1178\)](#) | [Search](#)

Search Quarantined Messages for karmaroo.com

Recipient Email:
@karmaroo.com

✓	Date	From	To	Subject	Type	Size
<input type="checkbox"/>	05/30 07:22	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/>	05/30 09:23	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/>	05/30 10:29	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/>	05/30 11:57	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/>	05/30 13:36	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/>	06/09 15:55	apowers@mxlogic.net	austin.powers@karmar	How's it going loser?	Content	430b
<input type="checkbox"/>	06/09 15:56	apowers@mxlogic.net	austin.powers@karmar	Earn Some Extra Cash	Spam	2KB
<input type="checkbox"/>	06/09 16:06	apowers@mxlogic.net	austin.powers@karmar	RE: You 200\$	Spam	1KB

3. To release or delete select messages, check (click) the corresponding checkboxes then either **release** or **delete** the selected messages using the buttons at the bottom of the page. (Clicking the checkbox again will deselect it.)
4. To release or delete all messages on the page displayed, click the single checkbox at the bottom of the page, and click either **release** or **delete**.
5. To view the actual message, including spam details, before release or deletion, click the linked email address in the **From** column.

A Safe Message View displays:

Message Quarantine

[Viruses \(1290\)](#) | [Junk Email \(4638\)](#) | [Attachments](#) | [Content Keyword \(1296\)](#) | [Search](#)

Safe Message View

From : apowers@mxlogic.net

To : austin.powers@karmaroo.com

Subject : ** You are -Approved-.

Date : Mon, 2 Jun 2003 09:39:40 -0600

Status : Message quarantined by Junk Email module (score High)

Attachments :

Filename	Size	Content Type
(NONE)	462	text/html

heart
 Your home refinance loan is approved!
 To get your approved amount go
 here.
 To be excluded from further notices go
 here.
 heart
 lgate
 3739w15


Message Action:

You can also release or delete a message from this detailed screen, using the **Message Action** buttons.

4 POLICIES TAB

4.1	Introduction – Policies Tab Functionality	25
4.2	Maintaining Allow/Deny Lists	27
4.3	Maintaining the Exempt Users List	30
4.4	Maintaining Anti-Spam Policies	31
4.5	Maintaining Anti-Virus Policies	33
4.6	Maintaining Attachment Policies	35
4.7	Maintaining Content Policies	39
4.8	Maintaining HTML Shield Policies	41

4.1 Introduction – Policies Tab Functionality

When you click the Policies tab ( Policies), the Policy Configuration screen displays a summary of the current inbound policies.

Policy Configuration

Domain:

Current Policies - Inbound

Policy Type	Conditions	Actions	
Allow/Deny	3 Allowed Sender(s)	Accept Message	[Modify]
Allow/Deny	6 Blocked Sender(s)	Deny Delivery	
Exempt Users	2 Exempt Recipient(s)	Accept Message	[Modify]
Anti-Spam	Medium likelihood of spam	Quarantine Message	[Modify]
Anti-Spam	High likelihood of spam	Deny Delivery	
Anti-Virus	Message contains a virus	Quarantine Message	[Modify]
Attachment	Attachment filename contains "federalaudit"	Quarantine Message	[Modify]
Attachment	Attachment filename ends with ".ozm"	Quarantine Message	
Attachment	Attachment filename is "ceospeech.wav"	Accept Message	
Content	Message contains word from 'Profanity'	Quarantine Message	[Modify]
Content	Message contains word from 'Racially Insensitive'	Quarantine Message	
Content	Message contains word from 'Sexual Overtones'	Quarantine Message	
HTML Shield	Medium - Strip malicious HTML and scripts	Strip	[Modify]
HTML Shield	Message contains image references	Replace	
HTML Shield	Message contains spam "beacons" / web bugs	Strip	

The summary screen shows all **Policy Types** available, their **Conditions**, the **Action** assigned for each condition, and the option to **Modify** each policy type.

The Policy Types are as follows:

- Allow/Deny** Allow List entries are not filtered for Junk (Anti-Spam) email, attachments, or content. (*Note: Virus scanning is never disabled.*)
- Deny List entries are refused and not delivered to the recipient(s).
- Exempt Users** The Exempt Users list contains recipients that do not have their mail filtered for Junk (Anti-Spam) email, attachments, or content. (*Note: Virus scanning is never disabled.*)
- Anti-Spam** The Anti-Spam settings indicate how you want the system to handle evident (high likelihood) and probable (medium likelihood) Spam email.


- Anti-Virus** The Anti-Virus settings indicate how you want the system to handle messages containing a virus.
- Attachment** The Attachment settings indicate which file types to allow and size restrictions for those files, how the system will handle disallowed attachments, and the action to take on any specific attachment filenames you identify.
- Content** The Content policies enable you to indicate unacceptable or suspicious content keywords and the action the system takes when any of those keywords exist in inbound-email content.
- HTML Shield** The HTML Shield settings indicate how you want the system to handle HTML coding in inbound messages.

4.2 Maintaining Allow/Deny Lists

You can configure MX Logic Email Defense to recognize specific sender addresses that are either always-acceptable (Allow lists) or never acceptable (Deny lists) for your domain. The Allow/Deny policies contain IP Addresses, Domain Names, and/or Email Addresses that are allowed or denied, regardless of the other policies applied by the system. (*Note: Virus scanning is never disabled.*)

- **Allow List** entries are not filtered for spam, attachments, content, or HTML. Using Allow lists ensures that email from specific sender addresses or domains are always delivered to the recipient (unless they contain a virus). Any newsletters that your employees are permitted to receive should be added to this list to avoid policy-filtering actions.
- **Deny List** entries are refused and not delivered to the recipient(s). Using Deny lists ensures that email from specific sender addresses or domains are always blocked, whether or not they contain viruses, spam, etc. that would otherwise be detected by the system.

To modify the Allow/Deny policies:

- From the Policies tab ( Policies), click the corresponding **Modify** text link.

Allow/Deny	3 Allowed Sender(s)	Accept Message	[Modify]
Allow/Deny	6 Blocked Sender(s)	Deny Delivery	

The Allow/Deny List management page displays.

Policy Configuration

Allow/Deny List Management for karmaroo.com

✓ Allow List

Add Entry:

Note: Entries present on the allow list will not be filtered for Junk email, attachments or content. Virus scanning is never disabled.

expedia.com
 newalerts@instantnewsbulletins.com
 updates@ual.com

Upload Allow List:

✗ Deny List

Add Entry:

Note: Entries on the deny list will be refused and not delivered to the recipient(s).

10.10.0.1
 clicknowonthis.com
 freeoffers.com
 joe@yahoo.com
 *@kongmail.com
 spammer.com

Upload Deny List:

Allow/Deny List Management Help:
 The following values are allowed in adding list entries:

<i>IP Address</i>	IP address (10.10.10.1) or partial address with wildcards (10.10.10.*)
<i>Domain Name</i>	Qualified domain name (xyz.com) or wildcard (*.xyz.com)
<i>Sender Address</i>	Complete e-mail address (user@xyz.com) or partial address (*@xyz.com)

When uploading a file, the file should be formatted with one entry (IP Address, Domain Name, or Sender Address) on each line.

The guidelines listed at the bottom of the screen define what entries are valid.

- To add a value to either list, type the value in the appropriate **Add Entry** field then click the **Add** button.

The value should appear in the corresponding list box.

- To upload (add) a list from a file, in the appropriate **Upload List** field, either enter the file path or click **Browse** to locate the file, and click the **Upload File** button.

(The file should be formatted with one entry on each line.)

The file values should appear in the corresponding list box.

4. To remove a value from either list, select the value from the list box then click the **Remove** button.


The page will refresh, and the value should be omitted from the list box.

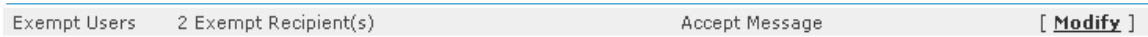
4.3 Maintaining the Exempt Users List

The Exempt Users list contains recipients who are exempt from having their mail filtered for Junk (Anti-Spam) email, attachments, or content. This may be a useful feature if certain end users frequently receive legitimate email that may be confused with spam, such as the classified ads department of a newspaper.

Note: Virus scanning is never disabled.

To modify the Exempt Users list:

1. From the Policies tab ( Policies), click the corresponding **Modify** text link.



The Exempt Users page for your domain displays.

Policy Configuration

Exempt Users for karmaroo.com

Add Entry:

Note: Recipients present on the Exempt Users list will not have their mail filtered for Junk email, attachments or content. Virus scanning is never disabled.

Exempt Users Help:
Enter only fully qualified email addresses into the Exempt Users list. All addresses must be in your domain (ie. "user@karmaroo.com").

Add >>

<< Remove

bferko@karmaroo.com
rblanchard@karmaroo.com

2. To add a user to the Exempt list, enter a complete valid email address (for your domain only) in the **Add Entry** field, and click the **Add** button.

The entry should appear in the list box.

3. To remove a user from the Exempt list, select the user from the list box, and click the **Remove** button.

The page will refresh, and the user should be omitted from the list box.

4.4 Maintaining Anti-Spam Policies

The Anti-Spam settings indicate how you want the system to handle evident (high likelihood) and probable (medium likelihood) Spam email.

For additional security, you can also enable additional, independent functions. The RBL, RSS, and DUL lists (for definitions, see the Glossary) are services maintained by the Mail Abuse Prevention System (MAPS)SM. These lists, which are databases of known spammer addresses, offer some of the best available protection from spammers. However, they may occasionally block legitimate email from getting through, or may block a legitimate sender address that has been wrongly (or unfairly) listed as a spammer. Because these functions operate outside of MX Logic, you should investigate them further before enabling them. More information about MAPS and MAPS databases is available from its website: <http://mail-abuse.org>.

To modify the Anti-Spam policies:

1. From the Policies tab (Policies), click the corresponding **Modify** text link.

Anti-Spam	Medium likelihood of spam	Tag Subject	[Modify]
Anti-Spam	High likelihood of spam	Quarantine Message	

The Anti-Spam Policies page displays.

Policy Configuration

Anti-Spam Policies for karmaroo.com

If a message is probably spam (medium likelihood):

Prepend "SPAM:" to message subject

Quarantine the message

Deny Delivery

If a message is almost certainly spam (high likelihood):

Prepend "SPAM:" to message subject

Quarantine the message

Deny Delivery

Enable Real Time Blackhole List (RBL) (what's this?)

Enable Dial-Up User List (DUL) (what's this?)

Enable Relay Spam Stopper List (RSS) (what's this?)

2. Select an action for an inbound message that is probably spam (**medium likelihood**).

The options are as follows:

- **Prepend “SPAM:” to message subject** – This will deliver the message to the recipient with only the Subject-line altered.
 - **Quarantine the message** – This will place the message in the recipient’s Junk Email Quarantine.
 - **Deny Delivery** – This will prevent the message from being delivered to the recipient.
3. Select an action for an inbound message that is almost certainly spam (**high likelihood**). The options are identical to those detailed in step 2 for medium likelihood.
 4. To enable any of the additional functions offered: The Realtime Blackhole List (RBL)SM, the Relay Spam Stopper List (RSS)SM, and/or the Dial-up User List (DUL)SM, click the corresponding checkbox.
(To disable the function, click the checkbox again to remove the checkmark).
To review a description of these function, click the corresponding (**what’s this**) text-link.
 5. To update the Anti-Spam policy with all your changes, click the **Update Policy** button.
 6. To exit the screen without saving your changes, click **Cancel**.

4.5 Maintaining Anti-Virus Policies

The Anti-Virus settings indicate how you want the system to handle inbound messages that contain a virus. MX Logic Email Defense Service operates on the assumption that viruses are never wanted by your enterprise. Only a network administrator can make the decision to release an infected message to its intended recipient. **Note:** Recipients who were sent an infected email will receive a notice with their message that the virus has been cleaned or stripped.

To modify the Anti-Virus policies:

1. From the Policies tab (Policies), click the corresponding **Modify** text link.



The Anti-Virus Policies page displays.

Policy Configuration

Anti-Virus Policies for karmaroo.com - Inbound

<p>If a message contains a virus:</p> <p><input type="radio"/> Clean the message</p> <p><input checked="" type="radio"/> Quarantine the message</p> <p><input type="radio"/> Strip the attachment</p> <p><input type="radio"/> Deny Delivery</p>	<p>If a message cannot be cleaned:</p> <p><input checked="" type="radio"/> Quarantine the message</p> <p><input checked="" type="radio"/> Strip the attachment</p> <p><input type="radio"/> Deny Delivery</p>
---	--

2. Select an action for a message containing a virus.

The options are as follows:

- **Clean the message** – This will clean the virus from the message, and still deliver the email to the recipient. (**Note:** Selecting this option requires that you complete step 3.)
- **Quarantine the message** – This will place the message in the recipient’s Virus Quarantine.
- **Strip the attachment** – This will deliver only the message text to the recipient after removing the attachment.
- **Deny Delivery** – This will prevent the message from being delivered to the recipient.

3. If you select “Clean the message” in step 2, then the secondary-action options become active, and you must select an action for messages that cannot be cleaned.

The options are similar to those in step 2, as follows:


- **Quarantine the message**
 - **Strip the attachment**
 - **Deny Delivery**
4. To update the Anti-Virus policy with all your changes, click the **Update Policy** button.
 5. To exit the screen without saving your changes, click **Cancel**.

4.6 Maintaining Attachment Policies

The Attachment policies allow you to indicate the following:

- File types to allow
- Size restrictions for each allowed file
- The action to take on disallowed attachments (any attachment types not specified as “allowed” are considered “disallowed”)
- Actions to take on any specific attachment filenames you identify

To modify the attachment policies:

1. From the Policies tab ( Policies), click the corresponding **Modify** text link.

Attachment	Attachment filename contains "federalaudit"	Quarantine Message	[Modify]
Attachment	Attachment filename ends with ".ozm"	Quarantine Message	
Attachment	Attachment filename is "ceospeech.wav"	Accept Message	
Attachment	Audio Files of any size	Accept Message	
Attachment	Video/Movie Files of any size	Accept Message	
Attachment	Image Files of any size	Accept Message	
Attachment	Executables of any size	Accept Message	
Attachment	Scripts of any size	Accept Message	

The Attachment Control Policies page displays.

Policy Configuration

Attachment Control Policies for karmaroo.com - Inbound

Action to take for disallowed attachments:

Deny Delivery
 Strip Attachment
 Quarantine Message

By default, all attachments which are not on the allow list (below) will be filtered with the selected action. Attachments are scrutinized by filename, MIME content type and binary composition.

Allowed attachment types:

Attachment Type	Max Size	Attachment Type	Max Size
<input type="checkbox"/> Microsoft Word Documents (.doc, .dot, ...)	Any Size ▼	<input checked="" type="checkbox"/> Audio Files (.wav, .mp3, .snd, .mid, ...)	Any Size ▼
<input type="checkbox"/> Microsoft Powerpoint Documents (.ppt, .pps, ...)	Any Size ▼	<input checked="" type="checkbox"/> Video/Movie Files (.mov, .mpg, .mpeg, .vdo, ...)	Any Size ▼
<input type="checkbox"/> Microsoft Excel Documents (.xls, .xlt, ...)	Any Size ▼	<input checked="" type="checkbox"/> Image Files (.gif, .jpeg, .bmp, .tiff, ...)	Any Size ▼
<input type="checkbox"/> Microsoft Access Files (.mdb, .mda, ...)	Any Size ▼	<input checked="" type="checkbox"/> Executables (.exe, .dll, ...)	Any Size ▼
<input type="checkbox"/> Other Microsoft Office Files (.frm, .wmf, ...)	Any Size ▼	<input checked="" type="checkbox"/> Scripts (.vbs, .js, .php, .bat, ...)	Any Size ▼
<input type="checkbox"/> Adobe Acrobat (PDF) Files (.pdf, ...)	Any Size ▼	<input type="checkbox"/> ASCII Text Files (.txt, ...)	Any Size ▼
<input type="checkbox"/> Macintosh Files (.bin, .hqx, ...)	Any Size ▼	<input type="checkbox"/> Postscript Files (.ps, ...)	Any Size ▼
<input type="checkbox"/> Compressed or Archived Files (.z, .zip, .gzip, .tar, ...)	Any Size ▼	<input type="checkbox"/> All Other Files	Any Size ▼

Attachment Filename Policies

Policy Type	Conditions	Action	
Attachment	Attachment filename contains "federalaudit"	Quarantine Message	[Delete]
Attachment	Attachment filename ends with ".ozm"	Quarantine Message	[Delete]
Attachment	Attachment filename is "ceospeech.wav"	Allow Delivery	[Delete]

Filename

- From the **Action to take for disallowed attachments** box at the top of the screen, select how you want the system to handle all disallowed attachments.

The options are as follows:

- **Deny Delivery** – This will prevent the message from being delivered to the recipient.
- **Strip Attachment** – This will deliver only the message text to the recipient after removing the attachment.

- **Quarantine Message** – This will place the message in the recipient’s Attachment Quarantine.
3. From the **Allowed Attachment Types** area, select all attachment types you want “allowed” by placing a check in the corresponding checkbox.

Note: Any attachment types without checkmarks are considered “disallowed”.

To view all qualifying file extensions for an attachment type listed, click on the file extensions for that attachment type. The complete list for that attachment displays next to the **Update Policy** button.

Allowed attachment types:

Attachment Type	Max Size	Attachment Type	Max Size
<input type="checkbox"/> Microsoft Word Documents (.doc, .dot, ...)	Any Size	<input checked="" type="checkbox"/> Audio Files (.wav, .mp3, .snd, .mid, ...)	Any Size
<input type="checkbox"/> Microsoft Powerpoint Documents (.ppt, .pps, ...)	Any Size	<input checked="" type="checkbox"/> Video/Movie Files (.mov, .mpg, .mpeg, .vdo, ...)	Any Size
<input type="checkbox"/> Microsoft Excel Documents (.xls, .xlt, ...)	Any Size	<input checked="" type="checkbox"/> Image Files (.gif, .jpeg, .bmp, .tiff, ...)	Any Size
<input type="checkbox"/> Microsoft Access Files (.mdb, .mda, ...)	Any Size	<input checked="" type="checkbox"/> Executables (.exe, .dll, ...)	Any Size
<input type="checkbox"/> Other Microsoft Office Files (.frm, .wmf, ...)	Any Size	<input checked="" type="checkbox"/> Scripts (.vbs, .js, .php, .bat, ...)	Any Size
<input type="checkbox"/> Adobe Acrobat (PDF) Files (.pdf, ...)	Any Size	<input type="checkbox"/> ASCII Text Files (.txt, ...)	Any Size
<input type="checkbox"/> Macintosh Files (.bin, .hqx, ...)	Any Size	<input type="checkbox"/> Postscript Files (.ps, ...)	Any Size
<input type="checkbox"/> Compressed or Archived Files (.z, .zip, .gzip, .tar, ...)	Any Size	<input type="checkbox"/> All Other Files	Any Size

Update Policy

The attachment category "Scripts" includes attachments with the following extensions:
 .vbs, .js, .php, .bat, .vba, .vbe, .hta, .wsh, .wst, .sct, .asp, .htx, .vbe, .acc, .ccs, .php, .php3, .wsc

4. For each allowed (checked) attachment type, set the maximum allowable size for that attachment type by either selecting a value from the corresponding **Max Size** drop-down list or accepting “Any Size” (default).

Any Size

- Any Size
- 500 KB
- 1 MB
- 2 MB
- 5 MB
- 10 MB
- 15 MB

5. To save your Allowed and Disallowed policy changes, click the **Update Policy** button.
6. To exit the screen without saving your Allowed and Disallowed policy changes, click the **Finished** button at the bottom of the screen.

4.7 Maintaining Content Policies

The Content policies enable you to indicate unacceptable or suspicious content keywords and the action the system should take when any of those keywords exist in inbound-email content. These policies are customizable for your environment:

- Three static groups exist in the system: Profanity, Racially Insensitive, and Sexual Overtones. These groups can only be enabled or disabled (you cannot modify their contents).
- You can create new lists (groups) and modify their contents or delete them as needed.

To modify the content policies:

1. From the Policies tab (Policies), click the corresponding **Modify** text link.

Content	Message contains word from 'Profanity'	Quarantine Message	[Modify]
Content	Message contains word from 'Racially Insensitive'	Quarantine Message	
Content	Message contains word from 'Sexual Overtones'	Quarantine Message	

The Current Content Groups page displays.

Policy Configuration

Current Content Groups for karmaroo.com - Inbound

Content Group	Active	Actions
	<input type="checkbox"/>	Quarantine ▼ [Edit Delete]
Profanity	<input checked="" type="checkbox"/>	Quarantine ▼ [View]
Racially Insensitive	<input checked="" type="checkbox"/>	Quarantine ▼ [View]
Sexual Overtones	<input checked="" type="checkbox"/>	Quarantine ▼ [View]

Group Name:

Keywords:

2. To view the contents of any static content group, click the corresponding **View** text-link.
The selected group's content populates the **Keywords** list box.
Note: You cannot modify the contents of these static content groups; you can only disable or enable them (step 3), or change the actions assigned to them (step 4).
3. To enable or disable any Content Group, simply check or uncheck the corresponding **Active** checkbox.
4. To assign an action to a group, the group must first be "Active" (see step 3), then you can select from the corresponding **Actions** drop-down list.
The options are as follows:
 - **Tag message** – This will deliver the message, but tag it.
 - **Quarantine** – This will place the message in the recipient's Content Keyword Quarantine.
 - **Deny** – This will prevent the message from being delivered to the recipient.
5. To create a new content group:
 - a. From the top (blank) Content Group line, click the **Edit** text-link.
 - b. In the **Group Name** field, enter a new content group name.
 - c. In the **Keywords** list box, enter the keywords you want include in that group (placing each term on a separate line).
 - d. Click the **Save Group** button.
The new group appears in the Content Group list, disabled (not "Active").
 - e. To activate the new content group and assign an action, see steps 3 – 4.
6. To modify a content group:
 - a. Click the corresponding **Edit** text-link.
The selected group's content populates the **Keywords** list box.
 - b. In either the **Keywords** list box or **Group Name** field, change the contents as needed.
 - c. Click the **Save Group** button.
The group appears in the Content Group list, disabled (not "Active").
 - d. To activate the content group and assign an action, see steps 3 – 4.
7. To delete a content group, click the corresponding **Delete** text-link.
The selected content group should no longer appear in the Content Group list.
8. To exit the screen, click the **Finished** button.

4.8 Maintaining HTML Shield Policies

The HTML Shield settings indicate how you want the system to handle HTML coding in inbound messages.

To modify the HTML Shield policies:

1. From the Policies tab (Policies), click the corresponding **Modify** text link.

HTML Shield	Medium - Strip malicious HTML and scripts	Strip	[Modify]
HTML Shield	Message contains image references	Replace	
HTML Shield	Message contains spam "beacons" / web bugs	Strip	

The HTML Shield Policies page displays.

Policy Configuration

HTML Shield Policies for karmaroo.com

No protection

Low

- Remove malicious HTML tags (iframe, frame, layer, span, meta, style)

Medium

- Remove malicious HTML tags (iframe, frame, layer, span, meta, style)
- Disable all Javascript/Java/ActiveX (script, style, embed, object, applet)
- Remove HTML comments
- Remove invalid HTML attributes

High

- Strip (remove) all HTML

Enable spam "beacon" and web bug blocking (what's this?)

Replace all image links with a default transparent image

2. Select your HTML policy from the available radio buttons.

The options are as follows:

- **No protection** – This provides no HTML protection from messages.
- **Low** – This removes malicious HTML tags from messages.
- **Medium** – This removes malicious tags, disables all Javascript/Java/ActiveX, removes HTML comments, and removes invalid HTML attributes from messages.
- **High** – This strips (removes) all HTML from messages.

3. You can also enforce further HTML policies by checking the appropriate checkboxes:

- **Enable spam “beacon” and web bug blocking** – This blocks spam “beacons” and web bugs that can access information about the recipient without their knowledge.
 - **Replace all image links with a default transparent image** – This reduces the size of image-intensive messages.
4. To save your changes to the HTML Shield policies, click the **Update Policy** button.
 5. To exit the screen without saving your changes, click the **Cancel** button.

5 SETUP TAB

5.1	Setting up Inbound Servers _____	44
5.2	Enabling/Disabling Spam Reporting _____	46
5.3	Changing Your Password _____	48

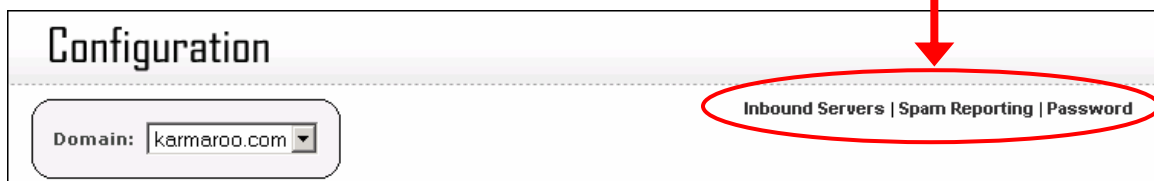
5.1 Setting up Inbound Servers

This page enables you to configure MX Logic Email Defense Service to deliver inbound SMTP traffic properly to the mail server(s) at your domain.

To setup inbound servers:

1. Click the Setup tab (Setup).

The menu bar displays the various pages you can access within this tab-screen:



By default, the first screen that displays is the Inbound Servers setup for the selected domain. You can also access this screen from any other Setup tab-screen by clicking **Inbound Servers** on the menu bar.

The screenshot shows the 'Inbound Servers Setup' page. At the top, there is a 'Configuration' header and a menu bar with 'Inbound Servers | Spam Reporting | Password'. Below the header is a 'Domain' dropdown menu set to 'karmaroo.com'. The main content area is titled 'Inbound Servers Setup' and contains a table with the following data:

SMTP Host Address	Port	Preference	Active		
mail3.karmaroo.com	25	5	<input checked="" type="checkbox"/>	Update	Delete
mail2.karmaroo.com	25	5	<input checked="" type="checkbox"/>	Update	Delete
mail4.karmaroo.com	25	10	<input checked="" type="checkbox"/>	Update	Delete
			<input type="checkbox"/>	Update	Delete

Below the table is a 'Inbound Servers Setup Help' box with the following text:

Inbound Servers Setup Help:
 In order to configure proper delivery to inbound SMTP servers please refer to the following field definitions:

- SMTP Host Address:** Host to delivery inbound SMTP traffic. Provide either an IP address or full hostname.
- Server Port:** Normally SMTP is port 25. If different, specify here.
- Preference:** MX Preference for this server. When delivering mail, the service will attempt to deliver to the lowest numbered server(s) first.
- Active:** Toggle if this SMTP host is currently accepting traffic.

2. In a blank line in the **SMTP Host Address** column, enter your full hostname for your domain's SMTP.
Enter either an IP address or a full hostname.
3. Enter the server port for SMTP traffic in the corresponding **Port** field.
Normally this is port 25.
4. Enter a **Preference** value for each SMTP.
Enter the preference value for this mail server (MTA). This value indicates which mail server (if you have multiple MX records) will receive mail first. The higher priority mail server should have the lowest preference value (*e.g.*, '10' for your highest priority mail server, '20' for your secondary mail server, etc.). If for some reason the mail server with highest priority is unable to receive incoming email, then email will be delivered to the mail server with the next highest priority, and so on.
Note: if two mail servers have the same preference value, MX Logic will balance email delivery between them.
5. To activate or deactivate a SMTP host, check or uncheck the corresponding **Active** checkbox.
These connections can be turned on and off as needed, without being reconfigured, simply by checking or un-checking the **Active** box.
6. To ensure that any new configurations or changes are saved and applied, click the corresponding **Update** button.
7. To delete an SMTP, click the corresponding **Delete** button.

5.2 Enabling/Disabling Spam Reporting

MX Logic Email Defense Service enables end users to manage their own spam quarantine, as well as create their own list of allowed email senders. However, for this functionality to become operational, as the MX Logic Email Defense Service administrator, you must first activate Spam Summary Reporting.

By enabling the Spam Summary Reporting feature, end users will receive periodic summaries of quarantined spam messages intended for them. By utilizing this feature, the administrator relieves the burden of managing the entire spam quarantine at the domain level, instead pushing the responsibility to end users who can view and clean out their personal spam quarantine at their convenience.

Recipient spam summary reporting enables email delivery of quarantine reports to all users with messages quarantined as junk email (spam). Recipients may view and delete or release quarantined messages listed in the delivered report. When initially enabled, reports are delivered daily. However, users may personalize the delivery frequency within the report they receive.

To manage spam reporting:

1. From the Setup tab (Setup) menu, click the **Spam Reporting** text-link.

The Recipient Spam Reports page displays.

Domain:

[Inbound Servers](#) | [Spam Reporting](#) | [Password](#)

Recipient Spam Reports

Recipient spam quarantine reporting

Enabled (report delivery ON)
 Disabled (report delivery OFF)

Recipient spam summary reporting enables email delivery of quarantine reports to all users which have messages that have been quarantined as junk e-mail (spam). Recipients may delete, view and release quarantined messages that are listed in the delivered report. When initially enabled, reports are delivered on a daily basis. Recipients may however personalize the frequency of delivery by choosing their desired reporting period within the email.



(click for preview)

2. Enable or Disable this feature completely by selecting the appropriate radio button.
3. To save your change, click **Update**.
4. To exit the screen without saving any changes, click **Cancel**.

Once the Spam Summary Reporting feature has been enabled, end users will receive Spam Summary Reports by email. The Reports appear as follows:

This email contains a list of all messages which have been quarantined.
 To view a message, simply click on the Subject. To move a message to your Inbox, click the "Release" link. To release a message and add the sender to your Allowed Senders List, click the "Always Allow" link. To delete all of the messages, click the "Delete All" link at the bottom of the Spam Summary Report.

Spam Summary Report

Spam Summary Report for demo@demo.com

Date	From	Subject	Size	
01/28/2003 10:53 AM	bulkmail@karmaroo.com	Need Some Extra Cash?29898	3kb	[Release Always Allow]
01/28/2003 10:53 AM	bulkmail@karmaroo.com	If you're not losing hair, don	4kb	[Release Always Allow]
01/28/2003 10:53 AM	bulkmail@karmaroo.com	eBay, Declare Independence! Jo	3kb	[Release Always Allow]
01/28/2003 10:53 AM	bulkmail@karmaroo.com	Free New Cars for the Taking	4kb	[Release Always Allow]
01/28/2003 10:53 AM	bulkmail@karmaroo.com	Get Professional Web Hosting f	6kb	[Release Always Allow]
01/28/2003 10:53 AM	bulkmail@karmaroo.com	Work at Home & Make Great Mone	5kb	[Release Always Allow]

[[Delete All](#)]

Continue to send this summary every: [day](#) | [2 days](#) | [3 days](#) | [week](#) | [never](#)

With this Spam Summary Report:

- Users can release [**Release**] one or more of the emails to their inbox (this is especially useful in the case of false positives, *i.e.*, legitimate email accidentally captured as spam), and then delete all remaining spam emails [**Delete All**].
- Users can also add a sender to their personal "Allow List" by clicking the [**Always Allow**] text-link; this will release the quarantined email, and will prevent future quarantining of email from that particular address. (**Note:** Because domain-level policies always override end-user policies, email from an address on an end user's "Allow List" will still be blocked if the same email address or domain is on the domain-level "Deny List.")
- Users can each choose the frequency that they receive their Spam Summary Report (every one, two, or three days, every week, or never).

5.3 Changing Your Password

You can change your password at any time for the domain (email address) you used to log into the MX Control Console.

To change your password:

1. From the Setup tab ( Setup) menu, click the **Password** text-link.

The Password Change page displays.

Configuration

[Inbound Servers](#) | [Spam Reporting](#) | [Password](#)

Password Change

E-mail Address: **austin.powers@karmaroo.com**

Old Password:

New Password:

Six-character minimum; no spaces

Retype New Password:

2. Enter your **Old Password**.
3. Enter a **New Password**.
Your password must be at least six-characters long, containing no spaces.
4. Confirm your new password by entering it again in the **Retype New Password** field.
5. Click the **continue** button.
 - If your password cannot be changed, a popup message denotes the reason.
 - If your password changed successfully, the page will refresh, displaying “Password Changed” in red text at the top.

6 USERS TAB

- 6.1 Searching for Users & Viewing User Details ____ 50
- 6.2 Changing User Roles & Settings _____ 53
- 6.3 Accessing Quarantined Messages for a User ____ 55

6.1 Searching for Users & Viewing User Details

From the Users tab, you can search for users and view user details. User details include account and login information as well as messaging traffic for that user.

To search for users:

1. From the tab menu, click the Users tab (👤 Users).

The User Management page displays.

User Management

Domain:
Search

Quick Jump:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Other	All
-------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	-------	-----

Pages: 1 2 3 4 [Next >] Page 1 of 4

User	Role	Last Login	Date Created
alamode@karmaroo.com	Customer Admin	06/04/03 13:06	06/04/03 10:32
austin.powers@karmaroo.com	Customer Admin	05/22/03 13:03	09/11/02 10:43
bradford@karmaroo.com	User	05/22/03 14:17	05/22/03 14:17
bill.lewis@demo.com	Domain Admin	12/11/02 11:35	12/11/02 11:35
cqe@karmaroo.com	Customer Admin	12/19/02 02:58	11/15/02 09:19
bulkmail@karmaroo.com	User	11/14/02 14:09	11/14/02 14:09
capehart@karmaroo.com	Customer Admin	06/02/03 09:03	06/02/03 08:07
fontana@karmaroo.com	Domain Admin	11/26/02 16:52	11/26/02 16:52

Pages: 1 2 3 4 [Next >] Page 1 of 4

The page shows All Users by default.

- To sort the list by any of the headings, simply click the heading title.
 - Each page lists up to 100 users. You can view additional pages by either clicking the **Next >** or **< Prev** links or clicking on the specific page number link.
2. To view only usernames that begin with a specific letter, click the letter on the **Quick Jump** menu.
 3. To view only usernames that begin with a character other than a letter, click the **Other** option on the **Quick Jump** menu.
 4. To find users via the Search function:
 - a. Click the **Search** button.
The search screen displays.

User Management

Domain:

User ID @karmaroo.com

User

No search performed yet.

- b. From the drop-down list, select a qualifier for your search entry (step c).
- c. In the text box, enter the characters by which to search.
- d. Click the **search** button.

The search results display.

User Management

Domain:

User ID @karmaroo.com

User	Role	Last Login	Date Created
austin.powers@karmaroo.com	Customer Admin	05/22/03 13:03	09/11/02 10:43
investors.life@karmaroo.com	Customer Admin	06/09/03 16:46	06/09/03 16:45
steve.klein@karmaroo.com	Reseller Admin	06/11/03 12:13	05/22/03 14:27
steve.ruskin@karmaroo.com	Reseller Admin	06/05/03 13:26	05/28/03 11:50

- e. To view user details, see step 5.
 - f. To return to the default page to view all users, click the **List All** button.
5. To view user details, click the username.

The User Details page displays, including a menu:

User Management

[Users](#) | [Details](#) | [Quarantine](#)

- The **Users** link displays the main User Management page that displays all users.
- The **Details** link (the page you are currently viewing) displays the details for the selected user.
- The **Quarantine** link displays the quarantined messages for the selected user.

User Management

[Users](#) | [Details](#) | [Quarantine](#)

User Details for austin.powers@karmaroo.com

Customer Name: Sample Customer
Date Created: 09/11/02
First Login: 05/22/03 12:54
Last Login: 05/22/03 13:03
Last Spam Report: 06/08/03 03:25
Role: Customer Admin
Domain Contact Email: scott@karmaroo.com

Recent Messaging Traffic

Messages Last 7 Days: 2030
Average Message Size: 18 KB

Date	Inbound Messages
06/03	380
06/04	380
06/05	350
06/06	300
06/07	300
06/08	80
06/09	220

The User Details page displays account and user information, as well as recent messaging traffic for the user.

- To edit user information, see the Changing User Roles & Settings instructions (on page 53).
- To access quarantines messages for this user, see the Accessing Quarantined Messages for a User instructions (on page 55).
- To return to the default page to view all users, click **Users** on the menu bar.

6.2 Changing User Roles & Settings

From the User Details page, you can change a user's role, spam report frequency, and password.

To change this user information:

1. Find the user and access the User Details screen as described in steps 1 – 5 of the Searching for Users & Viewing User Details instruction (on page 50).
2. From the User Details screen, click the **Edit User** button at the bottom of the screen.

The edit user page displays.

The screenshot shows the 'User Management' interface with a sub-header 'User Management' and navigation links 'Users | Details | Quarantine'. The main content area is titled 'Edit austin.powers@karmaroo.com' and contains the following form fields:

- Role:** A dropdown menu currently set to 'Domain Admin'.
- Spam Report Freq:** A dropdown menu currently set to 'Once per day'.
- Password:** A text input field with masked characters (dots).
- Verify Password:** A text input field with masked characters (dots).

At the bottom of the form are two buttons: 'Submit' and 'Cancel'.

3. To change the user's role, choose another option from the **Role** drop-down list.

The screenshot shows a dropdown menu for the 'Role' field. The current selection is 'Customer Admin'. The menu is open, displaying the following options:

- Customer Admin
- User
- Reports Manager
- Quarantine Manager
- Domain Admin
- Customer Admin

Note: You cannot change the role of a user whose role is more senior than your own.

4. To change the user's "spam report frequency" setting, choose another option from the **Spam Report Freq** drop-down list.

The screenshot shows a dropdown menu for the 'Spam Report Freq' field. The current selection is 'Once every 2 days'. The menu is open, displaying the following options:

- Once every 2 days
- Never
- Once per day
- Once every 2 days
- Once every 3 days
- Once per week

5. To change the user's password, enter a new password in the **Password** field and again in the **Verify Password** field.

6. To save your changes, click the **Submit** button.
7. To exit the screen without saving your changes, click the **Cancel** button.

6.3 Accessing Quarantined Messages for a User

From the User Details page, you can access the user's quarantined messages, enabling you to then view, release, or delete those messages.

To access and manage a user's quarantined messages:

1. Find the user and access the User Details screen as described in steps 1 – 5 of the Searching for Users & Viewing User Details instruction (on page 50).
2. From the User Details screen, click **Quarantine** on the menu bar.

The User Quarantine page displays.

User Management

[Users](#) | [Details](#) | [Quarantine](#)

Recipient Email: austin.powers@karmaroo.com

✓ Date	From	To	Subject	Type	Size
<input type="checkbox"/> 05/30 07:22	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/> 05/30 09:23	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/> 05/30 10:29	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/> 05/30 11:57	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/> 05/30 13:36	apowers@mxlogic.net	austin.powers@karmar	Check this out!	Virus	62KB
<input type="checkbox"/> 06/09 17:46	apowers@mxlogic.net	austin.powers@karmar	\$400 off pressure-re	Spam	9KB
<input type="checkbox"/> 06/09 17:46	apowers@mxlogic.net	austin.powers@karmar	Do your joints and b	Spam	4KB
<input type="checkbox"/> 06/09 17:57	apowers@mxlogic.net	austin.powers@karmar	Pass this on.	Virus	107KB

release delete

- To sort the list by any of the headings, simply click the heading title. Clicking the heading again will sort the list in the opposite order.
Note: Sorting the list automatically transfers you to the Message Quarantine screen for the specific user.
 - The “Type” column displays the policy enforced in quarantining the message.
 - For each quarantined message, you have the option to **delete** it completely, or to **release** it (sending it to the intended recipient).
3. To release or delete select messages, check (click) the corresponding checkboxes then either **release** or **delete** the selected messages using the buttons at the bottom of the page. (Clicking the checkbox again will deselect it.)

4. To release or delete all messages on the page displayed, click the single checkbox at the bottom of the page, and click either **release** or **delete**.
5. To view the actual message, before release or deletion, click the linked email address in the **From** column. A Safe Message View displays:

User Management

[Details](#) | [Quarantine](#)

Safe Message View

From : apowers@mxlogic.net

To : austin.powers@karmaroo.com

Subject : Quit Smoking Product Makes Breakthrough!!

Date : Wed, 11 Jun 2003 00:13:54 -0600

Status : Message quarantined by Junk Email module (score High)

Attachments :

Filename	Size	Content Type
(NONE)	2167	text/plain
(NONE)	2701	text/html

Quit Smoking Product Makes Breakthrough!!

Have you have ever wanted to quit smoking? With this product there is a proven 95% chance that you will!!

Don't delay; discover why All Natural "De-Nics" is different from anything you have ever seen! Guaranteed!!!

All third party products and services promoted in this email are offered exclusively by third party advertisers. SportTime.info makes no representations or warranties with respect to these offers and all claims for injury and damages related to such offers are the sole responsibility of the advertiser.

Message Action:
release
delete

You can also release or delete a message from this detailed screen, using the **Message Action** buttons.


- To return to the User Quarantine page, click **Quarantine** on the menu bar.
- To return to the User Details page, click **Details** on the menu bar.

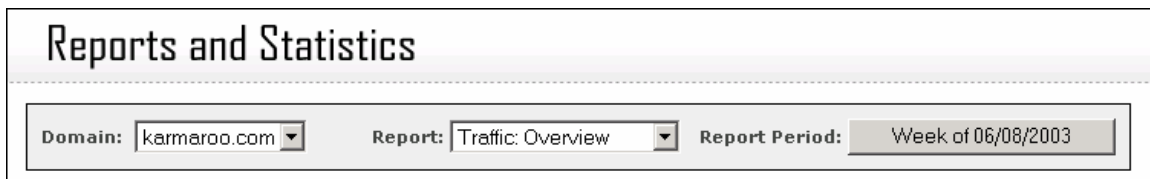
7 REPORTING TAB

7.1	Introduction – Reporting Tab Functionality _____	58
7.2	Viewing Traffic Overview _____	60
7.3	Viewing the Threats Overview _____	61
7.4	Viewing a Spam Threats Report _____	62
7.5	Viewing a Virus Threats Report _____	63
7.6	Viewing a Content Threats Report _____	65
7.7	Viewing an Attachment Threats Report _____	66
7.8	Viewing a User Activity Report _____	67
7.9	Viewing an Event Log Report _____	68
7.10	Viewing an Audit Trail Report _____	70

7.1 Introduction – Reporting Tab Functionality

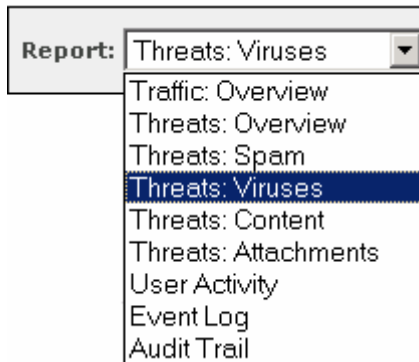
From the Reports and Statistics page, you can view information such as trends, policy actions, and a summary of traffic and various threats detected. You can also view and download data including the top inbound users; event logs that display actions taken for virus, content, or attachment policy violations; and audit trails that track activity within the system, such as login and system changes.

When you click the Reporting tab ( Reporting), the Reports and Statistics page displays with a top menu bar that contains **Domain**, **Report**, and **Report Period** options:



The screenshot shows the 'Reports and Statistics' page header. Below the header is a menu bar with three options: 'Domain: karmaroo.com', 'Report: Traffic: Overview', and 'Report Period: Week of 06/08/2003'.

1. As with any other page in the MX Control Console, you must select the correct domain from the **Domain** drop-down list.
2. The **Report** drop-down list enables you to select which report to view:

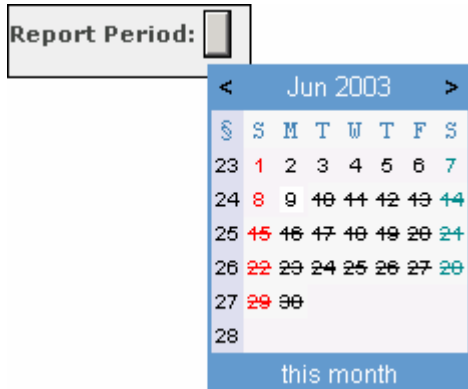


The screenshot shows the 'Report' drop-down list with the following options: Threats: Viruses (selected), Traffic: Overview, Threats: Overview, Threats: Spam, Threats: Content, Threats: Attachments, User Activity, Event Log, and Audit Trail.

Note: The first item listed is always the default page that displays upon clicking the Report tab.

3. The Report Period option enables you to select the time span for which you would like to view the selected reports (the default is the current week).

Clicking the **Report Period** button initiates a popup calendar.



- To view previous or subsequent months, click the < or > arrow.
- To select a specific day, click on the date.
- To select an entire week, click the week number (in the blue-shaded column).
- To select an entire month, click the **this month** text at the bottom of the calendar.

Note: The report period you choose will apply to all reports you view while still on this tab, unless/until you change it. Clicking another tab then returning to the Reporting tab will set the Report Period back to the default of the current week.

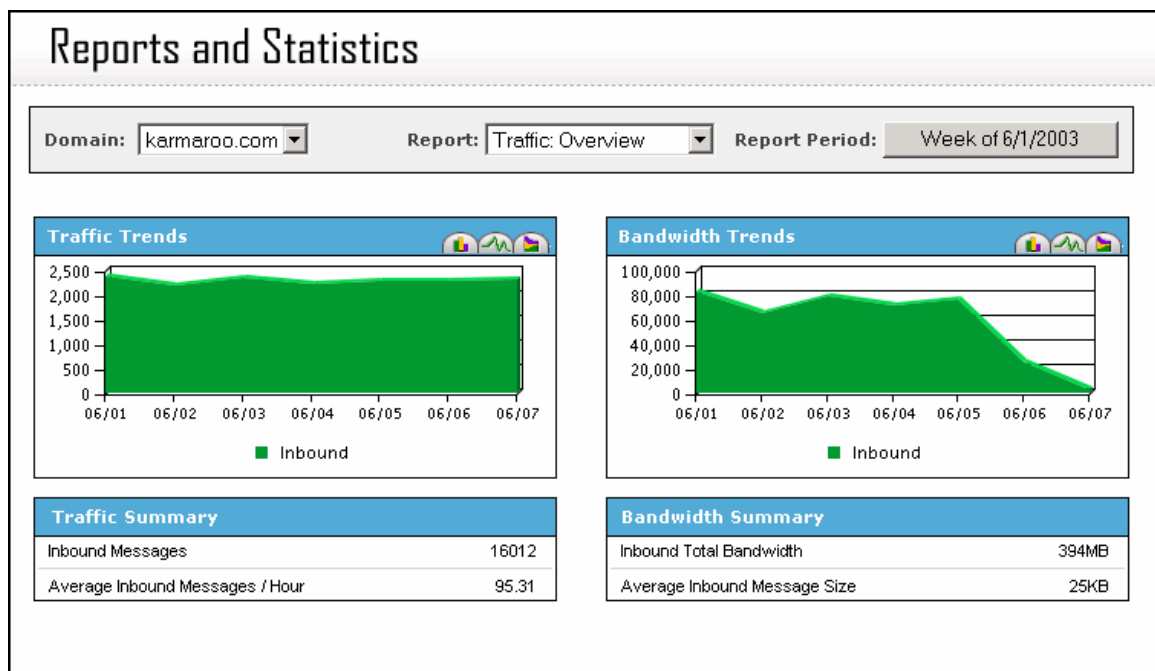
7.2 Viewing Traffic Overview

The Traffic Overview enables you to monitor your domain's general message traffic, including the total and average size and bandwidth for inbound messages.

You can access the Traffic Overview screen two ways:

- Because the Traffic Overview screen is the default report screen, you can simply click the Reporting tab (Reporting) from the main menu. **Note:** Accessing the page this way will reset the Report Period to the current week (default).
- From the Reports and Statistics page, you can select **Traffic: Overview** from the **Report** drop-down list on the top menu bar.

The Traffic Overview screen displays for the Domain and Report Period selected.



The screen contents include:

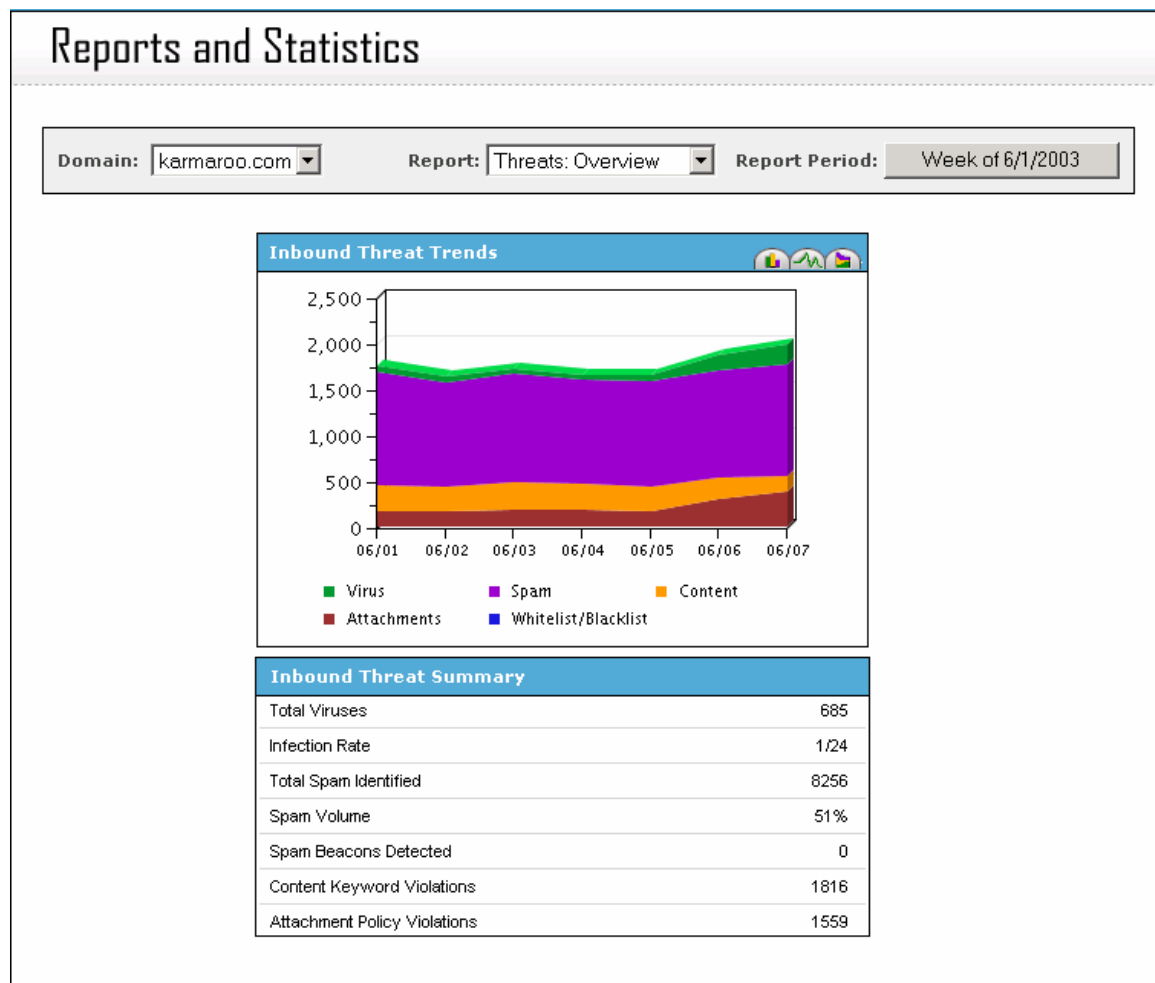
- **Traffic Trends** – This box contains a graphic showing the inbound email traffic.
- **Traffic Summary** – This box details the inbound message traffic, listing the number of inbound messages and the average number of inbound messages per hour.
- **Bandwidth Trends** – This box contains a graphic showing the inbound bandwidth.
- **Bandwidth Summary** – This box details the inbound traffic bandwidth, listing the total inbound bandwidth and the average inbound messages size.

7.3 Viewing the Threats Overview

The Threats Overview enables you to monitor your domain's inbound threat trends and general statistics on violations detected by policy type.

You can access the Threats Overview screen by selecting **Threats: Overview** from the **Report** drop-down list.

The Threats Overview screen displays for the Domain and Report Period selected.



The screen contents include:

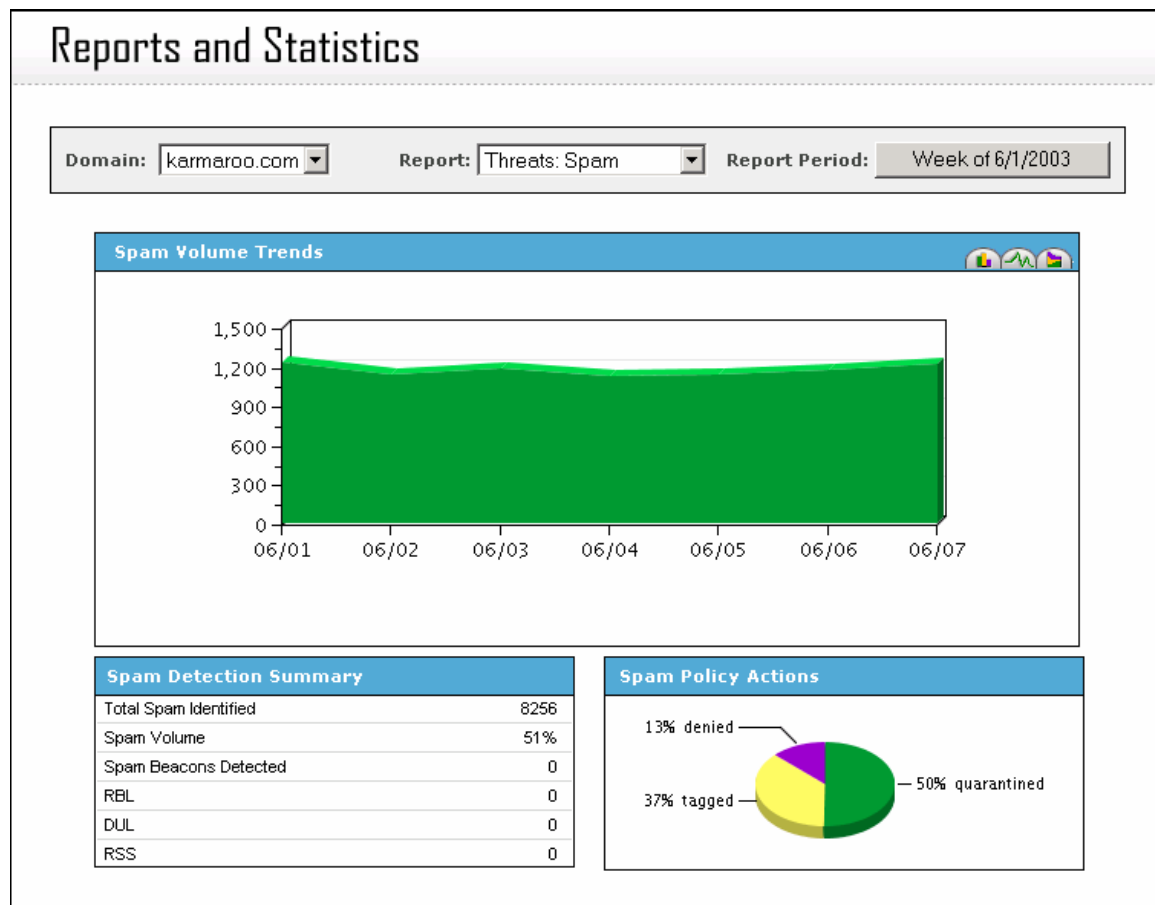
- **Inbound Threat Trends** – This box contains a graph showing the number of inbound messages quarantined. The graph is color-coded according to the threat detected: Spam, Virus, Content, Attachments, or Whitelist/Blacklist.
- **Inbounds Threat Summary** – This box details the threats detected, listing the Total Viruses, Infection Rate, Total Spam Identified, Spam Volume, Spam Beacons Detected, Content Keyword Violations, and Attachment Policy Violations.

7.4 Viewing a Spam Threats Report

The Spam Threats report enables you to monitor your domain's inbound spam-mail trends, details on the spam detected, and spam policy enforcement statistics.

You can access the Spam Threats screen by selecting **Threats: Spam** from the **Report** drop-down list.

The Spam Threats screen displays for the Domain and Report Period selected.



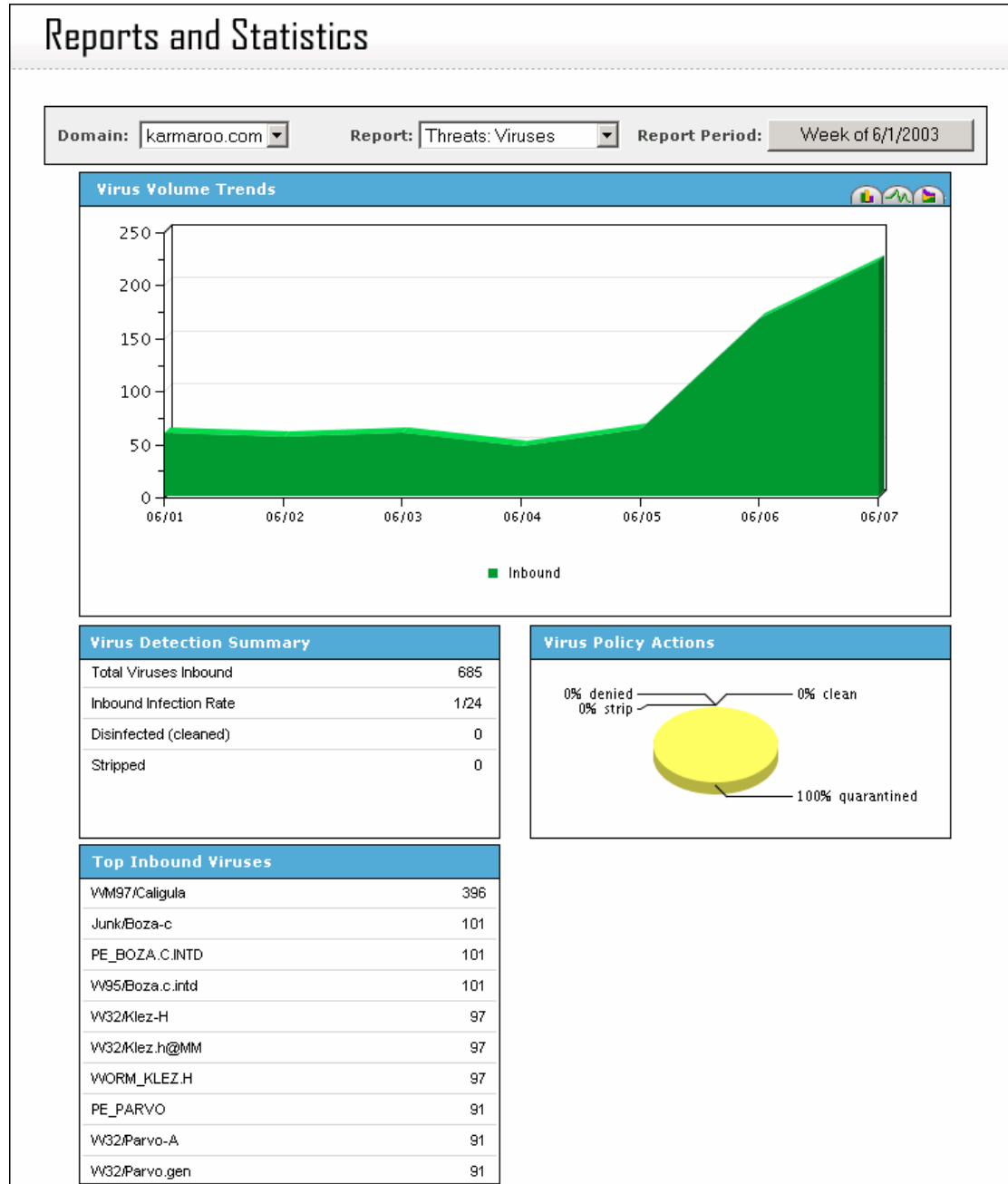
The screen contents include:

- **Spam Volume Trends** – This box contains a graph showing the total number of inbound Spam messages detected.
- **Spam Detection Summary** – This box details the spam messages detected, listing the Total Spam Identified, Spam Volume, Spam Beacons Detected, RBL, DUL, and RSS. (For definitions of these terms, see the Glossary.)
- **Spam Policy Actions** – This box contains a chart showing the Spam Policy actions enforced for the spam-detected messages.

7.5 Viewing a Virus Threats Report

The Virus Threats report enables you to monitor your domain's inbound virus traffic (volume trends and details), virus policy enforcement statistics, and top viruses detected. You can access the Virus Threats screen by selecting **Threats: Viruses** from the **Report** drop-down list.

The Virus Threats screen displays for the Domain and Report Period selected.



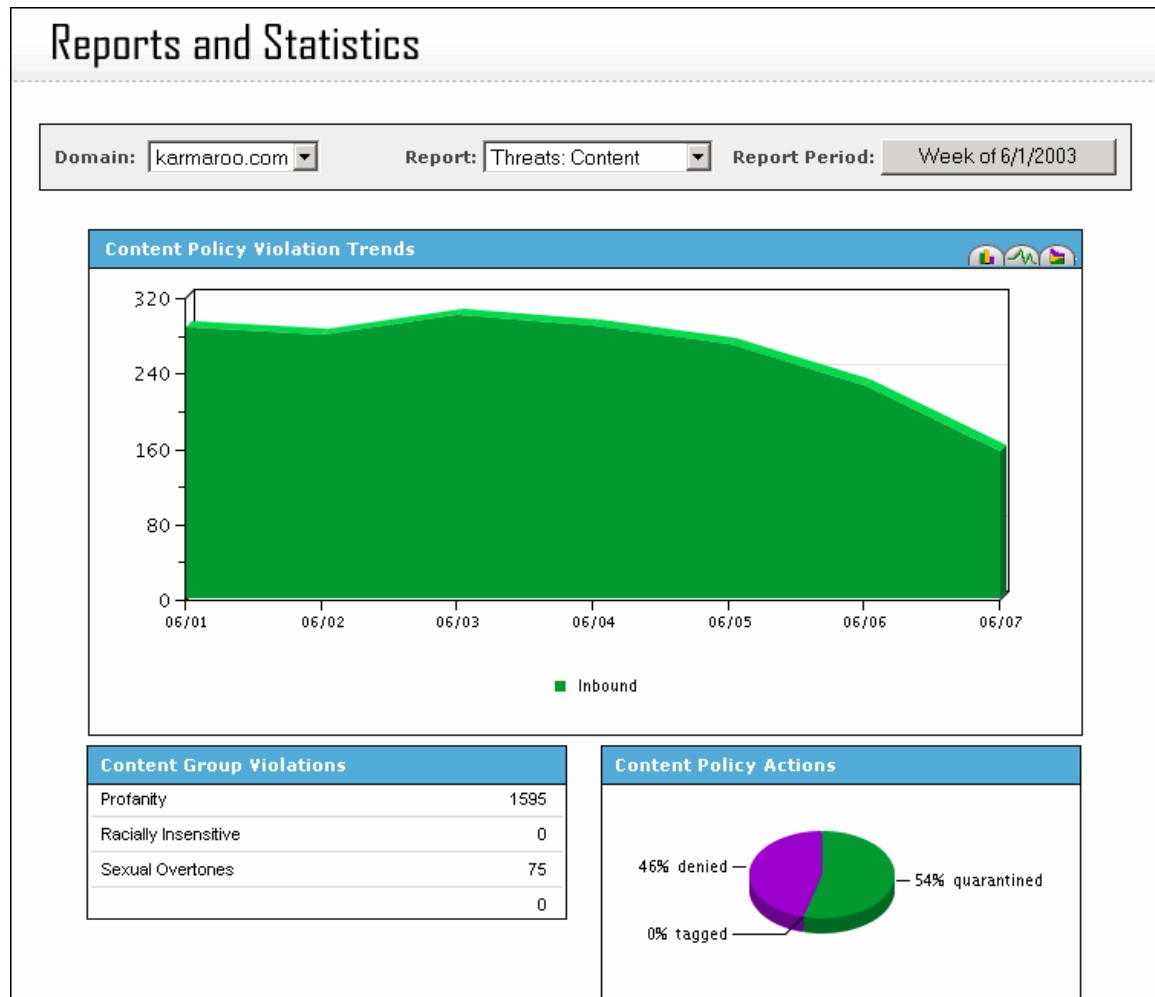
The screen contents include:

- **Virus Volume Trends** – This box contains a graph showing the total number of inbound virus-infected messages detected.
- **Virus Detection Summary** – This box provides the Total Viruses Inbound, Inbound Infection Rate, Disinfected (cleaned), and Stripped messages.
- **Virus Policy Actions** – This box contains a chart showing the Virus Policy actions enforced for the virus-infected messages.
- **Top Inbound Viruses** – This box lists the most common viruses detected, beginning with the most frequent.

7.6 Viewing a Content Threats Report

The Content Threats report enables you to monitor your domain's inbound email content violation trends, detected content group violations, and content policy enforcement statistics. You can access the Content Threats screen by selecting **Threats: Content** from the **Report** drop-down list.

The Content Threats screen displays for the Domain and Report Period selected.



The screen contents include:

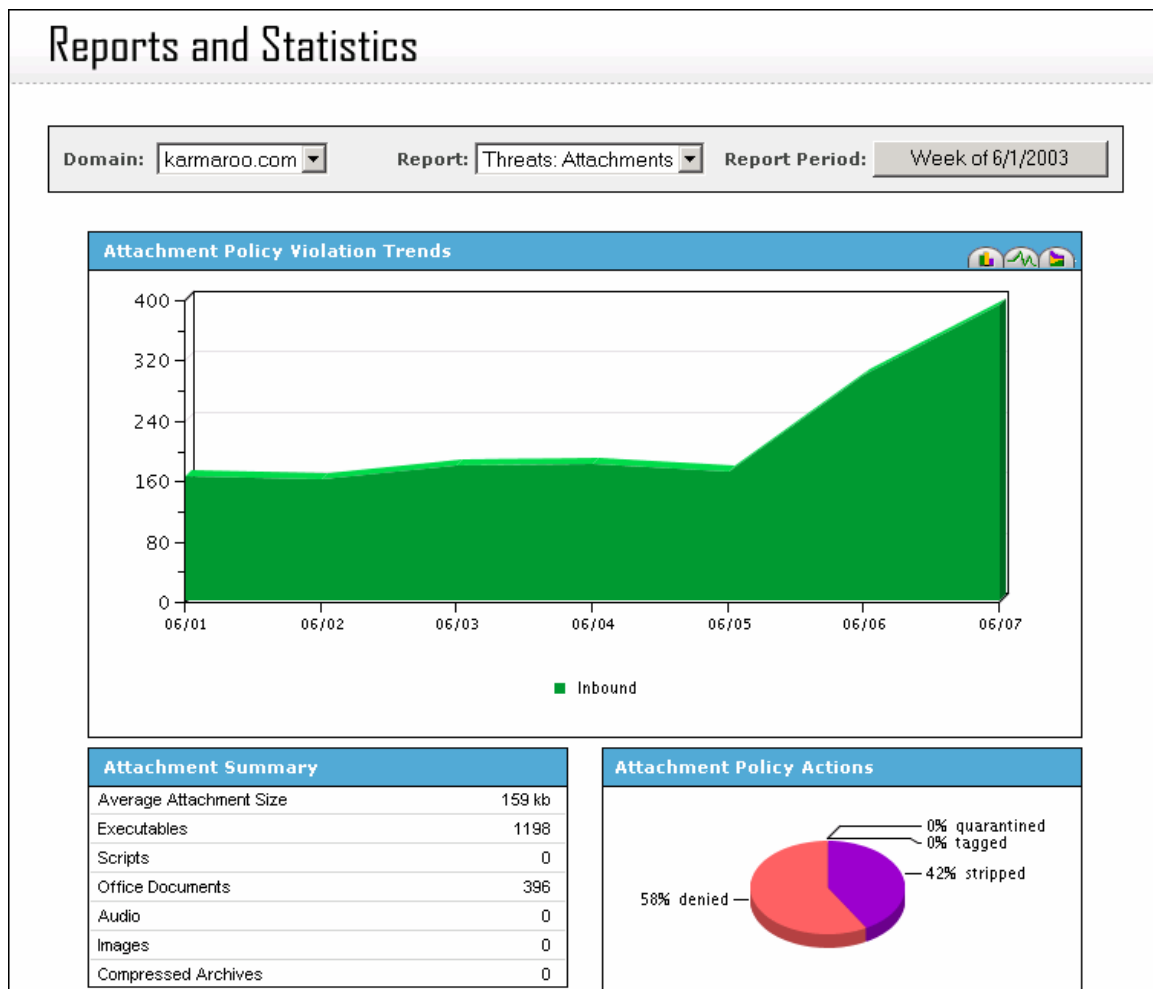
- **Content Policy Violation Trends** – This box contains a graph showing the total number of inbound content-flagged messages detected.
- **Content Group Violations** – This box provides the number of violations listed by active Content Group.
- **Content Policy Actions** – This box provides a chart showing the Content Policy actions enforced for messages containing unwanted content.

7.7 Viewing an Attachment Threats Report

The Attachment Threats report enables you to monitor your domain's inbound attachment violation trends, the violations detected by attachment type, and content policy enforcement statistics.

You can access the Attachment Threats screen by selecting **Threats: Attachments** from the **Report** drop-down list.

The Attachment Threats screen displays for the Domain and Report Period selected.



The screen contents include:

- **Attachment Policy Violation Trends** – This box provides a graph showing the total number of inbound messages containing unwanted attachments.
- **Attachment Summary** – This box provides the Average Attachment Size as well as the total number of each attachment type allowed.
- **Attachment Policy Actions** – This box provides a chart showing the Attachment Policy actions enforced for messages containing policy-limited or disallowed attachments.

7.8 Viewing a User Activity Report

The User Activity report provides brief statistics on the top five inbound message recipients, which you can download.

You can access the User Activity screen by selecting **User Activity** from the **Report** drop-down list.

The User Activity screen displays for the Domain and Report Period selected.

Reports and Statistics

Domain:
Report:
Report Period:

[Download]

Top Inbound Users		
Email Address	Messages	Size
tom.spears@karmaroo.com	2898	81MB
rex.ford@karmaroo.com	2598	63MB
peter.shipley@karmaroo.com	2584	64MB
austin.powers@karmaroo.com	2498	65MB
brad.johnson@karmaroo.com	2333	58MB

The **Top Inbound Users** box lists the five users who received the most messages and the size of the total messages received (over the Report Period you selected).

You can download the list displayed by clicking the **Download** text-link.

7.9 Viewing an Event Log Report

The Event Log indicates when and what type of threat events were detected during the report period selected; it also indicates what action was taken against each threat according to the policies you configured.

You can access the Event Log screen by selecting **Event Log** from the **Report** drop-down list.

The Event Log screen displays for the Domain and Report Period selected.

Reports and Statistics

Domain: Report: Report Period:

Display: [Download]

Pages: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) ... [Next >] Page 1 of 37

Type	Timestamp	From	To	Subject	Details	Action
Content	06/01 00:02	tspears@mxlogic.ne	tom.spears@karmaroo.	Hows it going I	secret	denied
Content	06/01 00:04	tspears@mxlogic.ne	tom.spears@karmaroo.	We Want Your Sk	secret	quarantined
Attachment	06/01 00:04	bjohnson@mxlogic.n	brad.johnson@karmaro	Run Me	Executables	denied
Content	06/01 00:08	apowers@mxlogic.ne	austin.powers@karmar	Hows it going I	proprietary	denied
Attachment	06/01 00:13	bjohnson@mxlogic.n	brad.johnson@karmaro	Pass this on.	Executables	denied
Content	06/01 00:16	rford@mxlogic.net	rex.ford@karmaroo.co	Let's Go Get St	proprietary	quarantined
Attachment	06/01 00:17	pshiple@mxlogic.n	peter.shiple@karmar	Run Me	Executables	denied
Content	06/01 00:18	apowers@mxlogic.ne	austin.powers@karmar	We Want Your Sk	secret	quarantined
Content	06/01 00:19	bjohnson@mxlogic.n	brad.johnson@karmaro	Increase your p	secret	quarantined
Attachment	06/01 00:19	pshiple@mxlogic.n	peter.shiple@karmar	Run Me	Executables	denied
Content	06/01 00:21	pshiple@mxlogic.n	peter.shiple@karmar	We Want Your Sk	secret	quarantined
Attachment	06/01 00:22	pshiple@mxlogic.n	peter.shiple@karmar	Urgent	Executables	denied
Content	06/01 00:25	rford@mxlogic.net	rex.ford@karmaroo.co	Sybil , Please	secret	quarantined
Content	06/01 04:18	apowers@mxlogic.ne	austin.powers@karmar	Hows it going I	proprietary	denied
Content	06/01 04:25	rford@mxlogic.net	rex.ford@karmaroo.co	Quit Smoking in	proprietary	quarantined
Content	06/01 04:26	rford@mxlogic.net	rex.ford@karmaroo.co	Am I Crazy?? Or	secret	quarantined
Content	06/01 04:30	tspears@mxlogic.ne	tom.spears@karmaroo.	Hows it going I	proprietary	denied

Pages: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) ... [Next >] Page 1 of 37

- The log automatically displays all events (default).
- Each page lists up to 100 events. You can view additional pages by either clicking the **Next >** or **< Prev** links or clicking on the specific page number link.

1. To limit the items displayed by Type, select an option from the Display drop-down list:



2. To download the event log as shown, click the **Download** text-link.

Note: The file that downloads will contain all the events for the Display type selected in step 1.

7.10 Viewing an Audit Trail Report

Using the “Audit Trail” feature, you can monitor who in your domain(s) has logged into the MX Control Console and any system changes made. This report provides information on who has logged into the Console to access the domain selected, and what actions and/or policy changes were made by those users, over a certain time period.

You can access the Audit Trail screen by selecting **Audit Trail** from the **Report** drop-down list.

The Audit Trail screen displays for the Domain and Report Period selected.

Reports and Statistics

Domain:
Report:
Report Period:

[\[Download \]](#)

Pages: 1 2 [\[Next >\]](#) Page 1 of 2

Timestamp	Domain	Details
06/07 14:54	karmaroo.com	User demo@karmaroo.com updated the content group
06/07 14:54	karmaroo.com	User demo@karmaroo.com unsubscribed from the custom content group for Inbound traffic
06/07 14:54	karmaroo.com	User demo@karmaroo.com changed the Inbound action for the custom content group from "TAG" to "QUARANTINE"
06/07 14:53	karmaroo.com	User demo@karmaroo.com subscribed to the custom content group for Inbound traffic
06/07 14:53	karmaroo.com	User demo@karmaroo.com created the custom content group
06/07 14:46	karmaroo.com	User demo@karmaroo.com logged in
06/06 14:47	karmaroo.com	User chris.readle@karmaroo.com logged in
06/06 14:47	karmaroo.com	User chris.readle@karmaroo.com logged in
06/06 10:25	karmaroo.com	User NewWorldVentures@karmaroo.com logged in
06/06 09:34	karmaroo.com	User NewWorldVentures@karmaroo.com logged in
06/06 09:34	karmaroo.com	User NewWorldVentures@karmaroo.com logged in
06/02 16:59	karmaroo.com	Reseller Admin chris.giblin@karmaroo.com added domain tucowstestdomain.com to customer Tucows Reseller

Pages: 1 2 [\[Next >\]](#) Page 1 of 2

- Each page lists up to 100 actions. You can view additional pages by either clicking the **Next >** or **< Prev** links or clicking on the specific page number link.

To download the event log as shown, click the **Download** text-link.

FAQs

Q: How does MX Logic Email Defense Service affect my MTA?

A: The MX Logic Email Defense Service architecture naturally provides high-level redundancy and disaster recovery by leveraging a secondary MX record set to your internal mail servers. The service is currently configured to deliver your inbound SMTP traffic to the Message Transfer Agent(s) on your premises configured during the setup process.

At anytime, you may change the address of where you want your incoming email traffic delivered through the MX Control Console. Be prudent when making changes to your delivery MTA configuration as any modifications will be enabled instantly and affect inbound SMTP routing.

Q: What are the default Anti-Virus policies?

A: The MX Logic engineering staff has created a set of default policies for the pilot period that should provide adequate protection from virus and spam threats. Currently, your Anti-Virus policy is configured to clean messages that contain viruses or infected attachments. If a message cannot be cleaned, the offending attachment(s) will be stripped from the email before delivery occurs. The recipient will be notified in either case with the results of the cleaning attempt.

You can also choose whether infected mail should be denied delivery, stripped, or quarantined. You can view the virus quarantine where you can take further action.

Q: How does the MX Logic Email Defense Service score spam? What about “false positives”?

A: The Anti-Spam filtering technology detects the likelihood that an email is spam by processing the message through blacklists, a heuristics engine, a statistical classification engine, and a distributed checksum clearinghouse, all as part of its Stacked Classification FrameworkSM. Each test provides a weighted score that is added to the overall “spam score”. We have pre-defined a threshold score for your Anti-Spam policy.

It is important to note that some messages might be marked as spam when in fact they are legitimate emails. While we believe that this “false positive” tagging will not be a frequent occurrence, it may happen occasionally, especially to mailing-list and newsletter traffic. In such cases, we ask that you help us “tune” our spam thresholds and rules by sending a forwarded copy of the message to spam@mxlogic.com. Your interaction is crucial in helping us build better Anti-Spam rules.

Via the MX Control Console, you can quarantine, tag, or block emails based on corresponding sensitivity levels. Additionally, you can construct enterprise-level “Allow” and “Deny” lists that override spam sensitivity levels. Finally, you can turn on or off

MAPSSM features, including the Realtime Blackhole List (RBL)SM, the Relay Spam Stopper List (RSS)SM and the Dial-up User List (DUL)SM. The default setting for each of these features is “enabled”.

Glossary

Definitions

Allow List	A list of acceptable sender email addresses. This ensures that all email from the listed addresses will be delivered (unless they contain a virus, in which case they will be filtered according to the Virus Policies configured for your domain).
Attachment	Any file attached to an email message; these are usually encoded to cross the Internet properly and decoded once they are received.
Deny Delivery	An option to refuse messages because they contain a virus, unwanted content, attachments or HTML, or are probably spam. This option must be configured within MX Control Console's "Policies" page.
Deny List	An option to create a list of unacceptable senders (using email or domain addresses). This option ensures that any email from these addresses will never be delivered to your enterprise.
Domain	A network of computers administered as a unit that share part of a common IP address.
DUL	<u>Dial-up User List</u> : A database maintained by MAPS (see MAPS definition) of known spammers who use direct connections to send junk email to victim's mail servers.
Junk Email	See Spam .
MAPS	<u>Mail Abuse Prevention System</u> : Subscription-based "deny" or blacklist database of known spammer addresses. (From more information, see the website: http://mail-abuse.org .)

MIME	<u>M</u> ultipurpose <u>I</u> nternet <u>M</u> ail <u>E</u> xtensions: A standard for encoding attachments so that they can be sent over the Internet .
MTA	<u>M</u> essage <u>T</u> ransfer <u>A</u> gent: Program responsible for routing and delivering incoming email to individual users.
MX Record	<u>M</u> ail <u>E</u> xchange Record: Entry in a DNS database identifying the mail server that handles email for a specific domain.
Prepend “SPAM:”	An option within the MX Control Console’s Anti-Spam configuration policies. This option will attach (or “tag”) the word “SPAM:” to the subject line of the message suspected as junk email, and deliver it. This will warn recipients that the message is possibly spam before they open it.
Quarantine	If configured to do so, MX Logic Email Defense Service will hold messages that contain viruses, unwanted attachments or content, or which are suspected to be spam. These messages are kept safely away from an enterprises’ network (in quarantine), and can be reviewed by an administrator (or the messages recipient) and either deleted or released.
RBL	<u>R</u> ealtime <u>B</u> lackhole <u>L</u> ist: A system maintained by MAPS (see MAPS definition) to create intentional network outages (“blackholes”) for the purpose of blocking spam. The RBL is essentially a database of known spammer addresses.
Recipient	The person for whom an email message is intended.
RSS	<u>R</u> elay <u>S</u> pam <u>S</u> topper: A database maintained by MAPS (see MAPS definition) of known spam-relaying mail servers.

SMTP	<u>S</u> imple <u>M</u> ail <u>T</u> ransport <u>P</u> rotocol: Most common protocol for sending email.
Spam	Unsolicited commercial email, also called “junk email”.
Tag Subject	An option to place a “tag” or warning within the subject line of a suspicious message to warn the recipient that the message may contain unwanted content, or may be junk email. See also Prepend “SPAM:” .
Virus	Code or programs loaded onto computers without users’ knowledge that was created to cause damage or inconvenience to users and their systems.